

1. Vorschlag zur Durchsetzung der Bestimmungen

Ein prinzipielles Problem der Videoüberwachung ist die Durchsetzung der Gesetze in diesem Bereich. Es gibt Schätzungen, dass zurzeit nur ca. 10% der Anlagen registriert sind. Es ist fraglich, ob dieser Prozentsatz nach einer Gesetzesänderung steigt wenn das Gesetz keine Kontrolle vorsieht. Daher würde ich mich für eine verpflichtende Überprüfung (z.B. einmal im Jahr) durch eine unabhängige Firma aussprechen. Eine solche Überprüfung würde gleichzeitig die flächendeckende Einhaltung der Gesetze garantieren, die staatliche Verwaltung aber nicht belasteten. Die Kosten sind vom Betreiber zu zahlen, nicht allzu hoch und berechenbar.

Wer eine Videoüberwachungsanlage betreiben will, müsste für diese einen Überprüfungsvertrag mit einer dementsprechenden Firma abschließen.

Diese Firma hält dann unangemeldet Überprüfungen ab und würde die rechtmäßige Verwendung der Anlage feststellt (z.B. mit Siegel an den Hinweisschildern). Auch bei Videoanlagen ohne Übertragung könnte damit sichergestellt werden, dass nicht trotzdem aufgezeichnet wird.

Ein solches Kontrollsystem funktioniert sehr gut in der biologischen Landwirtschaft.

Bsp.: 1. Die Bilder einer Kamera werden offiziell nicht aufgezeichnet, in Wirklichkeit jedoch archiviert und sind ohne geeignete Sicherung aus dem Internet abrufbar.

2. Wie soll die DSK oder ein Betroffener feststellen ob biometrische Systeme angewendet werden oder die Daten wirklich nur 48h gespeichert werden?

2. DVR-Nummer auf den Hinweisschildern

Es sind Hinweisschilder für überwachte Bereiche geplant. Es wäre sinnvoll die DVR-Nummer angeben zu müssen da somit sofort feststellbar ist ob es sich um eine beim DVR gemeldete Anlage handelt. Außerdem sollte noch mal ausdrücklich auch bei Live-Übertragungen darauf hingewiesen werden, dass Hinweistafeln notwendig sind.

Bsp.: Betreiber zeichnet ohne Genehmigung auf, auf Anfragen reagiert er nicht, die Hinweisschilder enthalten aber Hinweis und Namen des Betreibers.

3. Überwachung von geschlossenen Personenkreisen

Bei geschlossenen Betroffenenkreisen ist es unbedingt notwendig, dass die Betroffenen einer Videoüberwachung zustimmen müssen (z.B. bei Schulen, Miethäusern, Firmen etc.) oder zumindest Parteistellung vor der DSK haben. Eine Videoüberwachung die sich nur auf einen bestimmten Kreis an Personen bezieht kann keinesfalls über die Köpfe der Betroffenen hinweg genehmigt werden.

Bsp.: 1. Ein Schuldirektor will eine Schule aufgrund einer Sachbeschädigung überwachen. Lehrer und Schüler sind großteils dagegen und haben andere Vorschläge zur Eindämmung des Problems.

2. Eine Firma überwacht Ihre Mitarbeiter am Arbeitsplatz (Lidl-Skandal in der BRD).

4. Möglichkeit der Standartanwendung (§ 50c Abs. 1 iVm. §17 Abs. 2)

Das nach dem neuen Gesetz ausdrücklich die Möglichkeit einer Standartanwendung „Videoüberwachung“ besteht halte ich für sehr gefährlich.

Bei der Videoüberwachung handelt es sich um einen durchaus schweren Eingriff in die Rechte der Betroffenen was auch von weiten teilen der Bevölkerung so empfunden wird. Die Möglichkeit einen solchen Eingriff ganz ohne die Kontrolle der DSK zu erlauben halte ich für nicht hinnehmbar, da besonders die Betroffenen nur sehr schwach mit Rechten ausgestattet sind.

