ÖAW
Österreichische Akademie
der Wissenschaften

INSTITUT FÜR
TECHNIKFOLGEN-
ABSCHÄTZUNG

AKTUELLE DATENSCHUTZ-RECHTLICHE FRAGEN DER VIDEOÜBERWACHUNG

ENDBERICHT

ITA-PROJEKTBERICHT NR. A58
ISSN: 1819-1320
ISSN-ONLINE: 1818-6556

ÖAW
Österreichische Akademie
der Wissenschaften

AKTUELLE DATENSCHUTZ-RECHTLICHE FRAGEN DER VIDEOÜBERWACHUNG

ENDBERICHT

INSTITUT FÜR TECHNIKFOLGEN-ABSCHÄTZUNG
DER ÖSTERREICHISCHEN AKADEMIE DER WISSENSCHAFTEN

Autoren: *Mag. Dr. Walter Peissl*
Ing. Mag. Johann Čas
Dr. Thomas Strohmaier
Robert Rothmann, Bakk. MA

STUDIE IM AUFTRAG DER BUNDESARBEITSKAMMER

WIEN, JÄNNER 2011

IMPRESSUM

Medieninhaber:
Österreichische Akademie der Wissenschaften
Juristische Person öffentlichen Rechts (BGBl 569/1921 idF BGBl I 130/2003)
Dr. Ignaz Seipel-Platz 2, A-1010 Wien

Herausgeber:
Institut für Technikfolgen-Abschätzung (ITA)
Strohgasse 45/5, A-1030 Wien
www.oeaw.ac.at/ita

Die ITA-Projektberichte erscheinen unregelmäßig und dienen der Veröffentlichung der Forschungsergebnisse des Instituts für Technikfolgen-Abschätzung.
Die Berichte erscheinen in geringer Auflage im Druck und werden über das Internetportal „epub.oeaw" der Öffentlichkeit zur Verfügung gestellt:
epub.oeaw.ac.at/ita/ita-projektberichte

ITA-Projektbericht Nr.: A58
ISSN: 1819-1320
ISSN-online: 1818-6556
epub.oeaw.ac.at/ita/ita-projektberichte/d2-2a58.pdf

Inhalt

Abbildung

Zusammenfassung

Videodaten werden alltäglich, aber klare Regeln fehlen

Die Aufzeichnung von Bild- und Videodaten zählt zu jenen Bereichen, bei denen der technische Fortschritt der Informations- und Kommunikationstechnologien am deutlichsten das alltägliche Leben der Menschen prägt. Dies gilt unabhängig davon, ob man selbst mittels Digitalkamera oder Videohandy solche Daten aufnimmt und eventuell über Internetplattformen einem weiteren Personenkreis zur Verfügung stellt, oder ob man als KundIn, PassantIn oder NutzerIn von öffentlichen Verkehrsmitteln passiv von einer der zahllosen Videoüberwachungseinrichtungen erfasst wird. Was weitgehend fehlt, sind klare Regeln und ein Bewusstsein darüber, wie mit dieser Flut an Bilddaten verantwortungsvoll und rechtskonform umzugehen ist.

DSG-Novelle zur Videoüberwachung definiert Verbote und freie Standardüberwachungen

Mit wenigen Ausnahmen bleibt diese Unsicherheit auch nach der Novelle des DSG im Jahr 2010, welche die Videoüberwachung durch Privatpersonen bzw. Unternehmen zu regeln versucht, aufrecht. Zwar gibt es einerseits eindeutige Verbote für den höchstpersönlichen Lebensbereich von Betroffenen, der neben Privatwohnungen noch andere Bereiche umfasst, die die Intimsphäre betreffen wie zum Beispiel Umkleidekabinen oder Toiletteanlagen. Dazu zählt auch das Verbot von Leistungskontrollen von Mitarbeitern mittels Videosystemen. Andererseits wurde eine Reihe von Ausnahmen eingerichtet, in denen eine Videoüberwachung ohne Registrierung bei der Datenschutzkommission zulässig ist. Zu diesen Ausnahmen zählen Banken, Juweliere oder Trafiken, bei denen von einem erhöhten Gefährdungspotenzial ausgegangen wird, sowie Echtzeitüberwachungen – das sind solche ohne Speicherung der Bilddaten – zum Eigenschutz, die als das gelindere Mittel angesehen werden.

Anwendungen ohne Registrierungspflicht müssen eng definiert bleiben

Die von der Registrierungspflicht ausgenommenen Anwendungsfälle tragen zur Rechtssicherheit von Anwendern und auch zur Entlastung der Datenschutzbehörde bei, sie müssen allerdings auch zukünftig auf eng definierte Bereiche beschränkt bleiben, um nicht den Zweck des Datenschutzes zu untergraben. Hinsichtlich der Ausnahme Echtzeitüberwachung sollte überprüft werden, ob dieser Zweck nicht oft bloß als Vorwand dient. Die Registrierungsbefreiung sollte an klar beschränkte technischen Systemeigenschaften gebunden sein, so dass tatsächlich keine Aufzeichnungen möglich sind.

überwiegende Mehrzahl von Videoüberwachungen müssen auf Verhältnismäßigkeit überprüft werden

Da eine Videoüberwachung immer einen Eingriff in die Privatsphäre darstellt und auch sensible Daten generiert, muss für die große Mehrzahl von Videoüberwachungssystemen weiterhin im Einzelfall überprüft werden, ob das jeweilige Überwachungsvorhaben einen berechtigten Zweck verfolgt und verhältnismäßig ist. Hier gilt es sicherzustellen, dass Alternativen, die nicht oder weniger stark in die Privatsphäre eingreifen, auch tatsächlich erwogen und gegebenenfalls realisiert werden. Dazu zählen etwa die in den Erläuterungen erwähnten Sicherheitstüren, Wachpersonal oder der Schutz von Waren mittels an ihnen angebrachter Chips. Um dem in Verfassungsrang stehenden Grundsatz der Verhältnismäßigkeit in der Praxis anwenden und durchsetzen zu können sind zwei weitere Voraussetzungen zu schaffen: Erstens müssen die Antragsteller dazu angehalten werden, die Verhältnismäßigkeit nachzuweisen und unter Umständen auch Mehrkosten für die weniger eingriffsintensive Variante in Kauf nehmen; zweitens sind in der Datenschutzkommission die entsprechenden Ressourcen zu schaffen, um die Einhaltung dieses Grundsatzes auch effektiv prüfen zu können.

Möglichkeiten des technischen Datenschutzes nicht genutzt

Ähnliches gilt für die Anwendung von technischen Vorkehrungen zum Datenschutz. Gemäß dem Stand der Technik müssten bei einer Mehrzahl von Überwachungen die Videoaufzeichnungen generell verschlüsselt werden und nur bei konkreten Vorfällen die Möglichkeit bestehen, auf die unverschlüsselten Aufnahmen zuzugreifen, um vom Einsatz der gelindesten Mittel sprechen zu können. Bislang ist von dieser Möglichkeit, welche die Hinterlegung des Schlüssels bei der Datenschutzkommission vorsieht, noch kein einziges Mal Gebrauch gemacht worden. Moderne Software erlaubt die automatische Verpixelung (Unkenntlichmachung) von personenbezogenen Merkmalen wie Gesichtern oder auch KFZ-Kennzeichen. Diese datenschutzfreundlichen Technologien müssten bei der Beurteilung von neuen Systemen als Mindeststandard vorgesehen werden. Als Unterstützung dabei könnte die externe Beurteilung von IT-Systemen und deren Auszeichnung mit anerkannten Datenschutzgütesiegeln herangezogen werden.

fehlende Ressourcen bei Datenschutzbehörde

Neben klaren Vorgaben bezüglich der Umsetzung des Stands der Technik sind auch hier die entsprechenden personellen und fachlichen Ressourcen in der Datenschutzkommission einzurichten, ergänzt durch die Möglichkeit, selbstständig Prüfungen durchführen zu können, um die datenschutzrechtlichen Vorgaben tatsächlich durchsetzen zu können.

unzureichende Rechte der Betroffenen, …

Eine wichtige Rolle wird dabei auch die Stärkung der Rechte der Betroffenen spielen. Zu diesen gehören eine ausnahmslose – eventuell sogar standardisierte – Kennzeichnungspflicht, eine eindeutige Klärung der Auskunftsrechte bei Videoüberwachungen oder der Schutz vor nicht dem ursprünglichen Zweck entsprechenden Verwendungen von Aufzeichnungen. Hier wäre auch zu diskutieren, inwieweit Beschränkungen und Verbote der gerichtlichen Beweisverwertung sinnvoll und zielführend sind.

… insbesondere bei Bild- und Videodaten außerhalb von Überwachungssystemen

Dem Ausbau und der Stärkung der Rechte von Betroffenen wird auch bei den zahllosen Aufzeichnungen von Bilddaten eine zentrale Rolle zukommen, die nicht auf eine systematische Überwachung abzielen und daher auch nicht von den für Videoüberwachung im engeren Sinn geltenden Bestimmungen des DSG 2000 betroffen sind. Zwar sind auch hier grundsätzlich die allgemeinen Regeln des Datenschutzgesetzes, der allgemeinen Persönlichkeitsrechte, des Medienrechts und des zivilrechtlichen Schutzes am eigenen Bildnis anwendbar, allerdings ist die Durchsetzung dieser Rechte zumeist mit einem unverhältnismäßig hohen Aufwand und Kostenrisiko für den Einzelnen verbunden. Zudem gibt es eine große Grauzone, sowohl hinsichtlich der rechtlichen Beurteilung als auch des Wissens von Betroffenen.

Datenschutz und Persönlichkeitsrechte im Internet kaum durchsetzbar

Ein Beispiel dafür sind Veröffentlichungen von Bildern oder Videos auf Internetplattformen wie YouTube oder in „social networks“ wie Facebook. Derartige Veröffentlichungen werden wohl nicht mehr als private Zwecke gelten können, da diese Daten einem weit größeren Kreis als dem engsten Freundeskreis zugänglich sind. Wirksame Einschränkungen auf den unmittelbaren Freundeskreis können oft nur mit komplexen Änderungen der Default-Einstellungen ermöglicht werden, die zudem häufigen Änderungen der „Privacy Policies“ des Betreibers unterworfen sind. Die Betreiber behalten sich auch das Recht vor, die Daten selbst nach Löschung der betreffenden Mitgliedschaft weiterhin zu speichern und zu nutzen.

Webcams vielfach in Grauzone

In einer Grauzone befinden sich auch viele Webcams im Internet. Je nach Einsatzgebiet können sie harmlose und nützliche Anwendungen darstellen, etwa aus größerer Entfernung getätigte Aufnahmen von Skipisten zur Beurteilung der Wetterbedingungen, oder aber intime Einblicke in persönliches Verhalten offenbaren, etwa Übertragungen aus Veranstaltungslokalen oder Diskotheken. Bei Webcams verschwimmen ebenfalls die Grenzen zwischen Echtzeitübertragung und Aufzeichnung, da grundsätzlich davon ausgegangen

werden muss, dass die Datenströme mitgeschnitten werden können. Dies gilt auch für Videokonferenzen. Diese können wie Telefongespräche jederzeit unbemerkt aufgezeichnet werden.

Datenschutzstrafmandate zur Bewusstseinsbildung?

Neben wirksamen gesetzlichen Regelungen kommt hier der öffentlichen Diskussion und Bewusstseinsbildung eine zentrale Rolle zu. Eine zu diskutierende Variante könnte etwa sein, jede Veröffentlichung an eine ausdrückliche und nachweisbare Zustimmung der Betroffenen zu knüpfen. Ein fehlender Nachweis könnte, analog zu einfachen Übertretungen von Verkehrsbestimmungen, mit Datenschutzstrafmandaten geahndet werden. Ziel solcher Überlegungen sollte sein, ein vereinfachtes Verfahren zur Durchsetzung von Datenschutzregelungen anzubieten, welches weder einen erweiterten Rechtsschutz einschränkt noch Anreize zu einem kommerziell ausgenutzten Mahnunwesen bietet.

Herausforderungen bei StreetView & Co.

Massenhaft Bildmaterial verarbeiten auch kommerzielle geografische Dienste wie Google Street View. Sie stellen spezifische Herausforderung für den Datenschutz dar, so werden Bilder zunächst mit Personenbezug aufgezeichnet und erst später in den USA „verpixelt“, oder von Gebäuden können auch auf Rückschlüsse auf Bewohner und Besitzer gezogen werden. Offen ist dabei vor allem, ob überwiegend berechtigte Interessen für die Veröffentlichung tatsächlich bestehen, ob die Anonymisierung nicht schon bei der Datenermittlung vorgenommen werden müsste, oder ob nicht zumindest die Widerspruchsrechte schon vor der Verbreitung der Bilder im Internet und nicht erst nachträglich ausgeübt werden können.

Stärkung von Persönlichkeitsrechten und mehr Wissen notwendig

Angesichts der rasanten Entwicklung von technischen Möglichkeiten – jeder Gegenstand kann praktisch und unbemerkbar mit Videokameras ausgestattet werden, ein vermeintliches Modellflugzeug eine private Videodrohne darstellen, oder eine Überwachungskamera in einem kleinen Laden weltweit übers Internet zugänglich sein, um den Ladenbesitzer, wie in einem aktuellen Beispiel aus dem Vereinigten Königreich, bei der Überwachung von Kunden zu unterstützen – werden detaillierte Bestimmungen zu allen Möglichkeiten der Aufzeichnung von Bilddaten nicht sinnvoll sein. Hier gilt es eher, einerseits die Durchsetzung von Persönlichkeitsrechten von Betroffenen im Allgemeinen zu erleichtern, andererseits vor allem das Wissen über diese fast uneingeschränkten Möglichkeiten der Generierung und Verbreitung von Bilddaten zu fördern. Besonders problematisch erscheint die Tatsache, dass der leichten Generierung von Bilddaten die fast unmögliche Löschung einmal verbreiteter Daten gegenüber steht. Angesichts der wachsenden technischen Möglichkeiten wird für die Wahrung der Privatsphäre in der Zukunft neben gesetzlichen Regelungen ein verantwortlicher Umgang mit diesen Technologien unverzichtbar sein.

1 Einleitung

DSG-Novelle mit expliziten Regeln zur Videoüberwachung

Mit der im Jänner 2010 in Kraft getretenen Neufassung des Datenschutzgesetzes 2000 wurde die Videoüberwachung durch Private in Österreich erstmals explizit geregelt. Die damit erfolgte Einführung eines eigenen Abschnitts für Videoüberwachung stellt eine Ausdifferenzierung der zuvor oft unpräzisen Rechtslage dar, wobei es u. a. galt, die zunehmend unüberschaubare Anzahl von Neuinstallationen effizienter zu verwalten.[1] Dieser auffällige Anstieg in der Verbreitung technisch-optischer Überwachung von Mensch und Raum wird in der öffentlichen Debatte allgemein mit einer oft nicht näher spezifizierten Verbesserung der Sicherheit begründet. In der einschlägigen kriminologischen Literatur werden die potentiellen Wirkungsformen meist in Abschreckung (Prävention), Unterdrückung (Repression), Aufklärung und die Steigerung des subjektiven Sicherheitsgefühls unterteilt.[2] Der Einsatz von Videoüberwachungstechnologie lässt sich aber gerade durch die verschiedensten privaten Anwendungsbereiche jüngeren Datums nicht mehr nur auf kriminalpräventiv orientierte Sicherheitsaspekte reduzieren. In der technischen und rechtlichen Organisation von Videoüberwachung ist zudem eine sukzessive Vernetzung von öffentlichen und privaten Auftraggebern zu gleichsam hybriden Kooperationen zu erkennen.[3] Die tatsächlichen gesellschaftlichen Folgen der internationalen und über politische Systemgrenzen hinaus zu beobachtenden Ausbreitung von Videoüberwachung sind jedoch ungeachtet des letztlich nach außen getragenen Zwecks weitgehend unklar.[4]

Videoüberwachung ist Eingriff in das Grundrecht auf Privatsphäre

Unbestritten bleibt, dass es sich bei Videoüberwachung um einen Eingriff in die Grundrechte auf Privatsphäre und Datenschutz handelt, weshalb sich weiterhin Fragen nach der Verhältnismäßigkeit und denkbaren absoluten Grenzen für Videoüberwachung stellen. Die Proportionalität lässt sich dabei nur mit gesichertem Wissen über eine tatsächlich nachvollziehbare Erhöhung des Sicherheitsniveaus oder entsprechende Schadensminimierung beurteilen. Der Einsatz bestehender methodischer Instrumente zur Beurteilung der Verhältnismäßigkeit von Überwachungstechnologien könnte in diesem Sinne dabei helfen, Grenzen aufzuzeigen, Einsatzorte und -situationen zu beschreiben und den bestehenden Rechtsrahmen daraufhin auszuloten.

bewusster Umgang mit technischen Möglichkeiten der Überwachung notwendig

Ziel dieser Kurzstudie ist es jedoch nicht die deterministischen Folgen bzw. den so oft beschworenen Zielkonflikt zwischen Sicherheit und Freiheit abschließend zu klären. Worum es geht, ist eine generelle Diskussion zur Überwachungsproblematik anzureißen und unter den veränderten rechtlichen Rahmenbedingungen durch die DSG-Novelle 2010 einen analytischen Blick auf das Thema Videoüberwachung zu werfen, weiterhin offene Punkte des DSG anzusprechen und mögliche Lösungswege aufzuzeigen, um einen bewussten Umgang mit den zunehmenden Interventionen in gesellschaftliche Abläufe mittels technisch-optischer Überwachungssysteme zu ermöglichen.[5]

---

1 vgl. Rothmann 2010.

2 vgl. Eifler & Brandt 2005; Müller 2002; Gras 2005.

3 vgl. Hempel 2007; vgl. Rothmann 2009, 33; vgl. SPG § 53 Abs 5.

4 vgl. Hempel 2007, König 2001.

5 vgl. Peissl 2007.

2 Technische Entwicklungen und Anwendungstrends

2.1 Technische Grundlagen neuer Videoüberwachungssysteme

Digitalisierung, Miniaturisierung und Vernetzung

Technische Entwicklungen im Bereich der Information- und Kommunikationstechnologie sowie der Elektronik zählen zu den wesentlichen Faktoren, welche die Verbreitung von Videoüberwachungssystemen im Allgemeinen und die Integration von Videofunktionen in zahlreiche Geräte und Alltagsgegenstände im Besonderen ermöglichen und beschleunigen. Wie in vielen anderen Bereichen auch sind es vor allem die Digitalisierung der Systeme, deren Miniaturisierung und nicht zuletzt die einfach zu realisierende Vernetzung, die diese Tendenzen begründen. Dies trägt dazu bei, dass Geräte und Systeme, die zum Zweck der Videoüberwachung entwickelt werden bzw. dazu geeignet sind, immer leistungsfähiger und leistbarer werden und daraus folgend von einer steigenden Anzahl von Privatpersonen oder Unternehmen leichter einzusetzen und zu benutzen sind.

mehr Leistung zu sinkenden Kosten

Die Steigerung der Leistungsfähigkeit drückt sich in praktisch allen Eigenschaften und Funktionen aus. Bei den Kameras selbst betrifft dies etwa die Auflösung und Qualität der Aufnahmen, die Einsetzbarkeit bei Dunkelheit, die Möglichkeiten zum Heranzoomen an und zur Verfolgung von Objekten, gepaart mit immer kleineren und weniger Energie verbrauchenden Systemen. Eine ähnliche Entwicklung ist bei digitalen Speichermedien zu beobachten. Immer größere Speicherkapazitäten zu stark sinkenden Preisen je Einheit lassen technische und ökonomische Begrenzungen bei Umfang und Dauer der Speicherung zunehmend an Bedeutung verlieren. Eine digitale Speicherung erlaubt einen schnellen Zugriff auf bestimmte Sequenzen und bietet darüber hinaus wesentlich mehr Möglichkeiten der weiteren Verarbeitung und Analyse des Bildmaterials.

