Mag. Margot Artner Rechtsanwalt

Bundeskanzleramt
Verfassungsdienst

PER E-MAIL: v@bka.gv.at

Präsidium des Nationalrats

PER E-MAIL: begutachtungsverfahren@parlament.gv.at

20. Juni 2008
VSÖ/DSG08/MA/16.doc

Stellungnahme des Verbands der Sicherheitsunternehmen Österreichs zum Entwurf eines Bundesgesetzes, mit dem das Bundesgesetz über den Schutz personenbezogener Daten geändert wird (DSG-Novelle 2008) – BKA 810.026/0002-V/3/2008

Sehr geehrte Damen und Herren,

der VSÖ Verband der Sicherheitsunternehmen Österreichs ist ein neutral und gremial zusammengesetzter Verband von Sicherheitsunternehmen aus den Sparten elektronische Sicherheitstechnik, mechanische Sicherheitseinrichtungen und Sicherheitsdienstleistungen. Unter Mitwirkung der Exekutive, der Versicherungswirtschaft, der Wissenschaft und staatlich geprüfter Zivilingenieure gewährleistet er die Qualität von Sicherheitsprodukten und –dienstleistungen. Dies geschieht – einem Verbandsziel folgend – zum Nutzen der Anwender und zur Erhöhung der allgemeinen Sicherheit in Österreich.

Der VSÖ Verband der Sicherheitsunternehmen Österreichs hat mich mit der Erstattung der folgenden Stellungnahme zu dem im Betreff genannten Gesetzesentwurf (DSG-Novelle 2008), insbesondere zum neu geregelten Themenkomplex „Videoüberwachung“ beauftragt:

1. Meine Mandantschaft begrüßt das grundsätzliche Anerkenntnis von **Videoüberwachung als Mittel der Gefahrenabwehr durch Private**.

Wipplingerstraße 19
A -1010 Wien
Telefon +43 (1) 535 18 35
Fax +43 (1) 535 18 35-10
rechtsanwalt@margot-artner.at
www.margot-artner.at
UID: ATU56784233
Kto. Nr.: 10561863101
BLZ: 12000

Aus ihrer beruflichen Praxis wissen die Mitglieder meiner Mandantschaft, dass Videoüberwachung ein unverzichtbarer Bestandteil der Objektsicherung ist. Videoüberwachung hält die überwiegende Zahl möglicher Täter von Angriffen gegen das überwachte Objekt ab. Nur Täter in geistigen Ausnahmesituationen greifen vor laufender Kamera an. Nach erfolgten Angriffen liefert nur die Videoüberwachung mit Bildaufzeichnung (anders als alle anderen Sicherheitssysteme) jene Informationen, die zur Aufklärung, Täterergreifung und damit möglichen Schadenswiedergutmachung erforderlich sind.[1]

Es mag sein, dass Sicherheitstüren oder Alarmanlagen Angriffe auf Objekte verhindern können, zu denen nur wenige Personen Zugang haben. Überall dort, wo viele Personen ein- und ausgehen (Geschäfte aller Art, Museen, Banken etc.), lassen sich die geschützten Objekte nicht einfach wegsperren. Elektronische Warensicherungen sind heute genauso schnell entfernt wie Autos aufgeknackt. Noch schneller kann ein RFID-Chip von gesicherten Waren gekratzt werden. Der Einsatz von Wachpersonal anstelle von Videoüberwachungskameras ist nicht finanzierbar: Sollten Wachleute vergleichbare Areale überwachen, würden die dafür anfallenden Lohnkosten in der Regel schon nach einem Monat die Anschaffungskosten einer Videoüberwachungsanlage übersteigen.

Fazit: Im Bereich der Prävention können alternative Sicherheitstechnologien Videoüberwachung ergänzen aber nicht ersetzen. Im Bereich der Aufklärung gibt es keine Alternative zur Videoüberwachung[2].

2. Eingriff in den Anspruch auf Geheimhaltung?

Um die Frage nach einem Eingriff in Geheimhaltungsinteressen betroffener Personen durch Videoüberwachung beurteilen zu können, stelle ich im Folgenden kurz eine durchschnittliche Videoüberwachungsanlage dar.

Diese ist als solche gekennzeichnet (schließlich soll sie ja auch präventiv wirken) und damit für jedermann erkennbar. Die Kameras liefern Bilddaten von allen Personen, die die überwachte Zone (zB ein Geschäftslokal, eine Bank, ein Museum, ein Firmengelände etc.) betreten. In der Regel handelt es sich um Personen, die dem Auftraggeber der Videoüberwachung nicht bekannt sind. Die Bilder werden aufgezeichnet. Niemand schaut sie an (niemand hat Zeit, die unzähligen Bilder „aus Langeweile oder Neugier“ zu sichten). Nach einigen Tagen werden sie automatisch gelöscht.