Ich denke eine Standartanwendung würde die Flut von Überwachung nur durch die Hintertüre legalisieren. Es kann nicht sein, dass man es den Betreibern so leicht macht so tief in die Rechte von Betroffenen einzugreifen.

5. Nachweis über die Effektivität

In vielen Fällen wird eine Videoüberwachung aus Kostengründen betrieben (z.B. Eindämmung von Diebstahl oder Vandalismus). Es ist aber oft fraglich ob die Überwachung den gewünschten Effekt bringt. Ich denke daher, dass die Bewilligungen an einen Nachweis der Effektivität gebunden sein sollten. Es kann nicht sein, dass in die Rechtssphären Dritter eingegriffen wird wenn das Interesse des Betreibers nicht auch effektiv erfüllt wird. Die Betreiber sollten daher genaue Ziele definieren und die Erfüllung dieser Ziele beweisen müssen.

Bsp.: Wiener Linien haben mit der Begründung Kosten zu sparen € 3,7 Mio. für eine Einsparung von max. € 200.000/Jahr investiert. Durchrechnungszeitraum ohne Betriebskosten: 18 Jahre. Die Technik wird jedoch vermutlich nach 5-10 Jahren ersetzt werden müssen (techn. Fortschritt) und die Einsparungen von €200.000 sind nach der Erfahrung von 3 Jahren Testzeit sicher nicht erreichbar.

6. Problematik der Videoaufzeichnung bei Verkehrsbetrieben (§50a Abs. 3 Z 6)

Ich würde weiters noch genauer Überlegen ob nicht gerade z.B. bei Verkehrsbetrieben die erlangten Daten aller Betroffenen einen erhöhten Schutzwert genießen müssen. Die Videoüberwachung der gesamten U-Bahn (wie in Wien geplant) zeichnet täglich jede Bewegung der 1,3 Mio. Fahrgäste genau auf.

Betriebe im öffentlichen Interesse bieten auch dem Benutzer keine Ausweichmöglichkeit um der Videoüberwachung zu entgehen. Der Rückgriff z.B. auf §19 EisenbahnG in der Erörterung scheint mir fraglich, da eine Steigerung der Betriebssicherheit durch die Videoüberwachung eher fraglich scheint.

Auch ist es sicher nicht Aufgabe des Betreibers, sondern die der Polizei, auf die Jagt nach Dieben etc. zu gehen. Weiters sind gerade bei Verkehrsbetrieben besondere Schutzmaßnahmen für die Kunden vorhanden (z.B. Kontrahierungszwang §3 EBG).

Selbst wenn jedoch diese Betriebe eine solche Sorgfaltspflicht hätten, kann dies nur zu einer Videoüberwachung gewisser Problembereiche führen und nicht zu einer Generalvollmacht für die Überwachung aller Bahnhöfe etc. verkommen.

Analog müsste sonst die Pflicht der Polizei für Sicherheit zu sorgen zur Überwachung des gesamten öffentlichen Raums führen.

7. Grundlage für die Überwachung – Häufungen statt Einzelfälle (§50a)

Die Möglichkeit nach §50a Abs. 3 eine Videoüberwachung zu installieren sind zweifellos zu weit gegriffen. Das z.B. nach einem einmaligen „gefährlichen Angriff“, welcher nach SPG schon z.B. bei einem einfachen Diebstahl vorliegt, für immer und ewig das betroffene Objekt überwacht wird scheint absurd.

Nach dieser Regelung kann man praktisch in jedem Gebäude in Österreich Videoüberwachungsanlagen installieren, da es bestimmt in jedem Gebäudefrüher oder später strafbare Handlungen nach dem StGB vorkommen.

Nimmt man z.B. die Zahlen von 2007 gibt es 500.000 Angezeigte Delikte – Also 500.000 Orten denen eine Videoüberwachung potentiell möglich ist!

Es wäre sinnvoller die Überwachung auf Ort mit ungewöhnlichen Häufungen von Delikten sowie Ort mit besonders hoher Wahrscheinlichkeit für Delikte (z.B. Juweliere, Banken, etc.) zu beschränken.