Internetprotokoll vereinfacht Vernetzung

Ein weiterer wesentlicher Faktor, der hier zu nennen ist, betrifft die Vernetzung: Das universelle Internetprotokoll erlaubt die relativ einfache Übertragung von Videodaten zwischen unterschiedlichen Komponenten sowie die standortunabhängige Steuerung von Überwachungssystemen und den Zugriff auf die Daten ohne wesentliche räumliche und zeitliche Beschränkungen. Die drahtlose Vernetzung von Videoüberwachungsanlagen lässt eine wesentlich kostengünstigere Installation von solchen Systemen zu.

technischer Fortschritt verstärkt Trend zu Überwachungstechnologien

Der technische Fortschritt begünstigt hier den breiten Einsatz von Videoüberwachungssystemen und verstärkt somit den bestehenden gesellschaftlichen Trend, jeglichen Sicherheitsproblemen mit Überwachungstechnologien beikommen zu wollen. Er erleichtert auch verdeckte Nutzungsformen von Videoüberwachungen bzw. entzieht diese Technologien durch deren Kleinheit der Aufmerksamkeit der Überwachten; in diesem Sinne sind Hinweistafeln auf Videoüberwachungen oder absichtlich auffällige Systeme auch deshalb so gestaltet, um überhaupt die beabsichtigte präventive Wirkung erzielen zu können.

Informationstechnologien in Alltagsgegenständen

Der Einfluss technischer Entwicklungen beschränkt sich aber nicht auf Videosysteme im klassischen Sinn; er trägt auch dazu bei, immer mehr Alltagsgegenstände mit Fähigkeiten zu Video- und Audioaufnahmen auszustatten. Damit werden auch bestehende definitorische Begrenzungen von Regulierungen in Frage gestellt und neue Probleme aufgeworfen, von denen noch unklar ist, inwieweit sie mit dem vorhandenen Instrumentarium an Regeln und Werten beherrschbar sind.

unmittelbare Veröffentlichung im Internet

Als Beispiel seien hier nur die Videofunktionen genannt, die praktisch schon zur Standardausstattung von Mobiltelefonen gezählt werden können. Damit ist nicht nur ein Schritt in Richtung ubiquitäre Videoüberwachung getan – man kann in fast allen Situationen einer potenziellen Videoaufzeichnung unterworfen sein; mit der weiteren Möglichkeit, diese Videosequenzen unmittelbar ins Internet zu stellen und damit potentiell weltweit zu verbreiten, werden auch die Grenzen von bisherigen Videoaufnahmen zu rein privaten Zwecken durchbrochen.

automatisierte Analyse der aufgezeichneten Daten

Im Bereich von klassischen Videoüberwachungssystemen seien noch zwei weitere technische Entwicklungen genannt, welche einerseits die Verbreitung von Videoüberwachungen begünstigen, andererseits deren Eingriff in die Privatsphäre der erfassten Personen reduzieren können. Der Versuch, die aufgezeichneten Videodaten unmittelbar automatisiert in Hinblick auf „auffälliges Verhalten“ zu analysieren und nur im Alarmfall eine Entscheidung bzw. einen Eingriff durch Überwachungspersonal anzufordern, kann über die Reduktion eines wesentlichen Kostenfaktors die Verbreitung und den Einsatz solcher Systeme beschleunigen und verstärken. Gleichzeitig werden damit neben datenschutzrechtlichen Fragen bezüglich automatisierter Entscheidungen auch ethische Probleme eines Zwangs zu konformen Verhalten angesprochen.

Verschlüsselung als Datenschutzmaßnahme

Die Möglichkeiten der EDV-unterstützen Analyse des Videomaterials lässt sich aber auch in Form einer datenschutzkonformen und privatsphärenfördernden Gestaltung von Videoüberwachungssystemen nutzen. Ein Beispiel wäre hier die automatisierte Unkenntlichmachung und Verschlüsselung von identifizierenden Teilen der Videoaufzeichnung, insbesondere Gesichter oder Kfz-Kennzeichen, wobei die Verschlüsselung sicherstellen soll, dass bei konkretem Bedarf – und nur in diesem Fall – auf die gespeicherten Daten zugegriffen werden kann.

2.2 Beispiele für aktuelle Trends der Nutzung von Videoüberwachungstechnologien

breites Anwendungsspektrum

Die skizzierten technischen Entwicklungen und Innovationen sind die Grundlage für eine rasante Ausdehnung des Anwendungsspektrums von Videoüberwachungssystemen. Von Kameras in Kugelschreibern, Brillen und Feuerzeugen, über Kameras in Bewegungs- und Rauchmeldern bis hin zu Unterwasser- und Nachtsichtkameras – der Einsatzbereich kennt heute auch für Private nahezu keine Grenzen mehr – zumindest in technischer Hinsicht. Rechtlich wurde in Österreich mit der DSG-Novelle 2010 erstmals versucht, einen expliziten Rahmen zur Regelung privater Videoüberwachung zu erlassen, der in Kapitel 1 ausführlich diskutiert wird. Zuvor soll jedoch noch anhand konkreter Anwendungsbeispiele die Breite der (rechtlichen) Probleme illustriert werden, welche mit der leichten Verfügbarkeit und Anwendung von Videoüberwachungstechnologien einhergehen können.

problematische Nutzung von Webcams als Marketinginstrument

Eine häufige privatrechtliche Anwendung von Videotechnologie sind Webcams zum Zweck des Marketing bzw. Kundenservice. So greift beispielsweise eine Restaurantkette in Wien auf Webcams zurück, um interessierten Besuchern auf ihrer Website einen Einblick in das Küchengeschehen ihrer Filialen zu gewähren.[6] Aufgrund der Bildqualität bzw. geringen Auflösung sind zwar

[6] Akakiko Webcams (http://www.akakiko.at/webcams.html).

keine Details zu erkennen, jedoch sind die allgemeinen Arbeitsvorgänge der Küchenmitarbeiter gut einsehbar, was eine derartige Videoüberwachung höchst problematisch macht.[7]

Nebeneffekt Kontrolle von MitarbeiterInnen

Auch eine Elektrofachhandelskette bietet die Möglichkeit, die Kundenfrequenz an diversen Verkaufspulten österreichischer Filialen online einzusehen.[8] Laut Auskunft der IT-Abteilung werden die Bilder der Webcams auf einem Server zwischengespeichert, wobei das Bildmaterial dort drei Sekunden bis zur nächsten Aktualisierung liegt. Die Webcams wurden eigens unscharf gestellt, um die Identifikation von Personen zu erschweren.[9] Dieses Vorgehen entspricht auch den Empfehlungen der Datenschutzkommission,[10] dennoch können einzelne Personen (insbesondere das örtliche Verkaufspersonal) aufgrund von Köperhaltung und Körpersprache erkannt werden, wodurch die Problematik der MitarbeiterInnenkontrolle relevant wird. Die Darstellung der Kundenfrequenz am Verkaufspult hat somit (beabsichtigt oder unbeabsichtigt) eine Überwachung der MitarbeiterInnen und deren Arbeitsweise zur Folge, wobei zudem der tatsächliche Informationsgehalt des Webcam-Services für die Kunden fragwürdig bleibt, da sich selbst im Fall kurzer Anfahrtszeiten zur entsprechende Filiale das aktuelle Geschehen am Verkaufspult bis zum Eintreffen der KundInnen gänzlich wandeln kann.

grundrechtliche Integrität auch bei fürsorglich-pflegerischen Anwendungen gefährdet

Ähnliche Anwendungsfälle von Webcams sind beispielsweise die Möglichkeit zur Einsicht in das Studiogeschehen diverser österreichischer Radiosender.[11] Auch die von der dänischen Psychologin Jørgensen beschriebene Kameraüberwachung in Kindergärten kann hier genannt werden, wonach Firmen wie *WatchMeGrow* und *Kindercam* Eltern in den USA die Möglichkeit bieten, sich zu Hause oder während der Arbeit die Aktivitäten ihrer Kinder in Vorschulen oder Kindergärten „live" anzusehen.[12] Wenngleich der Zugriff auf die Bilder der Webcams mittels Passwort geschützt ist und das angebotene Service somit nicht denselben Öffentlichkeitscharakter wie die oben angeführten Webcam-Anwendungsfälle besitzt, findet neben der digitalen Fürsorge für die Kinder auch hier indirekt eine Überwachung des (pädagogischen) Personals statt. Auf der Website von *WatchMeGrow* wird zudem auf *Senior Care* als ein vergleichbares Service für Seniorenwohnheime verwiesen.[13] Im Zusammenhang mit derartigen Dienstleistungen wird deutlich, dass selbst der positiv besetzte Aspekt von Überwachung, nämlich fürsorglich-pflegerische Aufmerksamkeit, die grundrechtliche Integrität von Menschen beeinträchtigen kann.

Tonaufzeichnungen besonders kritische Zusatzanwendung

Eine weitere Form exotisch-innovativer Videoüberwachungsanwendung stellen sogenannte Türspionkameras dar. Dabei handelt es sich um elektronische Türsicherungssysteme bestehend aus einer Kamera, einem Bewegungssensor, einem Monitor sowie einem Mikrofon.[14] Erkennt der Sensor eine/n BesucherIn oder ein bewegtes Objekt, beginnt die Kamera mit der Aufzeichnung in

---

[7] Da die Leistungskontrolle von Mitarbeitern jedenfalls nicht zulässig ist. Details siehe den rechtlichen Teil in Abschnitt 4.

[8] DITech Webcams (http://www.ditech.at/info/webcam.html).

[9] Angaben beruhen auf einem Telefonat mit DiTech GmbH vom 05.01.2011.

[10] Datenschutzkommission (http://www.dsk.gv.at/site/6301/default.aspx).

[11] Z. B.: Ö3 Livestream & Webcam in das Ö3 Studio (http://www.arminrogl.com/hitradio_oe3/liveradio).

[12] Jørgensen 2005.

[13] WatchMeGrow (http://www.watchmegrow.com/seniorcare.php).

[14] Im Fall der Türspion-Camcorder „IntelliCorder" (PENTAX Europe GmbH) mit 2-fach digitalem Zoom und einem Bewegungsmelderradius von 2 Metern.

Bild und Ton. Das Produkt wird damit beworben, über die normale Funktion eines Türspions hinaus, die Türüberwachung selbst dann zu ermöglichen, wenn man nicht zu Hause ist. Bei Einsatz des Gerätes in einem Mehrparteienwohnhaus könnte dadurch u. a. eine Protokollierung und Archivierung des Geschehens im Hausflur erfolgen, wobei fremde Parteien, die die eigene Wohnungstür passieren müssen, in Bild und Ton miterfasst werden. Im konkreten Fall des Türspion-Camcorders „IntelliCorder" wird in der Informationsbroschüre darüber hinaus (wie in vielen anderen Fällen von Videoüberwachung), mit einer Erhöhung des Sicherheitsgefühls geworben, ein Effekt der in dieser Form vermutlich auch hier keiner Evaluation unterzogen wurde.

fragliche Zwecke und ...

Auch in Diskotheken wird Videotechnologie eingesetzt, um zum Beispiel jede/n BesucherIn beim Betreten ähnlich einem Passfoto systematisch zu fotografieren und damit die persönliche Zuordnung einer Karte für bargeldlosen Zahlungsverkehr zu gewährleisten.[15]

... aufdringliche Anwendungen

Eine Besonderheit stellt die technische Integration von Bild- und Audiodaten dar. Diese werden allerdings mittlerweile nicht mehr „nur" aufgezeichnet, sondern auch in der Gegenrichtung aktiv eingesetzt. Eine Leitlinie des europäischen Datenschutzbeauftragten beschäftigt sich mit „talking CCTV". Durch die Möglichkeit sich auch akustisch in ein Geschehen einzubringen, wird in der Leitlinie aufgrund des „aufdringlichen Charakters" grundsätzlich von einem Verbot ausgegangen. Ausnahmen sind laut Leitlinie schlüssig zu begründen und erfordern eine Folgenabschätzung sowie eine Vorabkontrolle.[16] Auch im Falle des Sicherheitspolizeigesetztes wird gesondert von Bild- und Tonübertragungsgeräten gesprochen, wohingegen im Datenschutzgesetz eine Berücksichtigung der Koppelung von optischer und akustischer Aufzeichnung und Interventionsmöglichkeit unterbleibt.[17]

Echtzeitüberwachung ohne Aufzeichnung technisch sicherstellen

Neuere Videoüberwachungssysteme beinhalten in ihrer Konfiguration meist auch eine Speicherfunktion, bzw. liegt der Unterschied zwischen Echtzeitüberwachung und Speicherung nicht in der generellen Beschaffenheit der Hardware, sondern kann mitunter von einem Mausklick abhängen. Die Meldepflicht bzw. rechtliche Zulässigkeit einer Videoanwendung müsste dementsprechend, um eine allzu leichte Umgehung datenschutzrechtlicher Meldepflichten zu verhindern, von der in Soft- und Hardware festgelegten Möglichkeit zur Speicherung abhängen. Eine strenge Auslegung würde im Umkehrschluss auch privatheitsfördernde – mit weniger Möglichkeiten ausgestattete Systeme bevorzugen. Ähnliches gilt auch für Kameraattrappen. So stellt sich die Frage, ob von einer Attrappe gesprochen werden kann, wenn die gegenständliche Kamera außer Betrieb gesetzt und als solche genutzt wird, aber ohne großen Aufwand die Möglichkeit besteht, sie zu aktivieren.

Beweissicherung auf Vorrat

Weitere Einsatzbereiche von Videotechnologie finden sich in der Automobilindustrie in Form von Park- und Ausfahrtsassistenten, Totwinkel-Überwachung oder automatisierter Verkehrszeichenerkennung, jedoch wird in diesen Fällen laut den Herstellern BMW, Mercedes und Opel keine Speicherung der

---

[15] Beispielsweise in der Wiener Diskothek Praterdome. Laut Angaben der Angestellten werden die Daten nach Verlassen der Veranstaltungsörtlichkeit wieder gelöscht.

[16] „Im Sinne dieser Leitlinien bedeutet „Videoüberwachungskameras mit Lautsprechern („talking CCTV")" eine Videoüberwachungskonfiguration, bei der in dem überwachten Bereich Lautsprecher eingesetzt werden, wobei die Bediener des Systems die beobachteten Bürger „ansprechen" können (z. B. „der Herr in der braunen Lederjacke – heben Sie bitte den Müll, den Sie gerade fallen gelassen haben, wieder auf")."

[17] Eine Funktion, welche in Österreich beispielsweise im U-Bahn Bereich des Verkehrsbetriebs *Wiener Linien* gegeben ist.

Daten z. B. zur Beweissicherung bei Unfällen vorgenommen.[18] Grundsätzlich werden derartige Lösungen aber bereits im branchenspezifischen Elektrofachhandel angeboten.[19]

Untersuchungen der Effektivität als Voraussetzung für Verhältnismäßigkeit fehlen

Die Verhältnismäßigkeit in Form von Eignung, Erforderlichkeit und Notwendigkeit einer Videoüberwachung richtet sich in ihrer Beurteilung nach dem (offiziellen) Zweck der Anwendung. Kann der Zweck nicht erreicht werden, so ist die Anwendung im Sinne der Verhältnismäßigkeit auch nicht geeignet. Derartige Effekte werden in der Regel mit dem methodischen Instrument der Wirkungsevaluation kontrolliert.[20] Ähnlich wie bei Testungen von Medikamenten auf Wirkung oder unerwünschte Nebenwirkung kann in Form von Experimenten oder (im Fall von Videoüberwachung leichter umsetzbaren) quasi-experimentellen Forschungsdesigns die tatsächliche Effektivität und Wirkung einer derartigen Maßnahme mit grundrechtlichem Eingriffscharakter untersucht werden. Für Österreich liegen derartige Evaluationen offiziell jedoch nicht vor.[21] Dies scheint u. a. auch hinsichtlich der erlassenen Standardanwendungen von Bedeutung, welche zukünftige Videoüberwachungen in den betroffenen Bereichen ohne Meldung beim DVR ermöglichen. Dass die kriminologische Effektivität von Videoüberwachungsmaßnahmen nicht als selbstverständlich vorausgesetzt werden kann, zeigen jedoch verschiedene Studien und Metaanalysen auf Basis internationaler Qualitätskriterien.[22] Angesichts dieser Tatsachen entsteht mitunter der Eindruck, dass der Grundsatz der Verhältnismäßigkeit im Kontext der Beurteilung von Videoüberwachungen zu einem theoretisch und formal schönen, in praktischer und funktionaler Hinsicht aber relativ schwachen Rechtsbegriff degradiert wird.

---

[18] Angaben beruhen auf Telefonaten mit den technischen Abteilungen der jeweiligen österreichischen Filialen der Hersteller vom 05.01.2011.

[19] z. B.: http://www.conrad.at/ce/de/product/857547/CARCAMEONE-MIT-SD %20KARTE/SHOP_AREA_17272&promotionareaSearchDetail=005.

[20] vgl. Cook & Campbell 1979; vgl. Sherman et al. 2002.

[21] vgl. Rothmann 2010.

[22] Bornewasser 2005; Bornewasser & Schulz 2007; Gill & Spriggs 2005; Welsh & Farrington 2002, Ditton 2000.

3 Was bedeutet (Video-)Überwachung?

3.1 Politisch-gesellschaftliche Trends

neue Praktiken der sozialen Kontrolle

Neben den technischen Neuerungen sind es vor allem die gesellschaftlich-politischen und sozio-ökonomischen Entwicklungen der post-fordistischen Moderne welche den Einsatz von Videoüberwachung fördern und zu legitimieren scheinen. Die globalisierte und neoliberal (de-)regulierte Marktwirtschaft führt zugleich auch zu einem Abbau wohlfahrtsstaatlicher Inklusions- und Sicherungsmechanismen und einem veränderten Umgang mit Kriminalität und abweichenden Verhalten. Eine ökonomisch geförderte Individualisierung und Pluralisierung von Lebensstilen, und damit einhergehende Normerosion bzw. der Verlust traditioneller Erwartungssicherheiten im täglichen Handeln, begünstigen in weiterer Folge auch die Etablierung neuer Praktiken sozialer Kontrolle. Anstelle von strukturellen gesellschaftlichen Bedingungen wird in der Erklärung abweichenden Verhaltens vermehrt auf individuelle Aspekte abgestellt. Somit steht nicht mehr der Besserungsdiskurs im Sinne von Rehabilitation und Resozialisierung im Zentrum, sondern ein versicherungslogisches Management gesellschaftlicher Randgruppen und räumlicher Situationen. [23]

Ausschließung und Kontrolle

Entsprechend neo-liberaler Orientierungen wird Kriminalität also als persönliches Versagen gesehen, welches im Sinne eines wirtschaftlichen Risikomanagements am besten vorbeugend – bevor Kosten entstehen – erkannt, verhindert und verdrängt werden soll. Gleichzeitig lässt sich auch eine Entpersonalisierung kriminalistischer Strategien feststellen die sich vermehrt als Ausschließung und Kontrolle von Räumen, Orten und Situationen ausdrückt.[24]

„New Surveillance“

Überwachung hat ihr Gesicht verändert, früher diente Überwachung und das Sammeln von personenbezogenen Daten zur Verbrechensbekämpfung, -aufklärung und Strafverfolgung. Daten wurden also insbesondere über jene Personen gesammelt, die einer Straftat verdächtig waren. Heute ist Überwachung alltäglich, routinisiert und sowohl lokal wie auch global – so besehen sind also alle verdächtig. Die „New Surveillance“[25] beobachtet und kategorisiert potentielle (Gruppen von) Unruhestifter(n) nach deren Verhalten und Äußerlichkeiten, um sie präventiv von der Teilhabe am gesellschaftlichen Leben auszuschließen. Somit wird Exklusion zu einem Zweck von Überwachung.

symbolische Politik statt Lösung struktureller Probleme

Die Ökonomisierung vieler Lebensbereiche unterstützt auch die hohe Technikzentriertheit dieser Ansätze. Es ist billiger – jedoch oft nicht effizienter – technische Überwachungssysteme zu installieren statt Präsenz mittels Personal zu zeigen. Aufnehmen, kategorisieren, wegweisen wirkt schneller als strukturelle Probleme in Angriff zu nehmen und zu lösen.[26] Weitere Grundlagen der verstärkt technikorientierten Überwachung finden sich in der Zunahme symbolischer Politik, die medial geschürte Sicherheitsbedürfnisse – das so oft zitierte „subjektive Sicherheitsgefühl“ – schnell zufriedenstellen muss. Überwachung wird vielfach eher als Schutz- und Ordnungsinstrument empfunden denn als Belästigungs- und Bedrohungspotential.[27]

---

[23] Garland 2001; Wehrheim 2002; Peissl 2007; Rothmann 2010.