---

1) Zur Eignung von Videoüberwachung zur Prävention und Aufklärung von Kriminalität: Erläuterungen zur Regierungsvorlage zur SPG-Novelle 2005, *Pürstl*/*Zirnsack*, SPG (2005), § 54, Anm 46ff.

2) Schwerpunktkontrollen durch die Polizei – wie *Gregor König* in seinem Beitrag „Videoüberwachung und Datenschutz – Ein Kräftemessen“ (*Jahnel*/*Siegwart*/*Fercher*, Aktuelle Fragen des Datenschutzrechts) anführt - wären zwar wünschenswert, stehen aber nicht zur Disposition des Einzelnen, der idR sein Eigentum schützt. Andere Beweise (zB Fingerabdrücke, genetische Spuren, Zeugen) stehen in den seltensten Fällen zur Verfügung. Überdies wären sie nur dann nutzbar, wenn entsprechende Datenbanken vorhanden wären (zB Datenbanken mit genetischem Material aller Bürger, wenig wünschenswert im Sinne des Datenschutzes).
Maskierte Täter nehmen ihre Maske spätestens beim Verlassen der überwachten Zone (also in der Regel noch im Blickfeld der Kameras) ab, da sie sonst auffallen würden. Im Übrigen liefern auch Bilder von vermummten Tätern zweckdienliche Hinweise.

Nur im klar vorab definierten Anlassfall (zB Angriff auf das geschützte Objekt – Vandalismus, Diebstahl, fahrlässige Sachbeschädigungen durch Kraftfahrzeuge) werden die zeitlich und örtlich in Frage kommenden Bilddaten eingesehen. Die relevanten Daten, die den Anlassfall zeigen, werden gesondert gespeichert. Noch immer ist keine Personenidentifizierung erfolgt; denn dazu benötigt der Auftraggeber der Videoüberwachung die Hilfe der Sicherheitspolizei.

Oft bestehen Videoüberwachungsanlagen aus mehreren Übersichtskameras, deren Bildqualität eine Personenidentifizierung nicht zulässt, und bloß einer Detailkamera mit besserer Bildauflösung im Ausgangsbereich. Im Anlassfall werden die relevanten Personen über die Übersichtsbilder bis zur Detailansicht verfolgt. Erst anhand der Detailaufnahme kann die Polizei die Identität der Betroffenen feststellen. In solchen Fällen werden keine zuordenbaren Bilder von Unbeteiligten eingesehen.

Unabhängig von der Ausgestaltung der Videoüberwachung sind nur jene Personen betroffen, die sich im unmittelbaren räumlichen und zeitlichen Umfeld eines entsprechenden Anlassfalls befinden. Dabei handelt es sich in der Regel um den Angreifer selbst sowie allfällige zufällig anwesende Personen, deren Identität gar nicht ausgeforscht wird. Es bedarf wohl keiner Erörterung, dass das Interesse des Geschädigten an der Aufklärung des Angriffs allfällige Geheimhaltungsinteressen des Angreifers überwiegt. Die Identität anderer Personen wird mangels Relevanz gar nicht festgestellt.

Das Bild eines Unbekannten erlaubt dem Auftraggeber einer Videoüberwachung nicht, dessen Identität mit vernünftigen Mitteln festzustellen. Sogar die Polizei muss ausgiebig recherchieren, um Bildern Namen zuzuordnen.

Ebenfalls von Bedeutung für die Frage der Eingriffsintensität ist der Ort der Videoüberwachung: Wer ein Geschäft, eine Bank oder ein Museum betritt, bewegt sich in der Öffentlichkeit. Er/sie rechnet damit, von anderen Menschen gesehen zu werden. Aufgrund der Kennzeichnung weiß er/sie von den Videokameras. Der überwiegende Teil der Bevölkerung akzeptiert solche Videoüberwachungsanlagen und fühlt sich dadurch nicht gestört.

Zusammengefasst ist die Beeinträchtigung der betroffenen Personen – bei entsprechender Ausgestaltung der Videoüberwachung (Privatsphäre frei von Kameras, Kennzeichnung, Zugriff auf gespeicherte Daten nur im Anlassfall und nur durch Berechtigte, Identitätsfeststellung nur wenn unbedingt erforderlich) – ausgesprochen gering.

3. Aktuelles zu Videoüberwachungsanlagen und deren Registrierung (Vorabkontrolle)

Aus den oben dargestellten Gründen haben sich nicht nur zahlreiche öffentliche Stellen sondern auch unzählige Private, vorwiegend Gewerbetreibende und Unternehmer, zur Installation von Videoüberwachungskameras entschlossen und beträchtliche finanzielle Mittel in diese Technologie investiert; dies häufig auf Empfehlung der Polizei.