Bsp.: 1. Ich inszeniere eine Sachbeschädigung welches ich mit einer Anzeige gegen Unbekannt komplettiere. Ich habe §50a Abs. 3 Z 5a erfüllt.

2. Nichteinmahl unsere Minister haben Personenschutz. Da ist es doch absurd, alle „bekannteren“ Personen als potentiell gefährdet zu qualifizieren.

3. In einer Garage steht ein Luxuswagen – Wert über 100.000€

8. Gesetzliche Einschränkung auf den privaten Grund

Ich finde im Gesetz keine Einschränkung, dass die Aufzeichnung nur den privaten Grund umfassen darf. Zum „überwachten Objekt“ gehören vermutlich auch die Außenmauern und folglich auch die Gehsteige/Straßen davor.

Bsp.: Heute finden sich schon vielerorts Kameras welche nicht nur den Gehsteig bzw. die Fassade filmen sondern auch die Kreuzung/Straße davor.

9. Technische Einschränkung der möglichen erfassten Gebiete

Es werden häufig „Dome“-Kameras und bewegliche bzw. zoombare Kameras eingesetzt. Diese müssten um den möglichen Missbrauch einzudämmen technisch so konzipiert sein (Zoom-, Auflösungs- und Winkelbeschränkung) dass nur der erlaubten Bereiche erfasst werden kann. Das müsste auch für Kameras zur reinen Bildübertragung Geltung finden.

Bsp.: Mann erinnere sich an die Kamera mit welcher in die private Wohnung von Angela Merkel gezoomt werden konnte oder die das filmen von Privatwohnungen durch die Polizei am Karlsplatz

10. Verwaltungsstrafbestimmungen (§ 52)

Wenn nicht auch entsprechende Strafen angedroht werden, wird die Bereitschaft Videoüberwachungsanlagen registrieren zu lassen nicht höher werden als bisher.

Weiters wäre es notwendig festzuhalten, dass eine automatische Löschung nach 48h einem Vergehen nach §26 Abs. 7 DSGVO 2000 gleich kommt und damit zu bestrafen ist. Andernfalls würde das Auskunftsrecht einfach durch eine automatische Löschung untergraben werden können.

Auch ist unbedingt zu überlegen, die Zuständigkeit für die Verwaltungsübertretungen bei der DSK statt den Bezirksverwaltungsbehörden zuzuteilen. Es ist fraglich ob diese Behörde immer die nötige Kompetenz haben.

Bsp.: 1. Nach einem Auskunftsbegehren nach §26 DSGVO 2000 werden die Daten einfach nicht ausgehoben, nach 48h bekommt der Betroffene eine „Negativauskunft“.

11. Auskunftsrecht bei Videodaten

Die Datenschutzrichtlinie ermöglicht die Einschränkung des Auskunftsrechts bei einem Interesse Dritter. Die geplante Möglichkeit bei einer Erfassung von mehreren Personen die Bilder nur zu beschreiben ist sinnlos. Ein Betroffener will wissen wie weit der Bildausschnitt geht, ob die Kamera ihm ev. nachgefahren ist, wie die Qualität der Bilder sind etc. - nicht jedoch was er gemacht hat, denn das ist ihm vermutlich bekannt. Aus der DS-RL lässt sich der Grundsatz ableiten immer die Daten selbst zu erhalten und keine Beschreibung der Daten.

Die Lösung muss daher (wie bei Datenbanken) eine Trennung der Daten sein, welche z.B. durch das Unkenntlichmachen der Dritten im Bild möglich wäre. Das Problem wird auch in anderen EU-Staaten (z.B. GB) so gehandhabt.

Außerdem wären wegen der kurzen Zeit bis zur Löschung genaue Fristen wünschenswert (z.B. Dauer bis zum Eingang des Auskunftsbegehrens).

Bsp.: 1. Der Betroffene verlangt Auskunft und teilt aufgrund der Mitwirkungspflicht mit was er getan hat. Antwort: „Sie tun was Sie beschrieben haben, sonst ist nichts zu erkennen“.