[24] Peissl 2007; vgl. Wehrheim 2002.

[25] Marx 1998.

[26] Eine umfassende Darstellung zu Fragen der Evaluation von Videoüberwachung siehe Hempel (2007).

[27] Nogala (2000, 141).

3.2 Gesellschaftliche Aspekte von Überwachung

„Social Sorting" und digitale Diskriminierung

Die Folgen breitgefächerter Überwachung können auf mehreren Dimensionen analysiert werden. An erster Stelle steht die Beeinträchtigung der Privatsphäre, die Bedrohung von Grundrechten freier BürgerInnen. Diese sollen u. a. durch das DSG2000 abgefedert werden (siehe dazu Kapitel 4). Eine weitere, meist mittel- bis langfristig wirksame Entwicklung ist das so genannte Social Sorting. Darunter versteht man die Tendenz Menschen nach ihrem Verhalten und anderen äußerlich wahrnehmbaren Merkmalen zu kategorisieren, zu bewerten und in Risikoklassen einzuteilen. Die Folgen des Kategorisierens, des Wert- und Risikozuschreibens an Personen sind oft nicht sofort offensichtlich und dennoch gesellschaftlich relevant. Es geht um die Beeinträchtigung von realen Lebenschancen aufgrund virtueller Merkmalszuschreibungen, um soziale Gerechtigkeit und digitale Diskriminierung. In diesem Zusammenhang kommt insbesondere der De-Kontextualisierung große Bedeutung zu. Digitale Aufnahmen, Merkmale – seien dies nun Einträge in Datenbanken oder auch Bildaufzeichnungen – können niemals den gesamten Kontext der Handlungen und schon gar nicht die dahinter stehende Motivation vermitteln. Damit besteht die große Gefahr, dass „objektiv" erhobene Tatbestände anders („dem Augenschein nach") ausgelegt werden, und es so zu falschen Zuordnungen und damit oft auch nachteiligen Konsequenzen für die Betroffenen kommt.

„Mainstreaming" und Konformismus

Eine weitere langfristig relevante Auswirkung zunehmender Überwachung liegt im so genannten Mainstreaming – dem subtilen Zwang zum Konformismus. Zweck von Überwachung und Kontrolle ist ja die Reduzierung von deviantem Verhalten. In den Sozial- und Wirtschaftswissenschaften ist aber weitgehend unbestritten, dass sozialer Wandel und auch ökonomische Entwicklung in Konformität nicht möglich sind. Wird nun der Geist des Wandels ausgemerzt, durch flächendeckende Überwachung verunmöglicht, wird gesellschaftliche Entwicklung gehemmt.[28]

Verlust von persönlicher Autonomie

Nicht zuletzt soll auch in diesem Zusammenhang auf ein grundsätzliches Problem hingewiesen werden, das sehr eng mit der Entwicklung des Grundrechts auf Privatsphäre zusammenhängt. In Folge des Bewusstseins flächendeckender Überwachung kann es zu einem Verlust an Autonomie, an persönlicher Freiheit kommen, der langfristig ein demokratiepolitisches Problem entstehen lässt.[29]

---

[28] vgl. Peissl (2005, 86f).

[29] vgl. dazu das Weg weisende Urteil des BGH zur Volkszählung 1983 in dem dieser festhält:
„Individuelle Selbstbestimmung setzt aber – auch unter den Bedingungen moderner Informationsverarbeitungstechnologien – voraus, daß dem Einzelnen Entscheidungsfreiheit über vorzunehmende oder zu unterlassende Handlungen einschließlich der Möglichkeit gegeben ist, sich auch entsprechend dieser Entscheidung tatsächlich zu verhalten ... Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. Wer damit rechnet, daß etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und daß ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten. Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist." (BVerfGE, 42f)

überzogene Erwartung hinsichtlich der Wirksamkeit

Wirkt Überwachung überhaupt? – Nein, in Bezug auf die überzogenen Erwartungen, die in sie gesetzt werden. Ja, wenn man bestimmte Delikttypen und besondere räumliche Gegebenheiten berücksichtigt. Studien zeigen[30], dass Überwachung dort am besten wirkt, wo sie räumlich stark begrenzte Territorien flächendeckend überwacht: in Tiefgaragen und auf Parkplätzen. Abschreckende Wirkung kommt ihr jedenfalls – wenn überhaupt – nur bei geplanten Taten zu und keineswegs bei Affekttaten oder gar ideologisch motivierten Attentaten. Während der Autoeinbrecher oder Supermarktdieb sich zumindest vergewissert, nur im toten Winkel der Kameras zu agieren, lässt sich ein ideologisch motivierter Selbstmordattentäter durch mögliche Kamerapräsenz sicher nicht von seiner Tat abbringen.

3.3 Vertrauen der ÖsterreicherInnen in den Datenschutz

Informationsdefizite bezüglich Datenschutz

Eine Erhebung der Firma Oekonsult zum Thema „Das Vertrauen der ÖsterreicherInnen in den Datenschutz“ zeigt, dass ein überwiegender Teil der Befragten hierzulande mit einem gewissen Unbehagen an Dinge wie den Schutz der persönlichen Daten und der Privatsphäre denkt, weil sie das unbestimmte Gefühl haben, dass das etwas sei, das außerhalb ihrer Kontrolle läge und das keinen angemessenen Schutz erfahre. Das führt aber kaum dazu, dass die Datenschutzdiskussion im Alltag stattfindet, oder sich viele BürgerInnen damit auseinandersetzten. Wobei man festhalten muss, dass sich viele schlecht informiert fühlen, nicht wissen, wo sie die relevanten Informationen bekämen, und sich wünschen, dass dieses Informationsdefizit durch geeignete Maßnahmen ausgeglichen wird.[31]

wenig Wissen über mögliche Konsequenzen für die eigene Person

Eine Studie, die das Verhalten von StudentInnen, die Web 2.0-Plattformen nutzen, und deren Wissen über Datenschutz beziehungsweise Möglichkeiten der informationellen Selbstbestimmung untersucht hat, kommt unter anderem zu dem Ergebnis, dass viele vermuten, dass ihre Daten dort zu lange gespeichert werden, für Werbezwecke ausgewertet werden etc., diese Vermutung an ihrem Verhalten aber nur wenig ändert. Mögliche Ursachen dafür sind vor allem ein Gewöhnungseffekt, der eintritt, wenn trotz dieser Datenschutzverletzungen keine unmittelbaren negativen Konsequenzen für die eigene Person festzustellen sind, und die Tatsache, dass das Thema in der Öffentlichkeit nicht breit genug diskutiert wird, um das Problem als wirkliche Bedrohung zu empfinden.[32]

---

[30] vgl. Töpfer (2007, 36); Gill& Spriggs (2005), Bornewasser (2005, 2007), Wesh & Farrington (2002) Ditton (2000).

[31] Allwinger Kristin/Joshi M.A. Schillhab (2008): Vertrauen der ÖsterreicherInnen in den Datenschutz, Juli 2008, http://www.oekonsult.eu/datensicherheit2008.pdf.

[32] Fuchs, Christian (2009): Social Networking Sites and the Surveillance Society. A Critical Case Study of the Usage of studiVZ, Facebook an MySpace by Students in Salzburg in the Context of Electronic Surveillance, http://fuchs.icts.sbg.ac.at/SNS_Surveillance_Fuchs.pdf.

fehlendes Datenschutzbewusstsein

Diese Tendenzen werden auch ganz deutlich von der Eurobarometer Umfrage Nummer 225 vom Februar 2008 zum Thema „Datenschutz in der Europäischen Union aus Sicht der BürgerInnen“ bestätigt. So würden beispielsweise 69 % der ÖsterreicherInnen der Aussage zustimmen, dass das Datenschutzbewusstsein der BürgerInnen in Österreich niedrig sei.[33]

unkritische Haltung zur Videoüberwachung

Auch das von Hempel und Töpfer koordinierte „Urban Eye“ Projekt, im Zuge dessen in Wien 200 Passanten auf verschiedenen allgemein zugänglichen Örtlichkeiten in der Nähe von Einkaufszentren und Stationen des öffentlichen Verkehrs befragt wurden, zeigt auf, dass lediglich 35,5 % der Befragten der Aussage „Kameras dringen in die Privatsphäre ein“ zustimmen.[34] Ähnliche Zahlen liefert auch eine Studie, welche etwas mehr als 300 Personen in der Wiener Innenstadt befragte. So pflichten nur rund 46 % der Aussage „Videoüberwachung ist ein Eingriff in meine Privatsphäre“ bei, wobei sich zeigt, dass männliche und jüngere Passanten tendenziell kritischer eingestellt sind.[35]

---

[33] The Gallup Organization (2008): Flash Eurobarometer Series #225: Data Protection in the European Union – Citizens' Perceptions, http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf.

[34] Hempel & Töpfer 2004.

[35] Rothmann 2009.

4 Aktuelle datenschutzrechtliche Fragen der Videoüberwachung

4.1 Allgemeines

explizite Regelung der Videoüberwachung seit Beginn 2010

Seit 01.01.2010 ist die Videoüberwachung durch Private in Österreich erstmals gesetzlich geregelt, und zwar in einem eigenen Abschnitt 9a des Datenschutzgesetzes 2000 (DSG 2000).[36] Neu ist, dass es nunmehr eine ausdrückliche gesetzliche Regelung gibt; nicht neu ist, dass die Videoüberwachung auch schon vor Inkrafttreten dieser Regelungen dem Regime des Datenschutzgesetzes unterworfen war. Gerade aber die in der Praxis aufgetretenen Vollzugsprobleme bei den „*aus dem Alltag fast nicht mehr wegzudenkenden*" Videoüberwachungen waren einer der Hauptgründe für die erste umfassende Novellierung des DSG 2000 durch die Datenschutznovelle 2010.[37]

datenschutzrechtlich relevantem Trend Rechnung getragen

Hier haben insbesondere die Datenschutzkommission (DSK) und das Datenverarbeitungsregister (DVR) Pionierarbeit geleistet: diese haben bereits im Datenschutzbericht 2005 – 2007 die *Registrierung von Videoüberwachungen* als „Datenschutzrechtlich bedeutsamen Trend"[38] ausgemacht (zum damaligen Zeitpunkt lagen etwa 300 Meldungen vor, von denen erst ein kleiner Teil auch registriert war) und in einem eigenen Anhang Leitlinien für die Registrierung von Videoüberwachungen entwickelt. Diese datenschutzrechtlichen Klarstellungen der zuständigen Behörden und der dazu ergangenen Rechtsprechung der DSK haben wohl dazu beigetragen, dass gem. dem nun vorliegenden „Datenschutzbericht 2009"[39] allein im zweiten Halbjahr 2008 „hunderte Meldungen von Banken zur Videoüberwachung"[40] beim DVR einlangten. Nicht zuletzt findet sich im Anhang auch des aktuellen Datenschutzberichtes ein ausschließlich der Videoüberwachung gewidmeter „Erfahrungsbericht über Videoüberwachung"; ein deutlicher Hinweis auf die Notwendigkeit, hier gesetzliche Vorkehrungen zu treffen, wie dies nun in der ersten umfassenden Novelle des DSG 2000 seit seinem Inkrafttreten am 01.01.2000, der DSG-Novelle 2010, geschehen ist.

---

[36] BGBl. I Nr. 133/2009, kundgemacht am 30.12.2009.

[37] siehe dazu insbesondere den Allgemeinen Teil der Erläuterungen in 472 der Beilagen XXIV. GP – Regierungsvorlage (http://www.parlament.gv.at/PAKT/VHG/XXIV/I/I_00472/fname_172230.pdf); neben der fehlenden rechtlichen Grundlage für die Videoüberwachung war auch das dem DSG 2000 zugrundeliegende Konzept der klassischen Datenbanken nicht wirklich anwendbar.

[38] siehe http://www.dsk.gv.at/DocView.axd?CobId=30637; nicht zu verwechseln mit dem „Trend", Videoüberwachung einzusetzen, auf deren Regelungsbedarf bspw. die ARTIKEL 29 – Datenschutzgruppe bereits in ihrem am 25.02.2002 angenommenen Working Paper Nr. 67 („Verarbeitung personenbezogener Daten aus der Videoüberwachung", http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2002/wp67_de.pdf) aufmerksam gemacht hat, wonach „... in den vergangenen Jahren in Europa von öffentlichen und privaten Einrichtungen immer häufiger Bildaufzeichnungssysteme (Videorecorder) eingesetzt ..." würden.

[39] deckt den Zeitraum 01.07.2007 bis 31.12.2009 http://www.dsk.gv.at/DocView.axd?CobId=40344.

[40] Seite 53 des Datenschutzberichts 2009 http://www.dsk.gv.at/DocView.axd?CobId=40344.

auch Persönlichkeitsrechte oder Arbeitsrecht betroffen

Nicht vergessen werden darf aber, dass die Zulässigkeit einer Videoüberwachung (als eine von vielen möglichen Bedrohungen der Privatsphäre) nicht nur speziell im Bereich „Datenschutz" eine Rolle spielt, sondern immer (auch) an den durch die Rechtsordnung geschützten jedermann zustehenden Persönlichkeitsrechten auf Achtung des Privatbereichs und der Geheimsphäre[41]zu messen sind; hier hat sich der Oberste Gerichtshof bereits wiederholt mit Fragen zur Zulässigkeit von Videoüberwachungen Privater auseinandergesetzt[42] und bspw. klar ausgesprochen, dass eine systematische, verdeckte, identifizierende Videoüberwachung mit abrufbarer Bildaufzeichnung immer einen Eingriff in das gemäß § 16 ABGB iVm Art 8 EMRK geschützte Recht auf Achtung der Geheimsphäre darstellt. Nicht zu vergessen im Zusammenhang mit Videoüberwachung sind auch arbeitsverfassungsrechtliche Bestimmungen, die dafür bspw. zwingend eine Betriebsvereinbarung vorsehen können.[43]

Folgewirkungen und offene Fragen im Mittelpunkt

Die folgenden Ausführungen dienen weniger der detaillierten Gesamtdarstellung der neuen Regelungen zur Videoüberwachung[44] als vielmehr der Untersuchung ihrer rechtlichen Folgewirkungen, Schwachstellen sowie der weiterhin offenen Regelungsbereiche und wie diese „geschlossen" werden könnten.

4.2 Was ist (k)eine Videoüberwachung aus Sicht des Datenschutzes?

Videoüberwachung: systematisch und fortlaufend

Videoüberwachung ist „*... die systematische, insbesondere fortlaufende Feststellung von Ereignissen, die ein bestimmtes Objekt (überwachtes Objekt) oder eine bestimmte Person (überwachte Person) betreffen, durch technische Bildaufnahme- oder Bildübertragungsgeräte*." Immer wenn dabei Personen zu sehen sind, fallen personenbezogene Daten an. Damit dem „Personenbezug" genüge getan wird, müssen diese Personen zumindest (für irgendjemanden) *identifizierbar* sein. Erläuternd wird in der Regierungsvorlage ausgeführt, dass bspw. Aufnahmen aus rein touristischen oder künstlerischen Beweggründen, aber auch Filmen für ausschließlich familiäre oder persönliche Tätigkeiten (bspw. Kindergeburtstag, aber auch Bildüberwachung von Babys) nicht darunter fallen sollen; sehr wohl aber auch gezieltes Fotografieren[45] und die Überwachung von Einfamilienhäusern und dazu gehöriger Grundstücke.

---

[41] insbesondere § 16 ABGB und Art. 8 EMRK; nicht ohne Grund regelt § 50a Abs 2 DSG 2000: „*Persönlichkeitsrechte nach § 16 ABGB bleiben unberührt.*"

[42] OGH, Urteil vom 19.12.2005, 8 Ob 108/05y („Systematische Videoüberwachung zur Beweissammlung") und OGH, Urteil vom 28.03.2007, 6 Ob 6/06k („Überwachungskamera-Attrappe").

[43] bspw. § 96 a Abs 1 Zif 3 ArbVG, wobei, wobei die Zustimmungsrechte des Betriebsrates von den Regelungen des DSG ohnehin unberührt bleiben.

[44] das haben bereits andere ausführlich getan: siehe u. a. *Jahnel*, Die DSG-Novelle 2010 im Überblick, jusIT 1/2010, 12ff und *Ennöckl*, Die DSG-Novelle 2010, ÖJZ 2010/35, 293ff.

[45] ... was bspw. für Berufsdetektive in vielen Fällen von Bedeutung sein wird. Auch andere Berufsgruppen haben hier Bedenken: bspw. der Österreichische Journalistenclub in seiner Stellungnahme zur DSG-Novelle 2010 vom 17.06.2009 (http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00062_40/fname_161638.pdf), der die freie Bildberichterstattung über längere Zeiträume (zum Beispiel: Baustellenskandale oder Recherchen über Umweltsünden) gefährdet sieht und eine Ausnahmebestimmung für Journalisten und Bildberichterstatter fordert (die es m.E. aber schon seit 01.01.2000 in Form des § 48 DSG 2000 gibt).

Videos zu Privatzwecken bzw. deren Veröffentlichung geregelt ...

„Videos zu Privatzwecken“ sind nach der eng gefassten Bestimmung des § 45 DSG 2000 zu beurteilen: diese erlaubt die Verarbeitung durch **natürliche Personen**[46] ausschließlich zum Zweck „persönliche oder familiäre Tätigkeiten“, wenn diese Daten vom Betroffenen *selbst mitgeteilt* wurden oder sonst rechtmäßig zugekommen sind.[47] Davon wäre bspw. auch eine ausschließlich zu diesen Zwecken eingerichtete Homepage umfasst, sofern diese ausschließlich die **eigenen** Daten enthält; werden dort jedoch auch Daten **Dritter** veröffentlicht (bspw. ein Kindergeburtstagsvideo auf Facebook oder YouTube), liegt keine private Tätigkeit mehr vor[48], da diese Art der „Veröffentlichung“ (iS. von Zugänglichmachung für Dritte) jedenfalls gem. § 45 Abs 2 DSG 2000 zwingend die Zustimmung des Betroffenen voraussetzt.[49] Bei einer solchen Veröffentlichung wäre darüber hinaus – die Anwendbarkeit des DSG 2000 vorausgesetzt – derjenige, der solche Videos auf den genannten Plattformen bereitstellt, datenschutzrechtlicher „Auftraggeber“[50] und müsste diese Datenanwendungen ua. ordnungsgemäß bei der DSK/dem DVR melden.