Auch die Mitglieder meiner Mandantschaft (Sicherheitsunternehmen) sind verpflichtet, ihre Kunden entsprechend dem Stand der Technik und der Kriminalitätsentwicklung zu beraten: Aufgrund ihrer Erfahrung und Fachkenntnis müssen sie vielen Kunden Videoanlagen als wesentlichen und vergleichsweise kostengünstigen Bestandteil eines zuverlässigen Sicherheitskonzepts empfehlen. Damit geraten sie allerdings – ebenso wie ihre Kunden – in einen Interessenskonflikt:

Denn Videoüberwachung gilt, wenn auf den Bildern Personen zu sehen sind, nach der derzeit herrschenden Interpretation der Rechtslage als Eingriff in das Recht auf Geheimhaltung nach § 1 Abs 1 DSG; dies mit der Konsequenz, dass jede Videoanlage zu rechtfertigen ist. Selbst dann, wenn sie alle Anforderungen des DSG erfüllt, darf sie erst nach Vorabkontrolle durch die Datenschutzkommission den Betrieb (die Bildaufzeichnung) aufnehmen[3].

Erfahrungsgemäß nimmt das Vorabkontrollverfahren derzeit zumindest zwei Monate, in der Regel jedoch weit mehr Zeit in Anspruch: Reagiert die Datenschutzkommission nicht binnen zwei Monaten auf die Meldung, ist diese zu registrieren. Die Videoaufzeichnung darf aufgenommen werden.

Oft ergeht jedoch ein Verbesserungsauftrag: Ob Kameras schwenkbar sind, ob Arbeitsplätze im Blickfeld der Kameras liegen, ob eine Betriebsvereinbarung abgeschlossen wurde etc[4]. Legitime Fragen, die jedoch zu beträchtlichen Verzögerungen führen. Denn der Verbesserungsauftrag kommt erst gegen Ende der zweimonatigen Reaktionsfrist zum Auftraggeber, dessen Antwort zum Verbesserungsauftrag muss erst im System des Datenverarbeitungsregisters erfasst werden und liegt dem zuständigen Bearbeiter erst Wochen nach seinem Einlangen vor. So kann es schon ein paar Monate dauern, bis die Videoaufzeichnung starten kann.

Bis zu diesem Zeitpunkt ist aber auch schwer vorhersehbar, ob die Videoüberwachung überhaupt der Vorabkontrolle standhalten wird – eine ausgesprochen unbefriedigende Situation, sowohl für den Auftraggeber der Videoüberwachung als auch für den Anlagenerrichter.

Verschärft wird die Thematik dadurch, dass der Bevölkerung die Anwendung des Datenschutzgesetzes auf Videoüberwachungsanlagen und die Meldepflicht erst aufgrund der verstärkten Medienberichterstattung des letzten Jahres bewusst werden. Schließlich ist die Registrierung der ersten Videoanlage mit ständiger, digitaler Aufzeichnung soweit überschaubar erst im Sommer 2005 (Probebetrieb der Wiener Linien) erfolgt. Im Herbst 2006 wurden die ersten Anlagen in ständigem Echtbetrieb (nach mehrmonatigen Verfahren) registriert. Im Jänner 2007 hat es erste Informationen auf der Website der Datenschutzkommission gegeben.

Im Ergebnis gibt es tausende Videoanlagen, deren Auftraggeber erst allmählich von der Meldepflicht Kenntnis erlangen. Im Datenschutzbericht 2007 heißt es: „Derzeit (Stand: Juni 2007) liegen etwa 300 Meldungen vor, von welchen nur ein kleiner Teil

---

3) Im Hinblick auf den geplanten § 50c Abs 2 DSG 08, wonach meldepflichtige Überwachungen stets der Vorabkontrolle unterliegen, entfällt ein Eingehen auf die Auslöser der Vorabkontrolle nach aktueller Rechtslage (§ 18 Abs 2 DSG).

4) Nur am Rande sei erwähnt, dass sich diese Fragen bei Videoüberwachung in einer Bank und einem Museum nicht gestellt haben und dementsprechend schwierig vorhersehbar sind.

bereits registriert ist.“ Vielleicht sind zwischenzeitig rund 200 Videoüberwachungen registriert. Alle anderen werden somit illegal betrieben; illegal allerdings nicht, weil kein berechtigtes Interesse die Videoüberwachung rechtfertigen würde; illegal nur deshalb, weil die Auftraggeber nicht wissen oder lange nicht wussten, dass sie die Anlage melden und die Vorabkontrolle durch die Datenschutzkommission abwarten müssen.

Diesen Auftraggebern drohen beträchtliche Geldstrafen; ob ihre Investition in die Sicherheit letztlich genehmigt wird oder abzubauen ist, wird noch lange unklar bleiben. Denn aufgrund der verstärkten Medienberichterstattung langen derzeit hunderte Meldungen von Videoüberwachungen im Datenverarbeitungsregister ein. Es steht zu befürchten, dass all diese Meldungen von zwei oder drei Mitarbeitern bearbeitet werden müssen; und zwar binnen einer Frist von zwei Monaten. Will man nicht riskieren, dass eine Anlage wegen Verstreichen der Zweimonatsfrist ohne ausreichende Prüfung eingetragen wird, muss – wenn nicht ein klarer Fall zulässiger Videoüberwachung (zB in einer Bank) vorliegt – ein Verbesserungsauftrag ergehen.