2. Der Betroffene erhält keine Auskunft aufgrund von anderen Personen welche auf den Bildern ebenfalls erfasst sind.

12. Beweislastumkehr und Wiederholung bei Auskunftsproblemen

Eine Auskunft kann ganz leicht untergraben werden, indem man a) eine Identifizierbarkeit, b) eine Funktion der Aufnahme, c) die Tatsache, dass aufgenommen wird an sich, d) eine Erfassung des Betroffenen abstreitet.

Für den Betroffenen ist dies nicht zu beweisen. Es bedarf daher einer Regelung wonach der Betreiber dies dem Betroffenen glaubhaft machen muss.

Außerdem sollte in einem solchen Fall eine weitere Auskunft wieder kostenlos sein.

13. Datenweitergabe auf Anfrage der Polizei

Sollte es wie geplant möglich sein, dass die Polizei auf die Videodaten zugreifen kann und von diesen Videoüberwachungen auch öffentlicher Grund erfasst werden (z.B. Straßen, Gehsteige, Plätze, Autobahnen etc.) ist damit der flächendeckenden Videoüberwachung Tür und Tor geöffnet.

Allein im 1. Bezirk in Wien sind weit über 200 Kameras auf öffentlichen Plätzen registriert worden. Damit kann man die Videoüberwachung jetzt schon sicherlich als „flächendeckend“ bezeichnen. Die Anlagen werden nun zweckentfremdet. Personen könnten also weil sie schlichtweg zur falschen Zeit am falschen Ort waren schnell ins Fadenkreuz der Polizei kommen.

Bsp.: Nach einer Auseinandersetzung außerhalb der U-Bahnstation werden die Daten von der Polizei angefordert und 10 verdächtige Personen gesucht. Einer von Ihnen war gerade am Weg zu seiner außerehelichen Partnerin. Er muss sich nun rechtfertigen weil er schlichtweg zur falschen Zeit am falschen Ort war.

14. Regelung für nicht rechtmäßig ermittelte Bilder

Vor allem durch die „Zufalltreffer-Regelung“ des §50a Abs. 5 ist es möglich auch nicht vom Zweck der Anwendung offiziell erfasste Daten zur Anzeige zu verwenden. Das öffnet der eigenmächtigen „Erweiterung“ des Zwecks Tür und Tor.

Auch die Einschränkung der rechtmäßigen Ermittlung ist z.B. in §9 Z9 entfallen. Kann es Sinn des Datenschutzgesetzes sein, dass nicht rechtmäßig ermittelte Daten verwendet werden dürfen anstatt sofort gelöscht werden zu müssen?

Bsp.: Eine Datenanwendung wird aus einem der Gründe des §50a Abs. 3 genehmigt aber in Wirklichkeit zum Zweck anderer Ermittlungen betrieben. Die unrechtmäßig erfassten Daten können verwertet werden.

15. Einschränkung des Personenkreises mit Zugriff auf die Daten

Die Aufzeichnungsgeräte sind oft nicht unter Verschluss oder haben sogar die Möglichkeit des direkten Zugriffs über das Internet (teilweise nicht einmal durch ein Passwort geschützt). Es muss unbedingt festgehalten werden, dass nur ein kleiner, ausgewählter, verantwortungsbewusster Personenkreis Zugriff auf die Daten hat. Außerdem müssen Sicherungsmaßnahmen verpflichtend sein.

Bsp.: Bei den Wiener Linien werden die Daten 1. verschlüsselt aufgezeichnet, und können 2. nur von wenigen, besonders geschulten Mitarbeitern ausgewertet werden. Die Auswertungsplätze sind vom Netzwerk der Wiener Linien getrennt.

16. Formvorschriften bei Eingaben an die DSK

Die Formvorschriften sind viel zu umfangreich und teilweise (z.B. bei mündlicher Auskunftsanfrage) gar nicht einhaltbar. Außerdem machen es diese Vorschriften für die Bürger nahezu unmöglich, eine Beschwerde an die DSK einzubringen.