... aber fehlendes Datenschutzbewusstsein bei den AnwenderInnen

4.3 Wer darf videoüberwachen?

hoheitliche Videoüberwachungen bedürfen eigener Rechtsgrundlage

Regelungsinhalt der DSG-Novelle 2010 ist die Videoüberwachung durch „Private“, d. h. für privatrechtlich handelnde natürliche oder juristische Personen, einschließlich der Privatwirtschaftsverwaltung öffentlicher Auftraggeber. Die Erläuterungen in der Regierungsvorlage sprechen gar von der *Anerkennung der Videoüberwachung als Mittel der Gefahrenabwehr durch Private.*[51] Die Novelle enthält keine ausdrücklichen Regelungen für „hoheitliche“ Videoüberwachungen (gemeint: in Vollziehung hoheitlicher Aufgaben), sodass eine solche auch nicht auf das DSG 2000 gestützt werden kann; diese bedarf vielmehr einer gesonderten Rechtsgrundlage.[52]

---

[46] somit bspw. nicht auch für Vereine oder sonstige Gesellschaftsformen.

[47] Diese Form der „Videoüberwachung“ ist gem. § 17 Abs 2 Zif 4 DSG 2000 auch von der Meldepflicht ausgenommen. Siehe dazu die Erläuterungen zur DSG-Novelle 2010 zu § 50a Abs 1, wonach – entgegen dem Judikat K600.064-001/0002-DVR/2009 der DSK vom 08.05.2009 – davon auszugehen sei, dass die Überwachung von Einfamilienhäusern und dazu gehörigen Grundstücken nicht umfasst und überdies neben potentiellen Einbrechern auch andere Personen (Besucher, Hausangestellte wie etwa Reinigungspersonal) davon betroffen sein können. Derartige Datenanwendungen fallen daher unter § 50a DSG 2000.

[48] Dieses Beispiel findet sich in *Jahnel*, Handbuch Datenschutzrecht, 2010, Rz 8/4.

[49] siehe dazu auch die Stellungnahme der DSK zur DSG-Novelle 2010 (http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00062_57/imfname_164857.pdf): „*Zu überdenken wäre auch, inwieweit der Ausschluss der Anwendbarkeit des DSG 2000 auf „Datenverwendung für private Zwecke“ in § 45 DSG 2000 auch für das Internet gelten soll: Gerade in „Freundschaftsnetzwerken“ können gravierende Datenschutzprobleme durch die Publikation von Daten über „Freunde“ entstehen*“.“

[50] siehe dazu *Leissler*, Social Networks – Datenschutz in der vernetzten Welt, ecolex 10/2010, 834ff, der die Kombination von Social Networks und dem österreichischen Datenschutzrecht treffend als „explosive Kombination“ bezeichnet.

[51] RV 472 BlgnNr 24. GP 18.

[52] siehe die Übersicht in *Robert König*, Videoüberwachung, Fakten, Rechtslage und Ethik, 127ff, der u. a. die Bestimmungen der §§ 149d ff Strafprozessordnung (StPO (kleiner Lausch- bzw. Spähangriff)) sowie § 20 Militärbefugnisgesetz (MBG) und § 54 Sicherheitspolizeigesetz (SPG) näher ausführt.

4.4 Was und zu welchem Zweck darf überwacht und geschützt werden … und was jedenfalls nicht.

4.4.1 Zweckbindung

Schutzzwecke als Ausgangspunkt

Während im Datenschutzbericht 2005 – 2007 die Videoüberwachung noch an die Überwachung einer „Örtlichkeit" und der darüber bestehenden Verfügungsgewalt (insbesondere das „Hausrecht") anknüpfte, geht die DSG-Novelle 2010 nunmehr vom Schutz des überwachten *Objekts* und der überwachten *Person* aus.[53]

nur „Eigenschutz" und ...

Objekte und Personen lassen sich aber zu vielerlei Zwecken schützen; als rechtmäßige Zwecke einer Videoüberwachung kommen aber ausschließlich nur zwei[54] in Frage: der „Eigenschutz", d. h. der Schutz der Person und des Eigentums des Auftraggebers, worunter auch der Schutz seiner Organe (Organwalter), also seiner Mitarbeiter etc. fällt.[55]

… „Verantwortungsschutz" zulässige Zwecke

Der zweite zulässige Zweck einer Videoüberwachung ist die Erfüllung rechtlicher Sorgfaltspflichten, im Datenschutzbericht 2005 – 2007 einprägsam als „Verantwortungsschutz" bezeichnet;[56] davon umfasst sind jene Fälle, in welchen der Auftraggeber den Schutz von Personen aus dem Titel der Verkehrssicherungspflicht oder aus vorvertraglichen Verpflichtungen und dergleichen vorzusorgen hat; bspw. die Videoüberwachung in einer Bankfiliale, die damit auch ihre Kunden (mit denen sie in einem Vertragsverhältnis steht bzw. für die die Bank bereits beim Betreten der Filiale Verkehrssicherungspflichten treffen) schützt. Der Zweck „Verantwortungsschutz" wurde in zahlreichen Stellungnahmen zur DSG-Novelle 2010[57] unter Hinweis darauf kritisiert, dass damit der Auftraggeber selbst „Verpflichtungen" und damit die Rechtsgrundlage für eine Videoüberwachung schaffen könne. Diese Bedenken werden m.E. insbesondere durch den Verweis auf die Geltung der §§ 6 und 7 DSG 2000 in § 50a Abs 2 DSG 2000 entschärft, wonach Daten nur soweit verarbeitet werden dürfen, als dies von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt ist; es hat sich damit um rechtlich anerkannte Sorgfaltspflichten zu handeln.[58]

---

[53] wobei *Ennöckl*, Die DSG-Novelle 2010, ÖJZ 2010/35, 293ff, auch hier zutreffend darauf verweist, dass die rechtliche Befugnis eines Privaten zur Vornahme einer „Videoüberwachung" ein privatrechtliches Rechtsverhältnis zum überwachten Objekt (Eigentümer, Mieter) oder zur überwachten Person (z. B. Sorgfaltspflicht) voraussetzt.

[54] Filmen für ausschließlich familiäre oder persönliche Tätigkeiten soll gem. den Erläuterungen nicht als „Videoüberwachung" gelten (siehe oben 4.2) und ist somit kein weiterer „Zweck"

[55] siehe dazu auch den Datenschutzbericht 2005 – 2007 (http://www.dsk.gv.at/DocView.axd?CobId=30637), S 68.

[56] siehe ebendort S. 68.

[57] U. a. vom Ludwig Boltzmann Institut für Menschenrechte (BIM) vom 17.06.2010 (http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00062_39/imfname_161639.pdf).

[58] Zwar ohne Anspruch auf allgemeine Gültigkeit, aber doch um beispielhaft die gesetzlichen Zuständigkeiten und rechtlichen Befugnisse des Arbeit-/Auftraggebers im Bereich des kollektiven Arbeitsrechts zu erwähnen: siehe die Erläuterungen zum Initiativantrag der ArbVG-Novelle 1986 (205/A – II 4371 Blg NR XVI. GP): „*Der Arbeitsvertrag darf allerdings nicht dazu verwendet werden, in Umgehungsabsicht durch Aufnahme von Vertragsbestimmungen die Verpflichtung des Betriebsinhabers zu konstruieren, Daten zu ermitteln, zu verarbeiten oder zu übermitteln, die für die Erfüllung des Arbeitsvertrages nicht erforderlich sind.*"

Webcams für Werbezwecke?

Die – durchaus wünschenswerte – Verengung der zulässigen Verwendungszwecke von Videoüberwachungen hat bspw. zur Folge, dass Videoüberwachungen zu Werbezwecken (Wetterkamera) mangels Rechtsgrundlage unzulässig bzw. einzustellen sind;[59] genau genommen handelt es sich hier um eine *Datenübermittlung an die Öffentlichkeit* und keine Videoüberwachung iS. des DSG 2000, da diese „Überwachung" weder zu Zwecken des Eigen- noch des Verantwortungsschutzes erfolgt. Auch das (Mit-)Filmen einer universitären Vorlesung **ohne Zustimmung** der vortragenden Person für Zwecke des „Selbststudiums" (gemeint: ausschließlich für den Filmenden) fiele nicht unter die beiden erwähnten „Zwecke"; hier könnte zwar die oben in Punkt 4.2 erwähnte Verwendung zu *privaten* Zwecken weiterhelfen,[60] doch kommen hier zusätzlich die umfassenden Persönlichkeitsrechte des § 16 ABGB ins Spiel:[61] demnach kann nach hL eine unbefugte Bildaufnahme ein Eingriff in das Recht auf Wahrung der Geheimsphäre sein. Da auch strittig ist, inwieweit an einem privat gesprochenen Wort bzw. an der eigenen Stimme ein Persönlichkeitsrecht auf der Grundlage des § 16 ABGB anzunehmen ist,[62] empfiehlt sich jedenfalls die Einholung der vorherigen Zustimmung der vortragenden Person.

Beweissicherung

Als Annex zu den beiden Zwecken des Eigen- und Verantwortungsschutzes gesellt sich schließlich noch die *Beweissicherung*, d. h. die Sicherung der zu diesen Zwecken ermittelten Videoaufnahmen, um diese als „Beweis" (für den Diebstahl eines Kunstgegenstandes im Museum („Eigenschutz") bzw. für die Ausforschung des Taschendiebes, der einem Kunst liebenden Besucher des Museums die Geldbörse entführt hat („Verantwortungsschutz")) verwenden zu können.

4.4.2 Schutzwürdige Geheimhaltungsinteressen ohne Interessenabwägung

schutzwürdige Geheimhaltungsinteressen dürfen nicht verletzt werden

Ist erst einmal die Hürde des zulässigen Zweckes genommen, bedarf es als weiterer Zulässigkeitsvoraussetzung, dass keine *schutzwürdigen Geheimhaltungsinteressen* Betroffener verletzt werden. Diese fehlen nach Ansicht des Gesetzgebers (weshalb es keiner *Interessenabwägung* mit dem Interesse des Auftraggebers an der Videoüberwachung bedarf), wenn: (i) die Datenverwendung im lebenswichtigen Interesse *einer* Person erfolgt und (ii) bei ausdrücklicher (da Videodaten potentiell „sensibel" sind) Zustimmung der betroffenen Person.

---

[59] wie dies zutreffend (und mit einem Schuss Ironie) *Dörfler*, Tatort Bergstation, ecolex 2010, 301, für Werbezwecken dienende Wetterkameras konstatiert hat, die neben dem Wetter auch die Auslastung der Pisten mitfilmen (d. h. die dort die Piste hinunterwedelnden Personen und sonstigen Pistenteilnehmer). Die DSK empfiehlt (konkret in Zusammenhang mit „Webcams") die technische Auflösung der Videoanlage so zu wählen, dass die Erkennbarkeit von Personen erst gar nicht gegeben ist (http://www.dsk.gv.at/site/6301/default.aspx).

[60] wobei schon fraglich ist, ob die „Daten" dem Filmenden vom Betroffenen wirklich *selbst mitgeteilt* wurden bzw. ob „Studien-" und „Privatzwecke" ident sind.

[61] dies gleich als Hinweis, dass für die Zulässigkeit einer Videoüberwachung neben den Regelung des DSG 2000 auch die *Persönlichkeitsrechte gem. § 16 ABGB zu berücksichtigen sind.*

[62] siehe *Schwimann*, AGBG Praxiskommentar, Teil I, Rz 29 und Rz 35 zu § 16 ABGB; auf das Recht am eigenen Bild gem. § 78 UrhG wurde hier nicht eingegangen, da diese Bestimmung nur gegen die Veröffentlichung von Bildnissen, nicht aber vor der Aufnahme eines Bildes schützt.

problematische Definitionen: lebenswichtige Interessen ...

Die auf den ersten Blick vertraute Variante „lebenswichtige Interessen“[63] ist im Zusammenhang mit Videoüberwachung nicht wirklich geglückt und wurde zurecht kritisiert: das Abstellen auf das lebenswichtige Interesse bloß *einer* Person würde die Videoüberwachung bspw. auch aller anderen Patienten einer psychiatrischen Abteilung rechtlich zulässig machen (und deren schutzwürdige Geheimhaltungsinteressen beseitigen), selbst wenn diese Überwachung nur im lebenswichtigen Interesse einer einzelnen Person erfolgt.[64] Zutreffend wurde darauf hingewiesen, dass dieses lebenswichtige Interesse ausschließlich auf den überwachten Patienten oder Bewohner eingeschränkt werden müsste; ebenso zutreffend wurde auf den sonst vorliegenden Widerspruch zur Verfassungsbestimmung des § 1 Abs 2 DSG 2000 aufmerksam gemacht.[65]

... auf öffentliche Wahrnehmung gerichtetes Verhalten

Dazu reiht sich hier aber ein m.E. durchaus problematischer weiterer Zulässigkeitstatbestand, nämlich (iii) die *Verarbeitung*[66] von Daten über ein Verhalten,“*... das **ohne jeden Zweifel** den Schluss zulässt, dass es darauf gerichtet war, öffentlich wahrgenommen zu werden, ...*“.[67]

unterschiedliche „Öffentlichkeiten“

Schon die in den Erläuterungen gegebenen Beispiele können schwer überzeugen, etwa wenn dort „Straßenkunst“ oder Auftritte im Rahmen von Veranstaltungen genannt werden: Ist dem Puppenspieler in der Wiener Kärntnerstraße wirklich bewusst, ob und wie viele Kameras ihm bei seinem Auftritt „zusehen“? ... immerhin gehen die Erläuterungen davon aus, dass ein solches Handeln einer „Zustimmung gleichzuhalten“ wäre.[68] Und umfasst die unbestritten von ihm gewählte „Öffentlichkeit“ nicht eher die Passanten besagter Einkaufsstraße als die „Weltöffentlichkeit“? Diese „automatische“ Zustimmung wird auch vom Bundesministerium für Arbeit, Soziales und Konsumentenschutz unter Hinweis darauf bezweifelt, dass solche Auftritte sich ja gerade auf die konkrete Veranstaltung beziehen würden und daher „*nicht öffentlich im Sinne einer Aufnahme oder gar Reproduzierbarkeit*“ wären.[69]

Kann der Straßenkünstler verbieten, sein „öffentliches Verhalten“ zu filmen, wie dies regelmäßig bei Musikkonzerten, somit bei Auftritten im Rahmen von Veranstaltungen, der Fall ist,[70] oder mangelt ihm schon aufgrund der *öffentlichen* Zurschaustellung seiner Künste jegliches Geheimhaltungsinteresse?

---

[63] vgl. für nicht-sensible Daten § 8 Abs 3 Zif 3 und für sensible Daten insbesondere die Bestimmung des § 9 Zif 8 DSG 2000, der die Verwendung sensibler Daten zulässt, soweit dies „zur Wahrung lebenswichtiger Interessen eines Dritten erforderlich“ bzw. „*zur Wahrung lebenswichtiger Interessen eines anderen notwendig ist*“.

[64] § 50a Abs 3 Zif 2 DSG 2000.

[65] dieses Beispiel findet sich in der Stellungnahme zur DSG-Novelle 2010 des Vereins VertretungsNetz – Sachwalterschaft, Patientenanwaltschaft und Bewohnervertretung vom/16.06.2009/(http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00062_38/imfname_161636.pdf).

[66] ob die „Übermittlung“ (ist von der Legaldefinition der „Verarbeitung“ gem. § 4 Zif 9 DSG 2000 nicht erfasst)hier bewusst nicht mit umfasst sein sollte ist fraglich; konkret dürfte daher die zulässige Videoaufnahme nicht an Dritte übermittelt werden, was im Ergebnis einer Nutzung zu „privaten“ Zwecken gleichkommt.

[67] § 50a Abs 3 Zif 2 DSG 2000.

[68] wiewohl eine gültige Zustimmung (die genau genommen auch eine „ausdrückliche“ sein müsste, da es sich bei Videobilddaten ja um potentiell sensible Daten handelt) gem. § 4 Zif 14 DSG 2000 nur „in Kenntnis der Sachlage“ erfolgen kann ... was gerade hier nicht der Regelfall sein wird.

[69] siehe die Stellungnahme des Bundesministeriums für Arbeit, Soziales und Konsumentenschutz zur DSG-Novelle 2010 vom 17.06.2009, GZ BMASK-15003/0009-I/6/2009 (http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00062_36/fname_161633.pdf).

[70] wenn auch das regelmäßig bestehende Filmverbot bei Musikkonzerten urheberrechtliche Gründe hat.

Handelt es sich somit um *allgemein verfügbare Daten* gem. § 1 Abs 1 DSG 2000, die nicht vom Schutzbereich des Grundrechts auf Datenschutz umfasst sind? Da diese Frage auch im Zusammenhang mit Google Street View eine zentrale Rolle spielt, wird dieser unten näher nachgegangen.

Von „ohne jeden Zweifel" kann hier m.E. keine Rede sein.

Exkurs: Google StreetView

„allgemein verfügbare" Daten?

Genau dieser Gedanke der „allgemeinen Verfügbarkeit" von Daten, speziell wenn es sich dabei um auf einem jedermann frei zugänglichen Platz aufhältige Personen oder Häuserfassaden[71] handelt, ist treibende Kraft hinter dem ambitionierten, aber datenschutzrechtlich durchwegs bedenklichen, Projekt der Google Inc/USA. Dabei werden Straßenzüge diverser Städten mittels auf Fahrzeugdächern von PKWs montierter Kameras abfotografiert; die so ermittelten Straßenansichten werden den Nutzern kostenlos in einer Form angeboten, die quasi virtuelle „Spaziergänge" in diesen Städten erlaubt. Die während der Fotofahrten „zufällig" aufgenommenen Gesichter von Personen und Autokennzeichen werden – mit mehr oder minder großem Erfolg[72] – mittels einer Anonymisierungssoftware unkenntlich und somit unidentifizierbar gemacht. Bei den fotografierten Straßenzügen handelt es sich nur um Momentaufnahmen (keine Live-Bilder).

keine systematische Überwachung

Wohlgemerkt: Google StreetView erfüllt mangels *systematischer* Überwachung (siehe oben Punkt 4.2.) zwar nicht den Begriff der Videoüberwachung gem. DSG 2000. Unabhängig davon bietet aber gerade diese Datenanwendung eine ideale Gelegenheit zur näheren Betrachtung des Begriffs der „allgemeinen Verfügbarkeit" von Daten; was in weiterer Folge auch für die Beurteilung der Zulässigkeit einer Videoüberwachung, insbesondere in Zusammenhang mit dem in Punkt 4.4.2 oben erwähnten Zulässigkeitstatbestand des auf „öffentlichen Wahrnehmung" gerichteten Verhaltens gem. § 50a Abs 3 Zif 2 DSG 2000 Bedeutung hat.

zulässig veröffentlichte Daten?

Ennöckl sieht bei diesem Zulässigkeitstatbestand in funktioneller Hinsicht m.E. zutreffend Ähnlichkeiten mit den *allgemein verfügbaren Daten* gem. § 1 Abs 1 DSG 2000,[73] wonach solche Daten überhaupt aus dem Schutzbereich des Grundrechts auf Datenschutz fallen würden und keine Geheimhaltungsansprüche geltend gemacht werden könnten.[74] Einen Schritt weiter geht *Jahnel*[75], der die Begriffe „*allgemein verfügbare*" Daten gem. § 1 Abs 1 DSG 2000 und die in Durchführung dieser Bestimmung in § 8 Abs 2 DSG 2000 geregelten „*zulässigerweise veröffentlichten*" Daten als die beiden Seiten ein und der-

---

[71] Google: „Nichts öffentlicheres als Häuserfassaden", http://derStandard.at/1282273214390/Street-View-Google-Nichts-oeffentlicheres-als-Haeuserfassaden.