Im Ergebnis warten derzeit hunderte Betreiber von Videoüberwachungsanlagen auf Vorabkontrolle und Registrierung. In dieser Situation kann die – auch in den Erläuterungen zum DSG 08 als wirksames Mittel zur Gefahrenabwehr anerkannte – Technologie der Videoüberwachung nicht zum Einsatz kommen.

4. Vorabkontrolle oder bloße Meldung?

Ich habe die aktuelle Registrierungssituation deshalb so ausführlich dargestellt, weil sich daran auch durch den vorliegenden Gesetzesentwurf nichts ändern wird. Gemäß § 50c Abs 2 DSG 08 unterliegen alle meldepflichtigen Überwachungen stets der Vorabkontrolle. Von der Meldepflicht ausgenommen sind – von allgemeinen und wenig relevanten Ausnahmen (§ 17 Abs 2 DSG) abgesehen – Überwachungen, die sich in einer bloßen Echtzeitwiedergabe und zwar zum Schutz von Leib, Leben und Eigentum des Auftraggebers erschöpfen (keine Datenspeicherung) oder Bilddaten nur auf einem analogen Speichermedium aufzeichnen.

Da die Mehrzahl der Videoüberwachungsanlagen digital aufzeichnen, bleibt es bei der Meldepflicht und damit auch Vorabkontrolle für die überwiegende Anzahl von Videoüberwachungsanlagen.

In Kombination mit der bis auf weiteres unabsehbar langen Verfahrensdauer (schließlich sind noch Tausende Videoüberwachungsanlagen zu registrieren, bevor man von einer Entspannung der Situation ausgehen kann) kommt dies einem Verbot der Videoüberwachung gleich.

Einerseits ist dadurch das Geschäftsfeld der Mitglieder meiner Mandantschaft stark eingeschränkt oder in die Illegalität gedrängt. Andererseits leidet die Sicherheit - insbesondere von jenen Personen, die sich keine aufwändigen anderen Sicherheitsmaßnahmen leisten können.

Dass ein solches in der Handhabung besonders aufwändiges Vorabkontrollverfahren nicht sein muss, zeigt der Vergleich mit anderen europäischen Ländern, die ja auch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom

24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Warenverkehr (im folgenden kurz: DS-RL) umsetzen müssen: Außer in Österreich unterliegen Videoüberwachungen nur in Luxemburg und Portugal einem ähnlichen Vorabkontrollverfahren („Prior Checking").[5]

Der entscheidende Vorschlag meiner Mandantschaft besteht daher darin, Videoüberwachungen und andere Videoanlagen zwar der **regulären Meldepflicht** (entsprechend dem DSG 08 mit sofort anschließender Registrierung nach Plausibilitätsprüfung) **nicht** jedoch der **Vorabkontrolle** durch die Datenschutzkommission zu unterwerfen.

Dadurch werden in kürzester Zeit alle derzeit „illegalen" Videoüberwachungen erfasst. Stichprobenartige Kontrollen der Behörden und Beschwerden von Betroffenen werden rasch die Spreu vom Weizen, also die Videoüberwachung zu verpönten Motiven von der Videoüberwachung zu rechtmäßigen Zwecken trennen. Gleichzeitig wäre für eine rasche Entlastung der beschränkten Personalressourcen des Datenverarbeitungsregisters und der Datenschutzkommission gesorgt, einem erklärten Ziel des DSG 08.

Die Einführung der regulären Meldepflicht und Abschaffung der Vorabkontrolle wäre durch umfassende Informationsmaßnahmen, insbesondere zur Ausgestaltung einer zulässigen Videoüberwachung, zu begleiten. Meine Mandantschaft bietet dazu gerne ihre Unterstützung an, beispielsweise durch Verteilung von Informationsblättern an ihre Mitglieder zur Weitergabe an Käufer von Videoanlagen.

Entscheidend ist, dass jene Personen, die legitime Videoüberwachungen betreiben wollen, dies in einem rechtlich gesicherten Rahmen tun können. Dass dabei die Wahrung der Rechte der Betroffenen höchste Priorität hat, ist selbstverständlich.

5. Rechtliche Qualifikation von Videoüberwachung und Anwendung des DSG

Das DSG knüpft an die Verwendung personenbezogener Daten an. Die Erläuterungen zum vorliegenden Gesetzesentwurf gehen davon aus, dass immer dann, wenn bei der Überwachung von Orten, Gegenständen und Personen durch Kameras Personen zu sehen sind, personenbezogene (Bild-)Daten im Sinn des DSG 2000 anfallen. Dafür genüge bereits Identifizierbarkeit.

Das DSG definiert personenbezogene Daten als Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist (§ 4 Z 1 DSG 2000). Betroffene sind alle vom Auftraggeber verschiedenen natürlichen Personen, deren Daten verwendet werden (§ 4 Z 3 DSG 08). Die DS-RL, in deren Licht das DSG Gemeinschaftsrechts konform auszulegen ist, geht eine Nuance weiter. So heißt es in der Erwägung 26 zur DS-RL: Bei der Entscheidung, ob eine Person bestimmbar ist, sollten alle Mittel berücksichtigt werden, die vernünftigerweise entweder von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen.

---

5) *Gregor König* in „Videoüberwachung und Datenschutz – Ein Kräftemessen" (*Jahnel*/*Siegwart*/*Fercher*, Aktuelle Fragen des Datenschutzrechts)

Zutreffend schreibt *Robert König*: „*Bei der Qualifikation von Videoüberwachung als Ermittlung personenbezogener Daten ist zu beachten, dass private Anwender im Unterschied zu den Sicherheitsbehörden idR keine Möglichkeit haben, die Identität von unbekannten Dritten im öffentlichen Raum festzustellen (keine Bestimmbarkeit). …*“ Daraus schließt *Robert König*, dass Videoüberwachung von Personen, nur dann als Datenanwendung im Sinne des § 4 Z 7 DSG gilt, wenn deren Identität für den Auftraggeber bestimmt oder bestimmbar ist. Als Beispiele führt er Videoüberwachung am Arbeitsplatz, Nachbarschaftsspionage oder Beschattung an.[6]

Auch die Datenschutzkommission geht in ihrem Bescheid vom 11. Oktober 2005, K121.036/0014-DSK/2005 davon aus, dass eine Verwendung von „personenbezogenen Daten“ im Sinne des § 4 Z 1 DSG 2000 bei Bildaufzeichnungen nur dann vorliegt, „*wenn sie in der Absicht geschieht, die darauf vorhandenen Personen zu identifizieren, wobei es genügt, wenn diese Absicht nur für bestimmte Fälle und nicht durchgängig besteht; dies schließt neben den vom DSG 2000 (§ 45) ohnehin insgesamt weitestgehend ausgenommenen Bildaufnahmen für private z.B. touristische Zwecke etwa Bildaufnahmen für Zwecke von Verkehrsstromanalysen, also für statistische Zwecke oder künstlerische oder kommerzielle Film- und Fotoherstellung mangels Absicht der Identifikation allenfalls abgelichteter Personen vom Begriff der Ermittlung personenbezogener Daten aus.* ***Fehlt das Kriterium der Identifizierungsabsicht nach dem Zweck der Herstellung von Film- oder Fotoaufnahmen****, ist dieser Vorgang – abgesehen von Datensicherheitsaspekten –* ***nicht datenschutzrelevant****.*“ (Hervorhebungen nicht im Original).

Konkret hat die Datenschutzkommission die Videoüberwachung von Hubschrauberflügen wie folgt qualifiziert: „*Die Beschwerdegegnerin* (Anm. Videoüberwacher) *hat hinsichtlich der Piloten der gefilmten Hubschrauber keine identifizierten Daten verwendet, da aufgrund des Sachverhalts feststeht, dass ja die Namen der Hubschrauberpiloten nicht bekannt waren. Es fehlte ihr auch an einer diesbezüglichen Identifizierungsabsicht … Im übrigen ist auch zu bezweifeln, dass es sich bei der Identität der Hubschrauberpiloten für die Beschwerdegegnerin überhaupt um identifizierbare Daten handelt, da es für sie unter ‚vernünftigem Aufwand’ (vergleiche Erwägungsgrund 26 der Richtlinie 95/46) wohl nicht möglich gewesen wäre, die Identität der Hubschrauberpiloten in Erfahrung zu bringen. Eine rechtliche Handhabe zur Bekanntgabe ihrer Namen bestand für sie jedenfalls nicht – dies ist nur den involvierten Behörden auf Grundlage luftfahrtrechtlicher Vorschriften … möglich.*“.

Im Ergebnis sind daher – entgegen dem Wortlaut der Erläuterungen zum Gesetzesentwurf - all jene Videoanlagen, denen überhaupt keine Identifizierungsabsicht zu Grunde liegt, schon begrifflich von der Anwendung des DSG ausgeschlossen. Personenbezogene Daten fallen nicht schon dann an, wenn Kameras Bilder von Personen liefern, sondern nur, wenn die Feststellung der Identität dieser Personen beabsichtigt ist. Eine entsprechende, ausdrückliche Klarstellung scheint im Lichte der Erläuterungen erforderlich.

6) *Robert. König*, Videoüberwachung – Fakten, Rechtslage und Ethik, 175.