[72] siehe dazu *Knoll*, Zur datenschutzrechtlichen (Un)Zulässigkeit von Google Street View, jusIT 1/2010, 16ff., der Beispiele nennt, in denen Hautfarbe, mitgeführte Gegenstände, Statur sowie die Adresse, an der sich diese Personen aufhalten, erkennbar wären und daher durchaus Identifizierbarkeit dieser Personen vorläge.

[73] wobei der EuGH in seinem Urteil vom 16.12.2008, C-73/07 auch öffentlich zugängliche Steuerdaten natürlicher Personen als personenbezogene Daten gewertet hat, wiewohl diese gem. DSG 2000 als „allgemein verfügbare" Daten gar nicht einmal dem Grundrecht auf Datenschutz unterliegen würden. In diesem Punkt entspricht die Umsetzung im DSG 2000 offensichtlich nicht den europarechtlichen Vorgaben.

[74] *Ennöckl*, Die DSG-Novelle 2010, ÖJZ 2010/35, 293ff.

[75] siehe *Jahnel,* Handbuch Datenschutzrecht, 2010,Rz 2/19ff, der auch darauf hinweist, dass in der datenschutzrechtlichen Literatur die Voraussetzungen und Rechtsfolgen der „allgemeinen Verfügbarkeit" bislang erst andiskutiert worden wären.

selben Medaille betrachtet; und in weiterer Folge unter Hinweis auf die Begrifflichkeit der Medienwissenschaft die Vieldeutigkeit des Begriffs „Veröffentlichung“ (je nach Reichweite der Kommunikation) darstellt und dabei (i) die spontane Gesprächsöffentlichkeit, (ii) die Versammlungsöffentlichkeit und die (iii) massenmediale Öffentlichkeit unterscheidet, bei der wiederum die sog. „Online-Öffentlichkeit“ die höchste Ebene bilde. Die Grenze, ab der von einer „allgemeinen Verfügbarkeit“ gesprochen werden könne, würde bei Vorliegen einer Medienöffentlichkeit zu ziehen sein.

Übereinstimmung mit Datenschutzrichtlinie?

Bei den zuletzt gemachten Ausführungen darf darüber hinaus nicht vergessen werden, dass das Nichtvorliegen schutzwürdiger Geheimhaltungsinteressen bei „allgemein verfügbaren“ (§ 1 Abs 1) und „zulässigerweise veröffentlichten“ (§ 8 Abs 2) Daten sowie nunmehr auch bei „Verhalten, dass ohne jeden Zweifel den Schluss zulässt, dass es darauf gerichtet war, öffentlich wahrgenommen zu werden“ (§ 50a Abs 3 Zif 1 DSG 2000) von den europarechtlichen Vorgaben der Datenschutzrichtlinie[76] nicht gedeckt ist.[77]

Zum besseren Verständnis: nicht jedes Verhalten in der Öffentlichkeit ist auch tatsächlich „öffentlich“; die flüchtige Umarmung zweier Menschen, ein inniger Kuss vor dem Stephansdom: beides ist dem privaten, dem jedenfalls schützenswerten, Bereich zuzurechnen. Dazu hat *Knoll* rechtlich schön herausgearbeitet, dass zwischen (allgemein verfügbarem) „Datum“ und (allgemein verfügbarem) „Betroffenen“ zu unterscheiden ist.[78] Dies soll heißen: Selbst wenn die Betroffenen damit rechnen müssten, dass ihr Abbild auf diversen Digitalkameras fotohungriger Touristen landet und sie somit im öffentlichen Raum „allgemein verfügbar“ sind, gilt dies noch lange nicht für ihre „Daten“, d. h. für das konkret geschossene Foto, das regelmäßig nur dem Fotografierenden, nicht aber „allgemein verfügbar“ ist. **Eine Person, die sich in der Öffentlichkeit aufhält, veröffentlicht keine Daten.** Mangels allgemeiner Verfügbarkeit von „Daten“, sind den Betroffenen daher auch hier sehr wohl schutzwürdige Geheimhaltungsinteressen zuzuerkennen; keinesfalls wird auf diese verzichtet, nur weil man sich in der Öffentlichkeit aufhält.

Recht am eigenen Bild

Schließlich müsste – um von allgemeiner Verfügbarkeit sprechen zu können – die Allgemeinheit über diese Daten verfügen dürfen; die Veröffentlichung der Fotos daher rechtlich zulässig sein. Dies ist regelmäßig schon allein aufgrund des Rechts am eigenen Bild nicht der Fall, weshalb eine „allgemeine Verfügbarkeit“ i.S. des DSG 2000 in Zusammenhang mit Google Street View gerade nicht vorliegt.

enge Auslegung von Ausnahmen notwendig

Diese Gedankengänge lassen sich auch auf die hier zu behandelnde Videoüberwachung übertragen. Die Nichtverletzung schutzwürdiger Geheimhaltungsinteressen gem. § 50a Abs 3 Zif 2 DSG 2000 bei einem Verhalten, das ohne jeden Zweifel den Schluss zulässt, darauf gerichtet gewesen zu sein, öffentlich wahrgenommen zu werden, ist jedenfalls äußerst eng auszulegen.

---

[76] RL 95/46 zum Schutz personenbezogener Daten und zum freien Datenverkehr.

[77] siehe dazu *Jahnel,* Handbuch Datenschutzrecht, 2010, Rz 4/26f sowie die in Art. 3 Abs 2 der RL 95/46 taxativ aufgezählten Ausnahmetatbestände für die Anwendbarkeit der RL 95/46, nämlich (i) die Ausübung von Tätigkeiten, die außerhalb des Anwendungsbereichs des Gemeinschaftsrecht liegen und (ii) diejenigen Tätigkeiten, die zum Privat- oder Familienleben von Privatpersonen gehören. Auch die ARGE Daten nimmt sich in ihrer Stellungnahme zur DSG-Novelle 2010 vom 08.06.2009, Seite 22f (http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00062_02/imfname_160593.pdf) dieser Problematik an und schlägt vor, dass veröffentlichte Daten nur in dem mit dem ursprünglichen Veröffentlichungszweck vereinbaren Umfang verwendet werden dürfen.

[78] siehe dazu *Knoll*, Zur datenschutzrechtlichen (Un)Zulässigkeit von Google Street View, jusIT 1/2010, 16ff.

Das Verhalten der betroffenen Person muss dabei – da dieser Zulässigkeitstatbestand ja auf einer Stufe mit der „ausdrücklichen" Einwilligung (siehe oben) steht – jedenfalls zweifelsfrei darauf gerichtet sein, nicht nur in der Öffentlichkeit wahrgenommen zu werden, sondern auch damit einverstanden zu sein, bei diesem Verhalten gefilmt (was wiederum Kenntnis der Videoüberwachung voraussetzt) und in der Folge veröffentlicht zu werden; nur damit wird eine Annäherung an die *allgemein verfügbaren Daten* iS. des § 1 Abs 1 DSG 2000 erreicht und wären keine schutzwürdigen Geheimhaltungsinteressen verletzt.

weitere Kritikpunkte zu Google StreetView

Am 21.05.2010 hat die DSK ein amtliches Prüfverfahren gem. DSG 2000 zur Klärung des Sachverhalts gegen Google eingeleitet und Google die Weiterverwendung aller Street View-Daten untersagt. Da sich im Ermittlungsverfahren herausstellte, dass die Erhebung der WLAN-Daten zu einem anderen Zweck erfolgte als die Anwendung „Google Street View" und daher nicht der Datenanwendung „Street View" zuzuordnen war, wurde der Mandatsbescheid per Ende November 2010 aufgehoben; zeitgleich wurde aber auch ein Verfahren zur Feststellung des für die Erfüllung der Meldepflicht erheblichen Sachverhalts betreffend die durch Google Inc. registrierten Datenanwendung „Google Street View" eingeleitet („Verfahren zur Überprüfung der Registrierung").[79] Das Ergebnis bleibt abzuwarten; ein weiterhin kritischer Punkt sei unter anderen, dass die aufgenommenen Bilder **nicht** anonymisiert in die USA weitergegeben würden; erst dort würden automatisiert Gesichter und Autokennzeichen technisch „verwischt" (gemeint: anonymisiert).[80]

fehlende Vorabwiderspruchsmöglichkeit

Eine Vorabwiderspruchsmöglichkeit wie in Deutschland[81] ist laut einem Google-Sprecher für Österreich nicht geplant.[82] In Deutschland können nämlich seit Mitte August 2010 Mieter und Eigentümer abfotografierter Gebäude bereits vorab Widerspruch gegen deren fotografische Verwendung im Rahmen von Google Street View erheben; Wirkung des Widerspruchs ist, dass die betreffenden Gebäude unkenntlich zu machen sind. Generell kann lt. Google nachträglich immer die Unkenntlichmachung von Gebäuden verlangt werden,[83] was sinngemäß dem Widerspruchsrecht gem. § 28 DSG 2000 entspricht.

---

79 Hintergrund für die Untersagung der Street View-Daten war die Ermittlung von W-LAN-Daten durch Google im Zuge der Datensammlung für Google Street View. (zum aktuellen Stand siehe http://www.dsk.gv.at/site/6733/default.aspx).

80 siehe Interview mit Eva Souhrada-Kirchmayer (geschäftsführendes Mitglied der Datenschutzkommission) vom 01.12.2010 in DiePresse.com (http://diepresse.com/home/techscience/internet/google/614732/Freie-Fahrt-fuer-Google-Street-View_So-geht-es-weiter?direct=615427&_vl_backlink=/home/techscience/internet/google/615427/index.do&selChannel=.

81 siehe dazu ausführlich das Infoblatt des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit: http://www.hamburg.de/contentblob/2453512/data/vorab-widerspruch-google-street-view.pdf; zur Situation in Deutschland generell und in Berlin im Speziellen siehe „Berlin will keine „Lex Google", http://derStandard.at/1281829326031/Street-View-Berlin-will-keine-Lex-Google.

82 vgl. dazu die Zitierung des Google-Sprechers Kay Oberbeck in Der Standard vom 17.08.2010, „Berlin will keine „Lex Google", der auch darauf hinwies, dass eine Beeinspruchung **nach** Veröffentlichung, wie auch den 23 Ländern mit Street View, möglich sein soll.

83 siehe FN 46.

4.4.3 Schutzwürdige Geheimhaltungsinteressen (unter Berücksichtigung überwiegender Interessen des Auftraggebers)

Videodaten potentiell sensibel

Die von einer Videoüberwachung erfassten Daten werden vom Gesetzgeber selbst als *potentiell sensibel* eingestuft, weil die Bilder regelmäßig Informationen über den Gesundheitszustand oder die ethnische Zugehörigkeit (Hautfarbe) der Betroffenen liefern würden.[84] Dass Videobilddaten vom DSG 2000 auch sonst wie „sensible" Daten[85] behandelt werden, zeigt auch die jeweils nötige Vorabkontrolle im Rahmen der Registrierung einer Videoüberwachung; dies aufgrund des gegenüber „herkömmlichen" Datenanwendungen größeren Gefährdungspotentials.

taxative Liste von Ausnahmen, ...

Dazu passend regelt auf den ersten Blick die DSG-Novelle 2010 auch – über die unter Punkt 4.2 aufgezeigten Fälle hinaus – taxativ (abschließend) diejenigen Fälle, in denen schutzwürdige Geheimhaltungsinteressen der betroffenen Personen bei Videoüberwachungen nicht verletzt sein sollen;[86] auch das steht in Einklang mit dem sonst bei sensiblen Daten vom DSG 2000 vorgesehenen Umgang, nämlich sich auf eine taxative Ausnahmenliste zu beschränken, um die Grenzen zulässiger Datenverwendungen im „sensiblen" Bereich möglichst eng abzustecken.[87]

Wichtig: selbst das Vorliegen einer dieser taxativen Ausnahmen macht eine Videoüberwachung nicht automatisch datenschutzrechtlich zulässig sind; vielmehr ist in jedem Einzelfall immer noch die *Verhältnismäßigkeit* der Maßnahme zu prüfen ist (dazu gleich mehr weiter unten).

Auf den zweiten Blick zeigt diese taxative Ausnahmenliste aber doch ihre Schwächen.

... aber durch unklare Begriffe unterlaufen

Bei allem Verständnis für die erstmalige Regelung einer neuen Materie: wie kann sich der Gesetzgeber in einem so eingriffsintensiven Bereich wie der Videoüberwachung dazu hinreißen lassen, die Zulässigkeit einer Videoüberwachung für den Fall zu bejahen, wenn

> „... ***bestimmte Tatsachen*** (Anm.: Hervorhebung durch den Autor) *die Annahme rechtfertigen, das überwachte Objekt oder die überwachte Person könnte das Ziel oder der Ort eines gefährlichen Angriffs werden ...*"? Viel unbestimmter als „bestimmte Tatsachen" kann schwer formuliert werden, wobei auch die nötige „Glaubhaftmachung" solcher Tatsachen bei Erstattung der Meldung (siehe unten Punkt 6.) kein wirklicher Trost ist; vom Begriff „gefährlicher Angriff"[88] ganz zu schweigen, der selbst vom Bundesministerium für Inneres – mangels Legaldefinition – abgelehnt wird.[89]

---

[84] siehe RV 472 BlgnNr 24. GP 18.

[85] bei diesen besonders schutzwürdigen Daten handelt es sich gem. § 4 Zif 2 DSG 2000 um Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszughörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben.

[86] § 50a Abs Zif 1-3 DSG 2000.

[87] siehe dazu § 9 DSG 2000, der insgesamt 13 Fälle auflistet, in denen schutzwürdige Geheimhaltungsinteressen bei Verwendung sensibler Daten nicht verletzt werden.

[88] darunter soll gem. den Erläuterungen nämlich nicht der Begriff des „gefährlichen Angriffs" gem. dem Sicherheitspolizeigesetz (SPG) verstanden werden, sondern ein „weiterer" (wohl ebenfalls „demonstrativ" zu konkretisierender) Begriff, unter den bspw. auch die Gefährdung von Betriebs- und Geschäftsgeheimnissen fallen soll.

[89] siehe Stellungnahme des BMI zur DSG-Novelle 2010 vom 18.06.2009, GZ GZ.: BMI-LR1420/0009-III/1/a/2009 (http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00062_44/fname_161644.pdf).

> Die Erläuterungen selbst räumen ein, dass hier „*... noch gewisse unbestimmte Rechtsbegriffe ...*“ verwendet wurden, die „*... nur demonstrativ konkretisiert werden ...*“. Dass damit Sinn und Zweck einer taxativen Aufzählung unterlaufen wird, liegt auf der Hand. Damit aber nicht genug.

Wenn schon „demonstrativ“ konkretisiert wird, dann wäre der Gesetzestext der richtige Ort für Konkretisierungen; statt dessen finden sich im Gesetzestext keine weiteren Hinweise; erst in den Erläuterungen finden sich die entscheidenden Hinweise, wie dieser „taxativ, demonstrativ zu konkretisierende“ Zulässigkeitstatbestand auszulegen ist. Hier werden ausdrücklich die (i) Bedrohung mit gerichtlich strafbaren Vorsatztaten und (ii) präventive Videoüberwachungen in Hinblick auf eine konkrete Gefährdung des überwachten Objekts oder der überwachten Person (auch wenn noch kein gefährlicher Angriff stattgefunden hat) genannt. Beispielhaft wird für potentiell zulässige Eingriffe angeführt:

> Objekt oder Person waren bereits innerhalb der letzten 10 Jahre einmal Ziel oder Ort eines gefährlichen Angriffs und eine Wiederholung sei wahrscheinlich,
>
> die Person/das Objekt habe einen überdurchschnittlichen Bekanntheitsgrad oder halte sich die Person dort auf,
>
> das Objekt ist ein beweglicher Gegenstand von erheblichem Geldwert oder ein Aufenthaltsort solcher Gegenstände,
>
> das überwachte Objekt ist ein Gegenstand von außergewöhnlichem künstlerischem Wert.

Konkretisierung nur in Erläuterungen

Abgesehen von der doch recht eigenwilligen Regelungstechnik (nämlich „Gesetzestext“ in den Erläuterungen zu verstecken) darf angemerkt werden, dass dieser „Fallkatalog“ im Ministerialentwurf zur (aufgrund der Auflösung der Koalitionsregierung im Sommer 2008 nicht mehr beschlossenen) DSG-Novelle 2008[90] noch ausdrücklich im Gesetzestext des § 50 a Abs 3 enthalten war. Wichtig ist festzuhalten, dass die Erläuterungen als solche keinerlei Gesetzeskraft haben[91] sondern lediglich dem besseren Verständnis des Gesetzestextes dienen (Motto: „Der Gesetzgeber beschließt das *Gesetz, nicht* die Materialien.“). Unbeachtlich sind auch solche Gesetzesmaterialien, die schon in sich widersprüchlich bzw. unklar sind. „Erläuterungen“, die mehr zur Verwirrung beitragen als erklären, sind daher gleichfalls unbeachtlich.

Echtzeitüberwachung

weder Speicherung noch Weiterverarbeitung

Ebenso werden gem. der DSG-Novelle 2010 keine schutzwürdigen Geheimhaltungsinteressen verletzt, soweit „*... sich die Überwachung in einer bloßen Echtzeitwiedergabe von das überwachte Objekt/die überwachte Person betreffenden Ereignissen erschöpft, diese also weder gespeichert (aufgezeichnet) noch in sonst einer anderen Form weiterverarbeitet (Echtzeitüberwachung) werden, und sie zum Zweck des Schutzes von Leib, Leben oder Eigentum des Auftraggebers erfolgt*.“ Mit dieser Art der Überwachung könne der Beweissicherungszweck nicht erreicht werden und liege deshalb eine weniger eingriffsintensive – ja sogar ein gelinderes Mittel i.S. des Verhältnismäßigkeitsgebots – vor.

---

[90] siehe 182/ME XXIII. GP – Ministerialentwurf, http://www.parlament.gv.at/PAKT/VHG/XXIII/ME/ME_00182/index.shtml.

[91] und wie hier Teil einer Regierungsvorlage sind, d. h. eigentlich von der „Exekutive“ und nicht von der „Legislative“ erlassen wurden.

nur für den Eigenschutz zulässig

Wichtig: wie oben in Punkt 4.1 ausgeführt, kommen als rechtmäßige Zwecke einer Videoüberwachung i.S. des DSG 2000 nur die Zwecke „Eigen- und Verantwortungsschutz“ in Betracht. **Die „Sonderregelung“ für die Echtzeitüberwachung erfasst aber nur einen dieser beiden Zwecke, nämlich den „Eigenschutz“.** Eine Echtzeitüberwachung zum Zweck „Verantwortungsschutz“, etwa die Überwachung ausschließlich des Kundenbereiches einer Bankfiliale, ist davon nicht umfasst und daher an den sonstigen Ausnahmetatbeständen des § 50a Abs 4 DSG 2000 zu prüfen; schutzwürdige Geheimhaltungsinteressen der Betroffenen sind hier zu berücksichtigen.

Der Gesetzgeber ordnet die Echtzeitüberwachung somit zwar grundsätzlich als „Videoüberwachung“ ein; soweit sie aber „nur“ zum Zweck „Eigenschutz“ erfolgt, überwiegen im Ergebnis die Interessen des Auftraggebers und wäre der Betroffene in seinen schutzwürdigen Geheimhaltungsinteressen nicht verletzt.