6. Definition von Videoüberwachung - Unklarheiten betreffend Anwendungsbereich

Das DSG 08 (§ 50a Abs 1) definiert Videoüberwachung als systematische, insbesondere fortlaufende Feststellung von Ereignissen, die ein bestimmtes Objekt („überwachtes Objekt“) betreffen, durch technische Bildaufnahmegeräte.

Dem vorgeschlagenen Gesetzeswortlaut nach ist die Definition von Videoüberwachung besonders weit ausgefallen. Unter die angeführte Beschreibung fällt wohl jede Videoanlage, auch dann, wenn sie anderen Zwecken als der Überwachung zu Sicherheitszwecken (zB Kundenstromanalysen, Statistik etc.) dient.

Die Erläuterungen verweisen zur Definition der Videoüberwachung auf die allgemeine Definition der Datenanwendung[7] in § 4 Z 7 DSG. Während die Definition der allgemeinen Datenanwendung ausdrücklich an das Verwenden von Daten (Verweis auf § 4 Z 8 DSG) und damit den Personenbezug (bestimmt oder bestimmbar, siehe oben Punkt 5.) anknüpft, fehlt ein solcher Bezug bei der Definition der Datenanwendung Videoüberwachung. Dennoch ist davon auszugehen, dass eine Videoüberwachung nur dann betroffen ist, wenn personenbezogene Daten verwendet werden, wenn also eine Personenidentifizierung – und sei es auch nur in Einzelfällen - beabsichtigt ist. Eine ausdrückliche Klarstellung wäre wünschenswert.

Nach den Erläuterungen sollen Aufnahmen etwa aus rein touristischen oder künstlerischen Beweggründen nicht unter die Videoüberwachungsdefinition fallen. Was ist das Kriterium für diese Ausnahmen? Ist es die fehlende Absicht, die Identität eines Betroffenen herauszufinden? Wie verhält es sich, mit dem Hotelier und Schiliftbetreiber, der die Schipisten filmt, um herauszufinden, welche seiner Gäste, welche Pisten bevorzugen? Rein touristische Beweggründe? Was unterscheidet den neugierigen Nachbarn, der die Straße vor seinem Haus filmt, vom Künstler, der das bunte Treiben auf derselben Straße dokumentiert. Offenbar gilt die Ausnahme auch für Videoanlagen für Kundenstromanalysen, Frequenzzählung und andere Statistikzwecke. Ein abgrenzendes Kriterium in der Definition wäre wünschenswert.

Schließlich stellt sich auch die Frage, ob bzw. welche Regeln für Videoanlagen gelten, die keine Videoüberwachungen im Sinne des 9a. Abschnitts des DSG 08 darstellen (also zumindest jene aus rein touristischen oder künstlerischen Beweggründen). Nach den Erläuterungen fallen ja immer dann, wenn Personen auf Videobildern zu sehen sind, personenbezogene (Bild-)Daten im Sinn des DSG an. Identifizierbarkeit der Personen wäre – in diesem Sinne - gegeben. Gilt für derartige Datenanwendungen die bisherige Rechtslage mit Meldepflicht weiter? Da hier keine strafrechtlichen relevanten Daten erwartet werden, würde die Anwendung wohl nicht der Vorabkontrolle unterliegen. Oder muss man bei Videoanlagen immer mit strafrechtlich relevanten Daten rechnen? Wie verhält es sich bei derartigen Anlagen mit Zufallstreffern (§ 50a Abs 5 DSG 08)?

---

[7]) § 4 Z 7 DSG: Datenanwendung: Die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8: Jede Art der Handhabung von Daten einer Datenanwendung, also sowohl Verarbeiten als auch Übermitteln), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zwecks der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen.

Die gewählte Definition der Videoüberwachung setzt nicht voraus, dass die Bilddaten aufgezeichnet werden. Vielmehr ergibt sich aus § 50a Abs 3 Z 4 DSG 08 (Echtzeitwiedergabe zum Schutz von Leib, Leben oder Eigentum des Auftraggebers der Überwachung) dass auch bloße Life-Bild-Übertragungen Datenanwendungen im Sinne des DSG 08 sein sollen. Im Hinblick darauf, dass derartige Systeme nach aktueller Rechtslage keine Datenanwendungen im Sinne des DSG sind[8], handelt es sich um eine beachtliche und nicht zu rechtfertigende Änderung der Rechtslage.

Dies gilt um so mehr, als ja nur Echtzeit-Videoüberwachungen zum Schutz von Leib, Leben und Eigentum des Auftraggebers von der Meldepflicht ausgenommen sind (§ 50c Abs 1 Z 1 DSG 08). Echtzeit-Videoüberwachungen, die nicht dem Schutz des Auftraggebers dienen (zB von Patienten auf der Intensivstation eines Krankenhauses) sind damit nicht nur neu als Datenanwendung zu qualifizieren sondern unterliegen auch der Meldepflicht und Vorabkontrolle durch die Datenschutzkommission.

7. Rechtsgrundlagen für Videoüberwachung

In § 50a Abs 3 DSG 08 ist geregelt, unter welchen Umständen Videoüberwachung schutzwürdige Geheimhaltungsinteressen von Betroffenen nicht verletzt. Die Aufzählung ist abschließend.

An dieser Stelle sollten die überwiegenden berechtigten Interessen möglicher Auftraggeber derart definiert sein, dass jeder klar erkennen kann, unter welchen Voraussetzungen Videoüberwachung zulässig ist. Auch ohne Jusstudium sollten Auftraggeber und Betroffene erkennen können, wer wo wozu unter welchen technischen Bedingungen videoüberwachen darf. Aus Sicht meiner Mandantschaft stellt der vorliegende Entwurf im Vergleich zur geltenden Rechtslage keine wesentliche Verbesserung dar.

Dem Wortlaut nach scheint die Regelung ausreichend, um alle rechtmäßigen Videoüberwachungen zu Sicherheits- und Beweiszwecken zu erfassen; schließlich soll Videoüberwachung zulässig sein, wenn Rechtsvorschriften dem Auftraggeber spezielle Sorgfaltspflichten auferlegen (Z 6) oder die Videoüberwachung zur Geltendmachung rechtlicher Ansprüche des Auftraggebers vor Gericht erforderlich ist (Z 7). Es hat den Anschein, als dürfte jeder, der eine Beeinträchtigung seines Eigentums oder Schadenersatzansprüche Dritter fürchtet, auf das Mittel der Videoüberwachung zurückgreifen.

Dies ist nicht der Fall. So scheinen vertragliche Sorgfaltspflichten nicht von Z 6 erfasst zu sein. Und die Anspruchsverfolgung im Gerichtsverfahren nach Z 7 muss schon „manifest“ und mittels Klage oder Klagsentwurf belegbar sein. Dem Umstand, dass Videoüberwachung Gerichtsverfahren vermeidet (aufgrund der eindeutigen Beweislage ist eine Klage nicht mehr erforderlich), wird nicht Rechnung getragen. Der Vorbereitung eines konkreten Gerichtsverfahrens kann Videoüberwachung schon aufgrund des langen Vorabkontrollverfahrens nicht dienen.

---

[8]) Vgl. Datenschutzbericht 2007, Seite 65

Wer fahrlässige Sachbeschädigungen (zB durch ein- und ausfahrende Fahrzeuge im Einfahrtsbereich eines Werks) fürchtet, wird sich nach dem DSG 08 schwer tun, eine Rechtsgrundlage für die Installation einer Videoüberwachung zu finden. Denn auch der in Z 5 angeführte drohende gefährliche Angriff erfasst nur Vorsatzstraftaten.

Allerdings rechtfertigt nach dem Gesetzesentwurf nicht jede Sorge vor gefährlichen Angriffen die Schutzmaßnahme der Videoüberwachung: Es müssen schon bestimmte Tatsachen vorliegen, die diese Sorge rechtfertigen. Auch wenn diese bestimmten Tatsachen nur beispielhaft angeführt sind, lassen sie doch Rückschlüsse auf die Wertung des Gesetzgebers zu.

So lässt sich aus dem Kriterium eines bereits – und zwar vor nicht länger als zehn Jahren - erfolgten Angriffs auf das überwachte Objekt schließen, dass länger zurückliegende Angriffe oder Angriffe auf vergleichbare Objekte nicht ausreichen, eine Videoüberwachung zu rechtfertigen.

Gleiches gilt für den Betrag von EUR 100.000,00, den der Wert beweglicher Gegenstände übersteigen muss, um eine Videoüberwachung zu rechtfertigen. Tatsächlich reichen viel niedrigere Beträge, um Überfälle zB auf Taxifahrer und Trafikanten auszulösen. Wird eine Videoüberwachung unzulässig, wenn die überwachten Objekte im Lauf der Zeit an Wert verlieren? Sind Immobilien nicht schützenswert? Fließt die Wertgrenze auch in die Beurteilung der anderen Rechtfertigungsgründe ein?

Im Ergebnis scheint eine abschließende Regelung der Rechtsgrundlagen für Videoüberwachung kaum denkbar. Zumindest sollten zusätzliche Regelungen für **fahrlässige Sachbeschädigungen** sowie für die Beweisführung im Bereich **vertraglicher Haftung** und vor einem bzw. **anstatt eines konkreten Gerichtsverfahrens** Eingang in den Gesetzestext finden. Im Bereich des gefährlichen Angriffs sollte die **Wertgrenze deutlich gesenkt** werden. Auch **Angriffe auf mit dem überwachten Objekt vergleichbare Objekte** sollten bei Beurteilung der Wiederholungsgefahr einbezogen werden (zB Wohnungseinbrüche im selben Viertel, Überfälle auf andere Taxifahrer etc.).