Sonderregelung gilt nicht bei Echtzeitüberwachungen zu Informationszwecken

Schutzwürdige Geheimhaltungsinteressen der Betroffenen sind auch bei Echtzeitüberwachungen zu „Informationszwecken“ bspw. über die Kundenfrequenz einzelner Filialen einer Computerkette (keine Rechtsgrundlage)[92] sehr wohl zu berücksichtigen. Auch in diesem Fall kommt die Sonderregelung für die Echtzeitüberwachung nicht zum Tragen.

Judikatur abzuwarten

Die mehr als zweifelhafte Sonderregelung für die Echtzeitüberwachung zum „Eigenschutz“ wird als Regelungslücke wohl durch die Judikatur des OGH zu schließen sein.[93] Dieser hat bereits in der Anbringung einer Überwachungskamera-Attrappe eine Verletzung der Privatsphäre des Betroffenen gesehen, da dieser einem ständigen Überwachungsdruck ausgesetzt wurde und sich aufgrund des Vorhandenseins der Kameraattrappe kontrolliert fühlen musste (OGH 28.3.2007, 6 Ob 6/06k).

fehlende Konformität mit Datenschutzrichtlinie

Nicht unerwähnt soll bleiben, dass der Datenschutzrat (DSR) in seiner Stellungnahme zur DSG-Novelle 2010 vom 04.08.2009 darauf hweist, dass eine Ausklammerung der Echtzeitüberwachung – unabhängig ob „Eigen- oder Verantwortungsschutz“ – aus dem Bereich der Videoüberwachung durch die Datenschutz-Richtlinie 94/46/EG nicht gedeckt wäre.[94]

---

[92] siehe dazu bspw. die Webcams der DiTech GmbH (http://www.ditech.at/info/webcam.html); die DSK hat generell auf ihrer homepage bereits ausdrücklich in Zusammenhang dem Einsatz von Webcams darauf aufmerksam gemacht (http://www.dsk.gv.at/site/6301/default.aspx), dass in diesen Fällen eine Datenübermittlung an die Öffentlichkeit vorliege (der der Betroffene regelmäßig wohl nicht vorab zugestimmt hat).

[93] siehe dazu auch die Stellungnahme des Ludwig Boltzmann Instituts für Menschenrechte (BIM) vom 17.06.2010, Seite 14, http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00062_39/imfname_161639.pdf, die im Ergebnis auf die unterschiedlichen Blickwinkel betr. Echtzeitüberwachung aus Sicht des DSG 2000 und der Judikatur des OGH aufmerksam macht.

[94] http://www.bka.gv.at/DocView.axd?CobId=36118.

4.4.4 Wo/was darf jedenfalls nicht überwacht werden

höchstpersönliche Lebensbereiche

Unabhängig vom Vorliegen von Eigen- oder Verantwortungsschutz dürfen – nun explizit gesetzlich geregelt[95] – mit einer Videoüberwachung keinesfalls Ereignisse an Orten festgestellt werden, die zum höchstpersönlichen[96] Lebensbereich eines Betroffenen zählen, wie das bspw. bei Privatwohnungen, Umkleide- oder WC-Kabinen der Fall ist. Eine Klarstellung dahingehend, dass eine solche Videoüberwachung auch nicht durch eine „Zustimmung" der betroffenen Person ersetzbar ist, wäre hier zweckmäßig; dies insbesondere deshalb, da § 50a Abs 5 DSG 2000 nur auf Videoüberwachungen gem. Abs. 4 verweist (die Videoüberwachung aufgrund einer „Zustimmung" aber in Abs. 3 geregelt ist.

Kontrolle von MitarbeiterInnen

Ausdrücklich verboten ist auch die gezielte Videoüberwachung zur Kontrolle von Mitarbeitern an Arbeitsstätten[97], da gem. den Erläuterungen[98] hier davon auszugehen sei, dass „*... hier auf Grund der Eingriffstiefe stets ein gelinderes Mittel zur Kontrolle von Mitarbeiterinnnen und Mitarbeitern gefunden werden ...*" könne; gemeint ist hier das Verbot der „Leistungskontrolle" von Mitarbeitern, nicht aber die Videoüberwachung zum Schutz des Umfeldes der Mitarbeiter vor besonderen Gefahren (gefährliche Maschinen, Intensivstation, etc. ...); weiters auch nicht die – auch Mitarbeiter betreffende – dauernde Überwachung besonderer Sicherheitszonen, wie etwa Serverräume, um unbefugte Eingriffe hintan zu halten, was zum Stand der Technik gehöre.[99]

4.5 Heiligt der Zweck die Mittel? Zum Grundsatz der Verhältnismäßigkeit

Gebot der Verhältnismäßigkeit

„*Auch im Falle zulässiger Beschränkungen darf der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden.*"; so regelt die Verfassungsbestimmung in § 1 Abs 2 letzter Satz DSG 2000 das Verhältnismäßigkeitsgebot. Soll heißen: selbst wenn der „Zweck" der Videoüberwachung zulässig und auch die Interessen des Auftraggebers die (soweit überhaupt vorhandenen) schutzwürdigen Geheimhaltungsinteressen des Betroffenen überwiegen, bleibt als letzte Bastion gegen eine solche Datenverwendung immer noch der Grundsatz der Verhältnismäßigkeit.

Grundsatz in Verfassungsrang

Die Bedeutung dieses im Verfassungsrang stehenden Grundsatzes wird in der DSG-Novelle 2010 noch dadurch hervorgehoben, als dieser in § 50a Abs 2 – neben der Geltung der §§ 6 und 7 DSG 2000 – ausdrücklich angeführt wird, um zumindest hier keine Missverständnisse aufkommen zu lassen.

---

[95] § 50 Abs 5 DSG 2000.

[96] die ARGE-Daten möchte bspw. in ihrer Stellungnahme vom 08.06.2009 zur DSG-Novelle 2010, Seite 20, darunter auch alle Bereiche verstehen, wo sich jemand „entblößt".

[97] siehe für die Situation in Deutschland: derStandard.at, Berlin bekämpft Bespitzelung vom 25.08.2010, http://derstandard.at/1282273584664/Videoueberwachung-im-Job-Berlin-bekaempft-Bespitzelung.

[98] RV 472 BlgnNr 24. GP 18.

[99] worauf die DSK in ihrer Stellungnahme zur DSG-Novelle 2010 vom 14.07.2009, Seite 17, hingewiesen hat (siehe http://www.parlament.gv.at/PG/DE/XXIV/ME/ME_00062_57/imfname_164857.pdf).

Die Erläuterungen[100] bieten auch hier wieder eine nicht selbstverständliche Fülle von Beispielen, wie dieser Grundsatz in Zusammenhang Videoüberwachung zu verstehen ist:

gelindere Mittel vorzuziehen

„Sofern taugliche Mittel zur Zielerreichung bestehen, die weniger eingriffsintensiv sind als das Mittel der Videoüberwachung, sind diese jedenfalls einer Videoüberwachung vorzuziehen. Zu denken wäre etwa an den Einsatz von RFID-Chips an Waren in Geschäften zur Sicherung vor Diebstählen.“ Das Bestehen gelinderer Mittel hat der Gesetzgeber in Zusammenhang der (Leistungs-)Kontrolle von Mitarbeitern (siehe oben Punkt 4.4.4) jedenfalls gleich selbst vorweggenommen (ohne aber konkrete Anhaltspunkte zu geben, wie diese alternative Kontrolle auszusehen hat bzw. darf). Weiters verweisen die Erläuterungen – soweit es um das Sicherheitsbedürfnis geht – auf die Möglichkeit der Verwendung von Sicherheitstüren, Gegensprechanlagen, Alarmanlagen etc..

Echtzeitüberwachung

Auch der Eingriff durch Echtzeitüberwachung (real time monitoring) stelle ein „gelinderes“ Mittel dar als die Videoüberwachung samt Speicherung der angefallenen Daten. Echtzeitüberwachung reiche bspw. bei Zweck des rechtzeitigen Schutzes vor einer Gefahr bzw. um bei einem Unfall sofort reagieren zu können; soweit aber – wie wohl häufig der Fall – auch der Schutz des Eigentums eine Rolle spielt, wird mit Echtzeitüberwachung nicht das Auslangen gefunden werden, da ja nachträglich (zur Beweissicherung) auch dokumentiert werden muss, wer wie bspw. einen Schaden konkret verursacht hat.

konkreter Zweck und ...

Schließlich nehmen die Erläuterungen auf einen der wohl häufigsten Fälle von Videoüberwachung, nämlich die Gebäudeüberwachung, Bezug und führen zutreffend (wenn auch wenig überraschend) aus, dass die Videoüberwachung eines Einfamilienhauses weniger eingriffsintensiv sei als die eines Mehrparteienhauses (hier wären bspw. auch Rückschlüsse auf sensible Daten bei einer Arztpraxis etc. möglich).

... Situation für Verhältnismäßigkeit ausschlaggebend

Die Zulässigkeit einer Videoüberwachung könne schließlich immer nur unter Bedachtnahme auf die konkrete Situation und unter sorgfältiger Abwägung der Geheimhaltungsinteressen der Betroffenen gegenüber den Interessen Dritter unter Einhaltung der Verhältnismäßigkeit beurteilt werden.

4.5.1 Technischer Datenschutz/privacy enhancing technologies

Privacy by design

Immer wieder wird zu Recht angeregt, die technischen Möglichkeiten datenschutzfreundlicher Gestaltung (durch sogenannte „privacy enhancing technologies“) von Videoüberwachungen durch eine Verwendungsprivilegierung zu fördern.[101]

Verschlüsselung der Aufzeichnungen von Personen

Als konkretes Beispiel führt die DSK den Einsatz von Technik an, die das Entschlüsseln des Abbilds einzelner von mehreren nicht-erkennbar aufgenommenen Person(en) ermöglicht, um das Problem des Eingriffes in die Datenschutzrechte Dritter bei Auskunftsersuchen aus Videoaufzeichnungen befriedigender lösen zu können.

---

[100] RV 472 BlgnNr 24. GP 18.

[101] siehe dazu die Stellungnahme der DSK zur DSG-Novelle 2010, Seite 19, http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00062_57/imfname_164857.pdf;
auch der DSR spricht sich in seiner Stellungnahme zur DSG-Novelle 2010 vom 04.08.2010 in Punkt 5g, http://www.oesterreich.gv.at/DocView.axd?CobId=36118, für die Prüfung bspw. der unkomplizierten und günstigen Verschlüsselung von Videodaten aus und schlägt vor, diese gegebenenfalls zu fördern.

keine konkreten Regelungen oder Mindeststandards

Die Richtervereinigung merkt in ihrer Stellungnahme[102] an, dass in den vorgeschlagenen gesetzlichen Regelungen nicht erkennbar sei, ob auf die Möglichkeiten des technischen Datenschutzes Bedacht genommen und diese ausgeschöpft wurden. Weiters sei *„auffallend, dass der Entwurf keinerlei Regelungen zum technischen Mindeststandard und über Verschlüsselung und Zugangssicherung enthält, um sicherzustellen, dass nur der Auftraggeber Zugang zu den Videoaufnahmen hat (auch im Falle von Echtzeitaufnahmen).“*

PETs als gelinderes Mittel privilegieren

Selbst wenn die ausführliche Nennung datenschutzfreundlicher Technologien (Privacy Enhancing Technologies – PEts) im Gesetz unterblieben ist, bleibt m.E. aber doch im Rahmen der Prüfung „gelinderer Mittel“ durchaus Raum, solche Technologien entsprechend zu „privilegieren“ bzw. den Maßstab für „gelindere Mittel“ an diesen auszurichten:

geprüfte Technologien sind verfügbar

Als konkretes Beispiel für eine solche Technologie darf hier der KiwiVision Privacy Protector[103]erwähnt werden; dem erstmalig in Österreich das Europäische Datenschutzgütesiegel[104] verliehen wurde. Der Privacy Protector ist eine Software und wird in ein Videomanagementsystem derart eingebunden, dass die von der Videokamera gelieferten Video-Klardaten an den Privacy Protector weitergeleitet werden; die Software lernt, zwischen (bewegtem) Vorder- und (stillstehendem) Hintergrund zu unterscheiden und verschleiert/verpixelt bewegte Objekte und Personen im Vordergrund derart, dass diese in Echtzeit anonymisiert werden (d. h. nicht mehr identifiziert werden können). Auch können Bereiche des Bildausschnitts festgelegt werden, die unabhängig vom aktuellen Bildvordergrund immer bzw. nie verschleiert werden sollen. Ein solches System wurde bereits erfolgreich im April dieses Jahres an einer Management-Institution in Tirol implementiert. Der Vorteil des Systems liegt auf der Hand: der Zugriff auf die (separat verschlüsselt gespeicherten) Videoklardaten erfolgt nur im begründeten Anlassfall (Vandalismus etc.), ansonsten sieht der für die Überwachung Zuständige nur anonymisierte Personen und Objekte am Campus.

4.6 Was ist wirklich neu?

4.6.1 Meldepflicht und wann die Videoüberwachung gestartet werden darf

Meldepflicht und Vorabkontrolle

Gem. der DSG-Novelle 2010 sind Videoüberwachungen im privaten Bereich hinsichtlich der Meldepflicht gleich zu beurteilen, wie sonstige Datenanwendungen. Da Videoüberwachungen potentiell sensible Daten verwenden, wird nun ausdrücklich die Vorabkontrollpflicht einer solchen Datenanwendung durch die DSK vorgeschrieben, soweit der Auftraggeber nicht bereits in der Meldung der Datenanwendung zusagt, die Videoüberwachungsdaten zu verschlüsseln und sicherzustellen, dass der einzige Schlüssel bei der DSK hinterlegt und eine Auswertung der Videoaufzeichnungen nur im begründeten *Anlassfall* durch eine bestimmte Stelle stattfindet (siehe dazu gleich unten). Die grundsätzliche Meldepflicht für Videoüberwachungen war schon in den Leit-

[102] siehe die Stellungnahme zur DSG-Novelle 2010 vom 17.06.2009 (http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00062_45/imfname_161897.pdf).

[103] näheres unter http://www.kiwi-security.com.

[104] näheres unter https://www.european-privacy-seal.eu/awarded-seals/de-090017.

linien des oben erwähnten Datenschutzberichts 2005 – 2007 vorgegeben und wurde in der DSG-Novelle 2010 fast 1:1 beibehalten.[105]

Ausnahme: Standardvideo-überwachung

Um die Flut der zu erwartenden Meldungen von Videoüberwachungen zumindest teilweise abzufangen, wurde die Standard- und Musterverordnung 2004 (StMV 2004) novelliert[106] und die bislang bestehenden Standardanwendungen um die „SA032 Videoüberwachung" ergänzt. Diese gilt für Banken, Juweliere, den Handel mit Antiquitäten und Kunstgegenständen, für Gold- und Silberschmiede, Trafiken, Tankstellen und bebaute Privatgrundstücke (samt Hauseingang und Garage) und soll die regelmäßig dort zum Einsatz kommenden Videoüberwachungsanlagen von der Meldepflicht ausnehmen. Der Verordnungsgeber hat sich dabei offensichtlich auch die Kritik an den fehlenden technischen Vorgaben zumindest teilweise zu Herzen genommen und mit Ausnahme der Videoüberwachung bebauter Privatgrundstücke nur „verschlüsselte Videoüberwachung" als „Standard" vorgegeben. Da in sämtlichen genannten Fällen (auch für Banken) die Speicherfrist mit 72 Stunden festgesetzt wurde, wird in vielen Fällen aber kein Weg an einer gesonderten Meldung der Videoüberwachung bei der DSK vorbeiführen.

Gemäß § 61 Abs 6 DSG 2000 dürfen alle Videoüberwachungen in Betrieb bleiben, die vor Inkrafttreten des § 50a registriert wurden und die den am 31.12.2009 geltenden DSG 2000-Bestimmungen genügen und bei denen die DSK keine Befristung verfügt hat; ansonsten gilt die Befristung bzw. endet die Zulässigkeit spätestens am 31.12.2012.

Nutzung der Option Schlüsselhinterlegung noch offen

Ob die nun neu ins DSG 2000 aufgenommene **Schlüsselhinterlegung** bei der DSK auch tatsächlich „angenommen" wird, bleibt abzuwarten.[107] Die bisherigen Meinungen sind skeptisch und verweisen auf durchaus praktische Probleme bei der Schlüsselbeschaffung;[108] etwa wenn der „Anlassfall" dringend und zur Nachzeit eintritt (speziell vor dem Hintergrund, dass die Daten spätestens binnen 72 Stunden zu löschen sind) oder durch die verzögerte Auslieferung des Schlüssels die Aufklärung eines Einbruchs vereitelt wird.[109]

Ausnahmen von der Meldepflicht: Echtzeitüberwachung und Verwendung analoger Speichermedien → zwei „Spezialfälle"

In § 50c Abs 2 Zif 1. und 2. wurden zwei schwer nachvollziehbare Ausnahmen von der Meldepflicht festgelegt:

unklare Definition der Ausnahme „Echtzeitüberwachung"

Die Echtzeitüberwachung: hier ist unklar, ob damit „nur" die Echtzeitüberwachung gem. § 50a Abs 4 Zif 3 DSG 2000 gemeint ist (d. h. zum Zweck „Eigenschutz") oder „Echtzeitüberwachung" generell; weder im Gesetzestext noch in den Erläuterungen finden sich hier passende Hinweis, wobei die Erläuterungen undifferenziert von der vergleichsweise niedrigen Eingriffstiefe der „bloßen Echtzeitüberwachung" sprechen ... was mE eher in Richtung eines generellen Ausnahmetatbestandes weist.

---

105 § 50b Abs 2 DSG 2000.

106 BGBl. II Nr. 152/2010.

107 gem. Telefonat mit der Leiterin des DVR, Huberta Goriup, vom 20.01.2010, wäre bislang noch kein einziger Schlüssel hinterlegt worden.

108 Pollirer/Weiss/Knyrim, DSG (2010), MANZ-Sonderausgabe, Anmerkung 1) zu § 50 c.

109 siehe dazu den DSG Info-Service der Secur – Data Betriebsberatungs – Gesellschaft m.b.H., http://secur-data.at/typo3/index.php?id=146, wo für den Fall der vereitelten Aufklärung auf das Vorliegen eines klassischen Amtshaftungsfalles hingewiesen wird.

analoge Speichermedien

Schließlich diejenigen Videoüberwachungen, soweit die Speicherung (Aufzeichnung) nur auf einem analogen Speichermedium (VHS-Rekorder etc.) erfolgt. Eine solche Ausnahme wird in den Erläuterungen damit begründet, dass auf Grund der nur sehr beschränkten Strukturierbarkeit und damit Suchbarkeit die Gefährdung von Geheimhaltungsinteressen unbeteiligter Dritter deutlich herabgesetzt wäre; wie dies mit der technisch jederzeit möglichen (und datenschutzrechtlich kaum untersagbaren) nachträglichen Digitalisierung vereinbar ist, wird offen gelassen. Auch der Hinweis auf Art 18 Abs 2 1. Spiegelstrich der DS-RL kann nicht überzeugen: dort ist zur Möglichkeit der Mitgliedstaaten zur Vereinfachung bzw. Ausnahme von der Meldepflicht geregelt: „*Sie legen für Verarbeitungskategorien, bei denen unter Berücksichtigung der zu verarbeitenden Daten eine Beeinträchtigung der Rechte und Freiheiten der betroffenen Personen* ***unwahrscheinlich*** (Hervorhebung durch den Autor) *ist, die Zweckbestimmungen der Verarbeitung, die Daten oder Kategorien der verarbeiteten Daten, die Kategorie(n) der betroffenen Personen, die Empfänger oder Kategorien der Empfänger, denen die Daten weitergegeben werden, und die Dauer der Aufbewahrung fes ...*“.

Dass eine Beeinträchtigung bei Speicherung auf analogen Medien „unwahrscheinlich“ wäre, wurde in den Erläuterungen (zutreffend) nicht einmal behauptet. Diese Ausnahme ist daher durch nichts zu rechtfertigen.[110]

Der Vollständigkeit halber ist festzuhalten, dass Videoüberwachungen gem. der oben in Punkt 4.6.1 beschriebenen Standardanwendung ebenfalls „meldefrei“ sind.

4.6.2 Zufallstreffer

Einschränkungen der Auswertung bei Fremdschutz ...

Ausgangslage gem. DSK: „*Auswertungen für Zwecke des Fremdschutzes (betrifft Personen, mit welchen der Auftraggeber in keiner Rechtsbeziehung steht, die ein Recht auf Schutz von Eigentum, Leben oder Sicherheit dieser Person begründet) dürfen nur vorgenommen werden, soweit für die Herausgabe eine gesetzliche Verpflichtung besteht, wie etwa nach §§ 109 ff, insbes. § 111 Abs. 2 der Strafprozessordnung 1975 idF. BGBl I Nr. 19/2004.*“[111]

... durch DSG-Novelle aufgeweicht

Die DSG-Novelle 2010 hat an dieser Ausgangslage insofern „aufgeweicht“, als nunmehr gem. § 50a Abs 6 DSG 2000 Auswertungen zum „Fremdschutz“[112] (somit über die in Punkt 4.4.1 angeführten zulässigen Zwecke „Eigen- und Verantwortungsschutz“ hinaus) praktisch insoweit „erlaubt“ werden, als die davon betroffenen Videodaten unter bestimmten Bedingungen an die zuständigen Behörden bzw. Gerichte übermittelt werden dürfen; in diesen Fällen sollen nach Vorstellung des Gesetzgebers keine schutzwürdigen Geheimhaltungsinteressen der davon Betroffenen verletzt werden.

---

[110] siehe dazu auch Pollirer/Weiss/Knyrim, DSG (2010), MANZ-Sonderausgabe, Anmerkung 2) zu § 50 c, die darauf hinweisen, dass die DS-RL nicht zwischen analogen und digitalen Aufnahmen unterscheidet.

[111] vgl. Bescheid der DSK vom 06.02.2008, Zahl: K600.049-424/0001-DVR/2008/00 betr. „V424 Videoüberwachung (temporär) in den Wohnhausanlagen der Stadt Wien“.

[112] bspw. „Disco-Mord“ in Wien Floridsdorf, bei dem laut Polizei aufgrund von Bildern aus zwei Überwachungskameras (eines dort ansässigen Unternehmens) aus über 700 infrage kommenden Pkw ein Fahrzeug ermittelt werden, das einen Tag nach der Tat abgemeldet worden ist (siehe http://diepresse.com/home/panorama/wien/590669/index.do).

begründeter Verdacht von gerichtlich zu verfolgenden Straftaten ...

Diese Fallkonstellationen sind (i) Übermittlung der Daten an die zuständige Behörde oder das zuständige Gericht, weil **beim Auftraggeber** der *begründete Verdacht* entstanden ist, die Daten könnten eine von Amts wegen zu verfolgende gerichtlich strafbare Handlung dokumentieren, oder (ii) an Sicherheitsbehörden zur Ausübung der diesen durch § 53 Abs 5 Sicherheitspolizeigesetz (SPG) eingeräumten Befugnisse.

... für Laien oft nicht leicht einzuschätzen

Die Erläuterungen verweisen beim „begründeten Verdacht" auf objektiv nachvollziehbare Tatsachen, wonach die gefilmten Ereignisse im Zusammenhang mit einer *von Amts wegen zu verfolgenden, gerichtlich strafbaren Handlung* stehen könnten; ebenso erlaubt wäre die Herausgabe der Daten, wenn die Behörde diese gem. § 53 Abs 5 SPG verwenden darf. Schon hier wird der **erste** (und m.E. bedeutendste) **Problembereich** sichtbar: wie soll der durchschnittliche Normunterworfene hier das richtige Vorgehen verlässlich beurteilen können, nämlich die strafgerichtliche Relevanz eines Verhaltens[113] oder gar die sicherheitspolizeilichen Befugnisse richtig einschätzen?[114] Immerhin trägt der Auftraggeber hier allein die Verantwortung für die Zulässigkeit der Datenweitergabe.[115]

Beweismittel aus unzulässigen Videoüberwachungen?

Der **zweite Problembereich** ist die potentielle Gefahr der Förderung der Vorlage von Zufallstreffern (Beweismittel) bei Gerichten und Sicherheitsbehörden, die aus unzulässigen Videoüberwachungen stammen.[116] Darauf hat auch schon die Österr. Richtervereinigung aufmerksam gemacht und einen konkreten Vorschlag zur Entschärfung dieser Situation gemacht.[117] Der Datenschutzrat hat die Schaffung einer Beweisverwertungsbeschränkung für zweckentfremdete Videoaufzeichnungen angeregt.[118] Die Bundesarbeitskammer hat gleich explizit ein Beweisverwertungsgebot für unzulässige Videoaufzeichnungen gefordert.[119]

---

[113] bspw. das strafrechtlich unbedenkliche Inbetriebnehmen eines Kfz im alkoholisierten Zustand.

[114] vgl. dazu auch die Stellungnahme des BMJ zur DSG-Novelle 2010 (http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00062_47/imfname_161898.pdf); dieses weist auf die Gefahr der missbräuchlichen Verwendung der Videoaufzeichnungen hin; vom durchschnittlichen Normadressaten können nicht erwartet werden, dass er erkennen kann, ob ein „begründeter Verdacht" einer strafbaren Handlung besteht. Auf Grund dieses wohl weit auszulegenden Begriffes könnten an sich unzulässige Videoaufnahmen durch eine unangebrachte Strafanzeige „legitimiert" und gegen bestimmte Personen verwendet werden."

[115] nur bei der Herausgabe von Beweismaterial an Behörden und Gerichte aufgrund bspw. gesetzlicher Herausgabepflichten (bspw. Anordnung der Sicherstellung durch die Staatsanwaltschaft) trägt die Behörde/das Gericht die alleinige Verantwortung (wie auch in den Erläuterungen zu § 50a Abs 6 DSG 2000 zutreffend erwähnt).

[116] siehe dazu auch Pollirer/Weiss/Knyrim, DSG (2010), MANZ-Sonderausgabe, Anmerkung 12) zu § 50 a.

[117] in ihrer Stellungnahme (http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00062_45/index.shtml) schlägt sie folgende Wortfolge vor:"... *dann nicht verletzt, wenn durch eine gemäß den Abs 2 bis 4 durchgeführte Videoaufzeichnung aufgezeichnete Daten über ihren ursprünglichen gesetzlichen Verwendungszweck hinaus in folgenden Fällen übermittelt werden* ..." → eine sehr passende Formulierung.

[118] siehe die Stellungnahme des DSR zur DSG-Novelle 2010 (http://www.oesterreich.gv.at/DocView.axd?CobId=36118), dies zur Vermeidung einerseits der systematischen Mitarbeiterüberwachung und um andererseits legitime Überwachungsbedürfnisse in bestimmten Branchen befriedigen zu können.

[119] siehe die Stellungnahme der Bundesarbeitskammer vom 10.06.2009 (http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00062_49/imfname_162386.pdf), Seite 3.

Dritter Problembereich ist die Frage, **wer** den begründeten Verdacht haben muss. Der Gesetzestext nennt ausdrücklich den Auftraggeber; die Erläuterungen führen aus, dass ein solcher Verdacht aber regelmäßig durch einen entsprechenden Hinweis eines Dritten entstehen wird. Im Ergebnis ist also an Fälle zu denken, in denen ein Vorgang für den Auftraggeber völlig verdachtsfrei ist (bspw. die gefilmte Aufgabe einer Paketsendung in der Postfiliale), er von der Behörde aber das Ersuchen um Herausgabe dieser Videosequenz erhält, da die betreffende Person im (strafrechtlich relevanten) Verdacht steht, Diebesgut per Paket versendet zu haben). ME kann ein solches Ersuchen nicht (nachträglich?) einen wie auch immer gearteten begründeten Verdacht beim Auftraggeber entstehen lassen, weshalb die Formulierung des § 50a Abs 6 Zif 1 DSG 2000 jedenfalls i.S. der Erläuterungen geändert werden müsste, um dieser grundsätzlich zweckmäßigen Bestimmung den richtigen Anwendungsbereich zu geben.

Verdacht durch Hinweise von Dritten?

4.6.3 Kennzeichnungspflicht ... das Ende der verdeckten Überwachung

Durch die sehr begrüßenswerte Bestimmung des § 50d DSG 2000 ist die verdeckte Videoüberwachung durch Private endgültig Geschichte. Der Auftraggeber einer Videoüberwachung hat diese nunmehr geeignet zu kennzeichnen; aus dieser Kennzeichnung (regelmäßig gut sichtbare Aufkleber/Hinweisschilder/Piktogramm etc.) hat auch der Auftraggeber eindeutig hervorzugehen (das Gesetz regelt hier nichts Näheres, sodass neben dem Namen des Auftraggebers bspw. auch die Angabe der DVR-Nr. denkbar ist).

verdeckte Videoüberwachung nicht zulässig

Die Kennzeichnung hat örtlich derart zu erfolgen, dass jeder potentiell Betroffene, der sich einem überwachten Objekt oder einer überwachten Person nähert, tunlichst die Möglichkeit hat, der Videoüberwachung auszuweichen.

Diese Kennzeichnungspflicht besteht unabhängig davon, ob es sich um eine Echtzeitüberwachung oder um eine solche handelt, bei der die Speicherung nur auf analogen Medien erfolgt.

Kennzeichnungspflicht obligatorisch

Ausgenommen sind Videoüberwachungen im Rahmen der Vollziehung hoheitlicher Aufgaben.

hoheitliche Überwachungen sind ausgenommen

4.6.4 ... und wenn nichts passiert ... Wann sind Videoaufnahmen zu löschen?

Gem. § 50b Abs 2 DSG 2000 sind die Aufnahmen spätestens nach 72 Stunden zu löschen, wenn die Daten *„nicht aus konkretem Anlass für die Verwirklichung der zu Grunde liegenden Schutz- und Beweissicherung oder für Zwecke der Herausgabe an die Behörde bei „Zufallstreffern" benötigt werden*."

generelle Löschungspflicht, außer bei konkretem Anlass zur Auswertung, 72 Stunden ab dem Zeitpunkt der Aufnahme

Der Beginn dieser 72 Stunden ist mit dem Zeitpunkt der Aufnahme (nicht etwa mit dem Zeitpunkt, an dem die Aufnahme erstmals tatsächlich betrachtet wird) anzusetzen; das Ende mit Ablauf der 72h ab Aufnahmezeitpunkt. Vielfach in der Literatur kritisiert wurde der Umstand der zu kurzen (ursprünglich überhaupt nur 48 Stunden langen) Speicherdauer. Diese wird sowohl durch Verweis auf die Geltung des § 33 Abs 2 AVG (bei Fristende am Samstag, Sonntag, gesetzlichen Feiertag oder Karfreitag verlängert sich das Fristende bis zum nächsten Werktag) und der Möglichkeit, eine längere Aufbewahrungsdauer in der Meldung an die DSK anzuführen und zu begründen entschärft.

Fraglich ist das Vorgehen, wenn innerhalb der 72 Stunden bspw. ein Behördenersuchen von der unzuständigen Behörde oder in der falschen Form kommt; m.E. reicht hier allein das Einlangen eines auf die Herausgabe von „Zufallstreffern" gerichteten Schreibens, um die Daten auch über die 72 Stunden hinaus aufzubewahren (bis zum Einlangen eines richtiggestellten" Behördenersuchens).

Aufbewahrungspflicht bei Auskunftsersuchen

Bei Auskunftsersuchen dürfen Daten gem. § 26 Abs 7 DSG 2000 ab Kenntnis vom Auskunftserlangen zumindest innerhalb eines Zeitraums von 4 Monaten nicht gelöscht werden; im Gesetz findet sich kein Hinweis, dass dies bei Auskünften zu Videoüberwachungen anders sein sollte. Es stellt sich vor dem Hintergrund der Speicherfrist von 72 Stunden aber das praktische Problem, dass im Einzelfall (etwa wenn sich das Auskunftsersuchen auf einen Zeitpunkt knapp vor Ablauf der 72 Stunden bezieht) die zu beauskunftenden Daten vielleicht schon gelöscht sind.

4.6.5 Auskunftsrecht

Kopie oder Einsichtnahme

Dieses ist bei der Videoüberwachung in § 50e DSG 2000 besonders geregelt und grundsätzlich durch (i) Übersenden einer Kopie der zur Person des Betroffenen verarbeiteten Daten in einem üblichen technischen Format oder (ii) Einsichtnahme auf einem Lesegerät (samt Anspruch auf Ausfolgung einer Kopie) zu gewähren.

schutzwürdige Geheimhaltungsinteressen Dritter

Da bei einer solchen Beauskunftung regelmäßig eine Vielzahl Dritter in ihren schutzwürdigen Geheimhaltungsinteressen beeinträchtigt sein kann, wurde für den Fall überwiegender Interessen Dritter vorgesehen, dass der Auskunftswerber Anspruch auf eine *schriftliche Beschreibung* seines von der Überwachung verarbeiteten Verhaltens oder auf eine Auskunft unter Unkenntlichmachung der anderen Personen hat.

Ein praktischer Fall eines ähnlich geregelten Auskunftsrechts war bereits Gegenstand eines Films einer österreichischen Filmschaffenden.[120]

kein Auskunftsrecht wenn Rechte anderer beeinträchtigt werden?

Um hier den nötigen Ausgleich zwischen Auskunftsanspruch des Betroffenen und den sonst von einer solchen Auskunft beeinträchtigten Dritten zu schaffen, hat die DSK schon bislang die Auffassung vertreten, dass, solange der Auftraggeber die gespeicherten Daten nicht auswertet, dem Betroffenen kein Auskunftsrecht zustünde. Diesen Standpunkt hat die DSK auch in ihrer Stellungnahme zur DSG-Novelle 2010 mE überzeugend beibehalten: demnach würde nämlich die Auskunft aus Videoüberwachungsdaten schon deshalb die Rechte anderer Betroffener unverhältnismäßig beeinträchtigen, „*... weil quasi „künstlich" ein Anlassfall für eine Auswertung erzeugt wird, wogegen bei Nicht-Erteilung der Auskunft die Daten aller Beteiligten geheim geblieben und innerhalb kürzester Frist – in den Anlassfällen waren es 48 Stunden – gelöscht worden wären*.". Diesen Rechtsstandpunkt hat die DSK in ihrem Bescheid vom

[120] „Faceless – Die Jagd nach dem Datenschatten" (http://cba.fro.at/show.php?eintrag_id=7911), der ohne Kamera auskam und nur aus den Videosequenzen bestand, die die Filmemacherin Manu Luksch aufgrund ihrer Auskunftsersuchen erhielt.

30. 7. 2010, GZ: K121.605/0014-DSK/2010[121] (der erste gem. der Rechtslage der DSG-Novelle 2010), aufrecht erhalten; die Entscheidung über die dagegen erhobenen Beschwerde an den Verwaltungsgerichtshof bleibt abzuwarten.

4.6.6 Lückenlose Protokollierung

generelle Pflicht zur Protokollierung von Verwendungen

Jeder Verwendungsvorgang einer Videoüberwachung (mit Ausnahme der Echtzeitüberwachung) ist zu protokollieren. Diese Pflicht besteht gem. den Erläuterungen auch bei Standardanwendungen; somit auch bei der zwischenzeitig per Verordnung in Kraft gesetzten SA 032 (siehe oben 4.6.1).

4.6.7 Verbot des Abgleichs von Videodaten mit sonstigen Bilddaten

Verbot von automatisierten Auswertungen

Gem. § 50a Abs 7 DSG 2000 dürfen mit einer Videoüberwachung gewonnene Daten von Betroffenen nicht automationsunterstützt mit anderen Bilddaten abgeglichen und nicht nach sensiblen Daten als Auswahlkriterium durchsucht werden. Gem. den Erläuterungen zu dieser Bestimmung soll damit insbesondere die automatisierte Suche nach „unerwünschten Personen“ ausgeschlossen werden (Diskriminierungsgefahr). Damit wird aber auch die automatisierte Suche nach „gewünschten Personen“ verhindert.[122] Eine praktikable Lösung wäre hier die von der Wirtschaftskammer Österreich vorgeschlagene „Genehmigungspflicht“ an Stelle des ausnahmslosen Verbotes.[123]

---

[121] der Beschwerdeführer hatte bei der ÖBB Personenverkehr AG als Auftraggeberin ein Auskunftsbegehren gemäß §§ 26 Abs. 1 und 50e Abs. 1 DSG 2000 mit der Begründung gestellt, er sei am Vortrag in einem Nahverkehrstriebwagenzug der Auftraggeberin Betroffener einer Videoüberwachung gewesen. Das Auskunftsbegehren wurde hinsichtlich der begehrten Übersendung einer Kopie der Videodatei mit Begründung abgelehnt, es sei keine Auswertung der Videodaten im näher bezeichneten Zug erfolgt.

[122] siehe dazu kritisch *Pollirer/Weiss/Knyrim*, DSG (2010), MANZ-Sonderausgabe, Anmerkung 13) zu § 50 a und die dort aufgezählten Datenanwendungen, die diese Bestimmung zukünftig ausschließen würde, bspw. „Zutrittskontrollsystem durch Gesichtserkennung, das in hochsicherheitskritischen Bereichen installiert ist (Flughäfen etc.)“.

[123] siehe dazu die Stellungnahme der WKÖ zur DSG-Novelle 2010 vom 12.06.2009 (http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00062_24/imfname_161495.pdf).

4.7 Zusammenfassung von Schwachstellen und offenen Regelungsbereichen der DSG-Novelle 2010 im Bereich der Videoüberwachung durch Private

keine abschließende Regelung

Gleich vorweg: die DSG-Novelle 2010 erhebt bewusst nicht den Anspruch, die Videoüberwachung Privater „abschließend" zu regeln. Da jede Videoüberwachung in die Persönlichkeitsrechte eines Menschen hineinspielt, verweist sie ganz bewusst auf die Geltung auch der Persönlichkeitsrechte des § 16 ABGB. Die nunmehrige ausdrückliche gesetzliche Regelung der Videoüberwachung ist aus Datenschutzsicht zwar zu begrüßen; bei näherer Betrachtung werden aber doch einige durchaus bedeutende Regelungsdefizite deutlich, die eine Überarbeitung angebracht erscheinen lassen.