Abschließend ist noch festzuhalten, dass die angeführten Rechtfertigungsgründe auf Videoanlagen zu Sicherheits- und Beweiszwecken zugeschnitten sind. Soll das DSG 08 bzw. dessen Abschnitt 9a (Videoüberwachung) auch auf Videoanwendungen ohne Sicherheits- oder Beweiszweck anwendbar sein, wären auch für diese Anwendungen entsprechende Rechtsgrundlagen zu definieren. Zu denken ist hier an Videoanlagen für Kundenstrom- und Verkehrsstromanalysen, touristische Zwecke, Eventmarketing, Gegensprechanlagen mit Videofunktionen, Babyphon, Regalgestaltung in Filialen durch Designer in der Zentrale, Videotelefonverbindungen in internationalen Konzernen und die zahlreichen Bildanalyseanwendungen (Verkehrsregelung entsprechend dem Verkehrsaufkommen, Organisation und Sicherheit von Zügen, Industrielösungen zur automatischen Überwachung von Fließbändern und anderen maschinellen Arbeitsabläufen, automatische Kontrolle des Befüllungsstands von Produktionsmaschinen, etc.).

8. Höchstpersönlicher Lebensbereich

Videoüberwachungen nach § 50a Abs 3 Z 4 bis 7 (also die primär praxisrelevanten Anwendungen) dürfen nicht an Orten erfolgen, die zum höchstpersönlichen Lebensbereich eines Betroffenen gehören.

Soweit überblickbar verwendet das österreichische Recht den Begriff des höchstpersönlichen Lebensbereichs bis dato nicht im Zusammenhang mit Orten. Unter dem höchstpersönlichen Lebensbereich des § 7 Mediengesetz ist verkürzt dargestellt das Leben mit der Familie, die Gesundheitssphäre, das Sexualleben zu verstehen. Er scheint sich mit dem durch Art 8 MRK geschützten Privat- und Familienleben zu decken. Die geschützte Privatsphäre ist also nicht auf bestimmte Orte beschränkt.

Bis sich also Rechtsprechung zur Definition des höchstpersönlichen Lebensbereichs im Sinne des DSG 08 entwickelt, wird einige Zeit vergehen. Um sofort Rechtssicherheit zu schaffen, ist eine **Definition**[9] des Begriffs wünschenswert.

9. Aufzeichnungsdauer von 48 Stunden

Die Erfahrung hat schon jetzt gezeigt, dass Private in den seltensten Fällen mit einer derart kurzen Aufzeichnungsdauer das Auslangen finden. Bis zur Entdeckung eines Anlassfalls (zB Schaden oder Fehlbestand) vergehen oft mehrere Tage.

Schließlich ist auch dafür Sorge zu tragen, dass nur zuständige, geschulte Personen nach entsprechender innerbetrieblicher Beschlussfassung Einsicht in die Bildaufzeichnungen nehmen. Und diese Personen sind nicht immer verfügbar. Anders als die Sicherheitsbehörden, die sich ausschließlich der Kriminalitätsbekämpfung widmen, haben Private nur begrenzte Ressourcen. Sie benötigen daher in der Regel eine längere Aufzeichnungsdauer, um tatsächlich von der Videoüberwachung zu profitieren.

Für all diese Fälle verlangt das DSG 08 eine Genehmigung der Datenschutzkommission. Diese Regelung trägt nicht zur Entlastung der Datenschutzkommission bei sondern erhöht deren Aufwand.

Verlängert man die reguläre **Aufbewahrungsdauer auf vierzehn Tage**, sind die Geheimhaltungsinteressen der Betroffenen durch automatische Datenlöschung nach einem absehbaren Zeitraum gewahrt; und zwar ohne zusätzliche Personalressourcen im Bereich Datenschutz in Anspruch zu nehmen.

---

9) Nach dem deutschen Strafgesetzbuch ist strafbar, wer von einer Person, die sich in einer Wohnung oder einem gegen Einblick besonders geschützten Raum befindet, unbefugt Bildaufnahmen herstellt … .

10. Kurze Übergangsfrist:

Wenig erfreulich für all jene, die als Vorreiter ihre Videoüberwachungen gemeldet haben, ist die kurze Übergangsfrist: Zahlreiche nach alter Rechtslage erstellte Meldungen werden in Kürze noch vor ihrer Registrierung überholt sein. Manche Videoüberwachungen sind zwar nach alter nicht jedoch nach neuer Rechtslage zulässig.

Selbst registrierte Videoüberwachungen dürfen nur noch bis 1. Juli 2010 nach alter Rechtslage betrieben werden. Dies stellt doch einen erheblichen Eingriff in die Rechte jener dar, die beachtlichen Aufwand nicht nur in die Sicherheitstechnik sondern auch in ein langwieriges Registrierungsverfahren investiert haben.

Meine Mandantschaft hofft, dass ihre Argumente und Anregungen Eingang in die bevorstehende Überarbeitung des Gesetzesentwurfs finden.

Mit freundlichen Grüßen
Mag. Margot Artner