Aus den oben gemachten Ausführungen lassen sich insbesondere folgende Schwachstellen und offenen Regelungsbereiche herausarbeiten:

4.7.1 Fehlende Richtlinienkonformität

nicht gedeckter Vorbehalt

Allgemeine Verfügbarkeit von Daten: das Grundrecht auf Datenschutz ist in § 1 Abs 1 DSG 2000 festgeschrieben; dort wird das jedermann zustehende Recht auf Geheimhaltung der ihn betreffenden personenbezogenen Daten aber nur auf die Fälle beschränkt, in denen an diesen Daten ein *schutzwürdiges Interesse* besteht; dieses wäre ausgeschlossen, wenn Daten infolge ihrer (nicht näher definierten) ***allgemeinen Verfügbarkeit*** einem Geheimhaltungsanspruch nicht zugänglich wären. Dieser „Vorbehalt" ist – wie oben in Punkt 4.4.2 gezeigt – durch die Datenschutz-RL (DS-RL) nicht gedeckt und widerspricht inhaltlich auch einer aktuellen Entscheidung des EUGH zur Weiterverwendung öffentlich gemachter Steuerdaten durch Private.[124]

unpräzis formulierte Ausnahmen

Diese Problematik ist nicht neu und nicht erst durch die Bestimmungen der DSG-Novelle 2010 zur Videoüberwachung schlagend geworden; diese Problematik hat sich durch diese Bestimmungen (konkret § 50a Abs 3 Zif 2 DSG 2000) aber insoweit verschärft, als nunmehr auch die Verarbeitung von Daten über ein Verhalten, „*das ohne jeden Zweifel den Schluss zulässt, dass es darauf gerichtet war, öffentlich wahrgenommen zu werden*" vom Schutzbereich des Grundrechts ausgenommen wurde. Wenn der Gesetzgeber schon vermeint, auch bei der Videoüberwachung *allgemein verfügbare* (iS. nicht dem Datenschutz unterliegende) Bereiche ausgemacht zu haben, dann wäre der Rechtssicherheit mehr gedient gewesen, die besagte Regelung so präzise zu fassen, dass Missverständnisse erst gar nicht aufkommen können bzw. eine solche Regelung erst gar nicht zu erlassen. Überhaupt passt eine solche Ausnahme auch überhaupt nicht zu *potentiell sensiblen* Daten einer Videoüberwachung; immerhin sucht man auch bei den taxativen Ausnahmen zulässiger Verwendung von sensiblen Daten[125] gem. § 9 DSG 2000 vergeblich einen solchen Ausnahmetatbestand.

---

[124] siehe EuGH in seinem Urteil vom 16.12.2008, C-73/07.

[125] Videodaten werden ja zumindest als *potentiell sensibel* eingestuft.

Schließlich wurde hier auch die Chance nicht ergriffen, die unterschiedlichen Arten der „Öffentlichkeit“[126] auch im Sinne einer Annäherung an die vorliegende Rechtsprechung des EUGH durchzuführen.

größerer Schutz betroffener Personen wünschenswert

Gerade bei der mit einer Videoüberwachung verbundenen hohen Eingriffsintensivität wäre ein größerer Schutz der davon betroffenen Personen wünschenswert gewesen. Keinesfalls darf diese Gesetzeslage dazu führen, dass die Teilnahme am öffentlichen Leben damit „bestraft“ wird, seiner Persönlichkeitsrechte in bestimmten Fällen verlustig zu gehen; noch dazu ohne dass es der betreffenden Person in den meisten Fällen auch nur ansatzweise bewusst ist.

Privilegierung der Echtzeitüberwachung

Auch die **Privilegierung der Echtzeitüberwachung bei „Eigenschutz“** (auch hier werden nach Ansicht des Gesetzgebers keine schutzwürdigen Geheimhaltungsinteressen verletzt) sowie die Ausnahme von der Meldepflicht sowohl bei (jeder Form von) Echtzeitüberwachung und generell bei Videoüberwachungen, soweit die Speicherung auf analogen Medien erfolgt, ist europarechtlich – da in der RL 95/46 nicht vorgesehen – nicht zu rechtfertigen.[127]

Zumindest die Richtlinienkonformität hat vorrangiges Ziel speziell bei neu dem Datenschutz hinzugefügter Regelungen zu sein.

4.7.2 Nur ansatzweise Berücksichtigung des technischen Datenschutzes

Vorgaben fehlen weitgehend

Wie in Punkt 4.5.1 oben ausgeführt, blieben die zahlreichen Hinweise in diese Richtung vorerst ungehört. Bislang erkennbare Ausnahme ist die ausdrückliche Vorgabe einer „verschlüsselten Videoüberwachung“[128] in der neu erlassenen Standardanwendung „SA032 Videoüberwachung“.

Privacy by design als Maß für „gelinderes Mittel“

Die bislang fehlende Bevorzugung datenschutzfreundlicher Technologien ist zwar zugegebenermaßen legistisch (nicht zuletzt aufgrund der sich ständig weiterentwickelnden Technik) nur schwer umzusetzen; es spricht m.E. aber nichts dagegen, solche Technologien in weiterer Folge als Maßstab für den Einsatz „gelinderer Mittel“ zu berücksichtigen und diesen damit indirekt zum Durchbruch zu verhelfen. Eine konkrete datenschutzrechtliche „Förderung“ solcher Technologien wäre jedenfalls die bevorzugte Behandlung von IT-Produkten und IT-Services, die bspw. mit einem Europäischen Datenschutzgütesiegel ausgestattet sind.

---

[126] siehe die oben in Punkt 4.2 angeführte Unterscheidung zwischen spontaner Gesprächsöffentlichkeit, Versammlungsöffentlichkeit, massenmedialer Öffentlichkeit und deren höchste Ebene, der Online-Öffentlichkeit.

[127] Diese „Privilegierungen“ sind nicht zu verwechseln mit den durch die Standardverordnung SA032 Videoüberwachung neu geschaffenen Ausnahmen von der Meldepflicht für bestimmte Videoüberwachungen.

[128] mit einer Ausnahme, nämlich der Videoüberwachung in Zusammenhang bebauten Privatgrundstücken.

4.7.3 Verwendung unbestimmter und bestimmter (mit neuem Verständnis) Gesetzesbegriffe und überbordender widersprüchlicher erläuternder Bemerkungen

„bestimmte Tatsachen"

Hier sticht insbesondere die zentrale Regelung des § 50a Abs 4 Zif 1 DSG 2000 hervor; wie oben in Punkt 4.3 ausgeführt, ist für die Aufzählung taxativer Ausnahmen zulässiger Videoüberwachungen die Verwendung des (im Gesetzestext nicht näher bestimmten) Begriffs des Vorliegens „***bestimmter Tatsachen***" völlig ungeeignet. Hier wären – wie auch sonst im Umgang mit sensiblen Daten üblich – möglichst konkrete Ausnahmen zu regeln, die den Normunterworfenen eine klare Vorgabe geben, was zulässig ist und was nicht. Genau diese konkreten Ausnahmen in den Erläuterungen zu „verstecken"[129], die zwar eine willkommene Auslegungshilfe bilden, aber selbst keinerlei Gesetzeskraft haben, ist überhaupt völlig unverständlich und erschwert die korrekte Rechtsanwendung für den Norm-Rechtsunterworfenen unnötig. Dass im Registrierungsverfahren bei Erstattung der Meldung diese bestimmten Tatsachen „glaubhaft" zu machen sind, hilft auch nicht so recht weiter; schließlich kann im Rahmen des § 50a Abs 4 Zif 1 DSG 2000 auch eine präventive Videoüberwachung zulässig sein.

widersprüchliche Erläuterungen

Schließlich, immer noch § 50a Abs 4 Zif 1 DSG 2000 betreffend, die Verwendung des aus dem Sicherheitspolizeigesetz (SPG) bestens vertrauten und dort auch legaldefinierten Begriff des „***gefährlichen Angriffs***";[130] dieser wird nun im DSG 2000 gem. den Erläuterungen „eigenständig" (und abweichend vom SPG) „geschaffen". Spätestens jetzt wird das Gesetz für den Durchschnittsmenschen nicht mehr les- und verstehbar. Überhaupt stellt sich die Frage, inwieweit diese Erläuterungen überhaupt zu berücksichtigen sind, da sie teilweise mehr zur Verwirrung beitragen und widersprüchlich sind. So wird für den gefährlichen Angriff festgehalten, dass es sich um eine „*Bedrohung mit strafbaren Vorsatztaten"* (was so dem Gesetzestext nicht entnehmbar ist) handeln muss ... um ein paar Sätze später davon zu sprechen, dass darunter „*auch die konkrete Gefahr einer groben Verwaltungsübertretung*" fallen kann.

Generell finden sich in den Erläuterungen überdurchschnittlich viele wichtige Ausführungen, um den Gesetzestext überhaupt praktisch anwendbar zu machen.

4.7.4 Punktuelle Probleme

Hier sollen abschließend nur mehr kurz einige Anmerkungen zu sonstigen Problembereichen erfolgen.

fehlende Berücksichtigung von „Social Networks"

Ohne gleich eine „Lex Facebook" zu schaffen, wäre jedenfalls eine generelle Berücksichtigung der diversen Möglichkeiten von **Web 2.0-Anwendungen** wie Social-Networks (Facebook, YouTube etc.) und der damit verbundenen datenschutzrechtlichen Problemstellungen wünschenswert.[131] Dass die Gesetzgebung der technischen Entwicklung regelmäßig (wenn auch nicht freiwillig)

---

[129] die in der RV der DSG-Novelle 2008 noch dazu noch Teil des Gesetzestextes waren.

[130] siehe § 16 SPG.

[131] siehe dazu auch den aktuellen Vorschlag des deutschen Bundesinnenministers zur Verbesserung des Persönlichkeitsschutzes im Internet, wonach im Internet keine persönlichen Daten in „ehrverletzender Weise" verwendet werden dürften, ohne dass der Betroffene zugestimmt habe (Süddeutsche Zeitung vom 01.12.2010, http://jetzt.sueddeutsche.de/texte/anzeigen/515499).

hinterherhinkt ist bekannt; unabhängig davon werden aber die das DSG vollziehenden Behörden mit diesen Entwicklungen über kurz oder lang konfrontiert werden; sei es zwecks Abklärung allfälliger „Meldepflichten" von fleißigen (Privat-)Video Uploadern oder dem Ausloten des Bereichs der *privaten Nutzung* von Videodaten gem. § 45 DSG 2000.

Unklarheiten bei Zufallstreffern

Weiters die Problematik der nun zulässigen Herausgabe von „**Zufallstreffern**", die gleich drei Fragen aufwirft, nämlich (i) die m.E. unzulässige Verschiebung der Verantwortung für die Zulässigkeit der Datenweitergabe an den durchschnittlichen Normunterworfenen, dem regelmäßig die nötigen Rechtskenntnisse zur verlässlichen Beurteilung des jeweils gefilmten „verdächtigen" Verhaltens fehlen wird; weiters (ii) die Gefahr der Förderung der Datenweitergabe aus unzulässigen Videoüberwachungen und (iii) der schwer aufzulösende Widerspruch zwischen Gesetzestext (*beim Auftraggeber* entstandenen begründeten Verdacht) und den Erläuterungen (wonach dieser begründete Verdacht durch Hinweis von Dritten entstehen würde).

nicht anwendbares Auskunftsrecht

Schließlich das zwar auf den ersten Blick datenschutzfreundlich gelöste **Auskunftsrecht**, dass sich bei näherer Betrachtung aber doch – soweit die Videodaten sonst gar nicht ausgewertet würden – durchaus als Eigentor erweist.

unzureichender Strafrahmen

Abschließend ist noch der Punkte „**Strafe**" zu behandeln. Abgesehen von dem gerichtlich strafbaren Tatbestand des § 51 DSG 2000 sind es doch die Verwaltungsstrafen gem. § 52 DSG 2000, die hier zum Zug kommen. Derzeit beträgt die höchstmögliche Verwaltungsstrafe bis zu EUR 25.000,00. Zum Vergleich: die derzeitige Verwaltungsstrafe gem. dem Telekommunikationsgesetz für das Versenden unerbetener mails (Spamming) beträgt gem. § 109 Abs 3 Zif 20 TKG bis zu EUR 37.000,00(!). Welcher von beiden Eingriffen schwerer wiegt, die unzulässige Videoüberwachung (und damit die Verletzung eines Grundrechts) oder der (bloße) Erhalt eines Werbe-Mails, braucht hier nicht näher erläutert zu werden. Nicht ohne Grund hat auch die DSK unter Berufung auf eine kürzlich ergangene Studie selbst darauf aufmerksam gemacht, dass der Strafrahmen in Österreich weit unter jenen anderer Staaten liegt.[132]

[132] siehe dazu die Stellungnahme der DSK zur DSG-Novelle 2010, letzter Absatz (http://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00062_57/imfname_164857.pdf); teilnehmende Länder waren: NL, B, F, D, Lux und Ö.

5 Schlussfolgerungen und Politikempfehlungen

Einschränkung auf Videoüberwachung i.e.S. lässt zentrale Bereiche von Bild- und Videodaten ungeregelt

Die explizite Regelung der Videoüberwachung durch die Novellierung des Datenschutzgesetzes 2000 ist grundsätzlich ein sehr positiver und wichtiger Schritt, auf die stetig steigenden technischen Möglichkeiten der Überwachung und auf politisch-gesellschaftliche Trends, diese auch exzessiv zu nutzen, zu reagieren und zu versuchen, bei dieser Entwicklung auch dem Recht auf Wahrung der Privatsphäre einen entsprechenden Platz einzuräumen. Gleichzeitig wird damit aber auch deutlich, wie schwierig es geworden ist, Regelungen zu entwerfen, die gleichzeitig Grundrechte wirksam schützen können, in die alltägliche Praxis umsetzbar sind und auch tatsächlich Anwendung finden können. Hier tritt insbesondere die Einschränkung auf „systematische" Videoüberwachung hervor, da neben dieser insbesondere ad hoc Aufnahmen etwa mittels Handy und der Publikation der Aufnahmen in Social Networks ein zunehmendes Problem bezüglich der Privatsphäre der gefilmten darstellt. Neben den vielen legistischen Detailproblemen (siehe Abschnitt 4.7), welche durch diese Novelle teilweise gelöst oder auch neu aufgeworfen werden und die in diesem Bericht beschrieben und diskutiert werden, wird offensichtlich, dass eine Reihe von fundamentalen Fragen aufgeworfen werden, die mit dem gegenwärtigen Instrumentarium nicht oder nur schwer zu lösen sind.

technische Entwicklung schafft neuen Bedarf zum Schutz der Privatsphäre

So wird etwa mit der Etablierung einer Standardvideoüberwachung eine administrative Erleichterung für weithin verbreitete und anerkannte Anwendungen mit einer entsprechenden Entlastung der Behörde geschaffen, eine wirksame Stärkung des Rechts auf Privatsphäre ist damit aber nicht verbunden. Allein die technischen Entwicklungen führen dazu, dass die Grenzen zwischen Videoüberwachung und Videoaufzeichnung verschwimmen, dass diese mobil und jederzeit durchgeführt werden können, dass Echtzeitüberwachungen in der Regel mühelos mit Aufzeichnungen ergänzt werden können, oder dass Aufzeichnungen zu privaten Zwecken in Zeiten von Social Networks und Internetplattformen ihre vermeintliche Privatheit weitgehend verlieren. Gerade diese privaten Anwendungen, seien es Aufzeichnungen mit mitgeführten Geräten oder Überwachungseinrichtungen für private Wohnungen oder Grundstücke, sind normalerweise mit zusätzlichen Tonaufzeichnungsmöglichkeiten ausgestattet, welche auch mit einer neuen Qualität der Eingriffstiefe in die Privatsphäre einhergehen.

Balance zwischen überschießenden Einschränkungen und unzureichendem Schutz von grundlegenden Persönlichkeitsrechten

Hier stellt sich die grundsätzliche Frage, inwiefern, notwendigerweise nachhinkende, detaillierte Regelungen für spezifische Tatbestände gefunden werden können oder ob nicht der Rechtsschutz stärker in Richtung Verwendung der Daten bzw. Persönlichkeitsrechte auszubauen sein wird. Die gegenwärtigen Regelungen laufen jedenfalls Gefahr, einerseits überschießende Einschränkungen vorzusehen, wenn etwa Wetterkameras als kritische Anwendungen zu sehen sind, andererseits etwa keine konkreten, durchsetzbaren Bestimmungen für die Verbreitung von verletzenden oder diskriminierenden Privataufnahmen auf Internetplattformen zu beinhalten. Ein wichtiges Kriterium bei zukünftigen Reformen zum Schutz von Daten und der Privatsphäre wird es sein, den Schutz von Grundrechten nicht von deren (einfachen) Durchsetzbarkeit abhängig zu machen. Gesetze und Durchführungsbestimmungen, welche Anwendungen mit geringem Gefahrenpotenzial und allgemeiner Akzeptanz einschränken oder verbieten, etwa das Beispiel von Wetterkameras auf Skipisten, die Verbreitung von diskriminierenden Aufzeichnungen im Internet zwar ebenfalls als illegal erachten, aber keine konkrete Hilfestellung für Betroffene zur Durchsetzung ihrer Rechte bereitstellen, sind in diesem Sinne nicht hilfreich.

Entkoppelung von technischer Entwicklung und dem Schutz von Rechten

Notwendig sind gesetzliche Regelwerke, welche zwar technische Entwicklungen nicht ignorieren, aber stärker auf die zu schützenden Rechte ausgerichtet sind, um nicht bei jeder Innovation reformiert werden zu müssen und damit zwangsläufig der technischen Entwicklung hinterherzulaufen sowie die technischen Möglichkeiten im positiven Sinn zum Datenschutz nutzen, auch hier ohne detaillierte Vorgaben, aber mit dem Ziel, den jeweiligen Stand der Technik auch beim Datenschutz garantieren.

In der folgenden Darstellung (siehe Seite 41)wird versucht, darzustellen, was nach derzeitiger Rechtslage im Bereich Videoüberwachung erlaubt bzw. verboten ist.

Empfehlungen an die Politik

Um über die Regelung des DSG 2000 hinaus der weiteren Erosion des Grundrechts auf Privatsphäre durch Videoüberwachungen Einhalt zu gebieten, erscheinen insbesondere die folgenden Maßnahmen erforderlich:

Bewusstseinsbildung bei allen AnwenderInnen, dass Bildaufnahmen jedenfalls eine Eingriff in die Privatsphäre des/r Betroffenen bedeuten und möglichst restriktiv eingesetzt werden sollten.

Reale Chancen auf Durchsetzung der Verhältnismäßigkeit durch Verpflichtung der NutzerInnen von Videosystemen, den Nachweis der Notwendigkeit und Verhältnismäßigkeit zu erbringen und Ausstattung von DSK/DSR mit entsprechenden Mitteln, dies auch überprüfen zu können.

Förderung des „technischen Datenschutzes“ durch avancierte Mindestregelungen und bevorzugte Genehmigung von datenschutzgerechten Systemen.

Förderung von Datenschutzgütesiegeln und von Anwendungen, die sich externer Zertifizierung unterziehen.

Stärkung der Rechte von Betroffen und bessere Durchsetzbarkeit von Ansprüchen bei Verletzung der Privatsphäre.

Veröffentlichung von Bilddaten im Internet

Neben den Videoüberwachungen in eigentlichen Sinn sind die Aufzeichnung und Veröffentlichung von Bild- und Videodaten, die nicht systematisch und dauerhaft erfasst werden, ein Bereich, der einer effektiveren Regulierung und besseren Schutzes der Grundrechte der Betroffenen bedarf. Auch hier werden die genannten Maßnahmen zur Bewusstseinsbildung und Verbesserung bei der Durchsetzbarkeit von Persönlichkeitsrechten und Schadenersatzforderungen eine unverzichtbare Rolle spielen. Angesichts der weitgehend fehlenden Transparenz bei der Weiterverbreitung von einmal hochgeladenen Daten und der praktischen Unmöglichkeit, diese Daten wieder tatsächlich und umfassend zu löschen, ist eine striktere Durchsetzung der Einholung des ausdrücklichen Einverständnisses der Betroffenen unumgänglich.

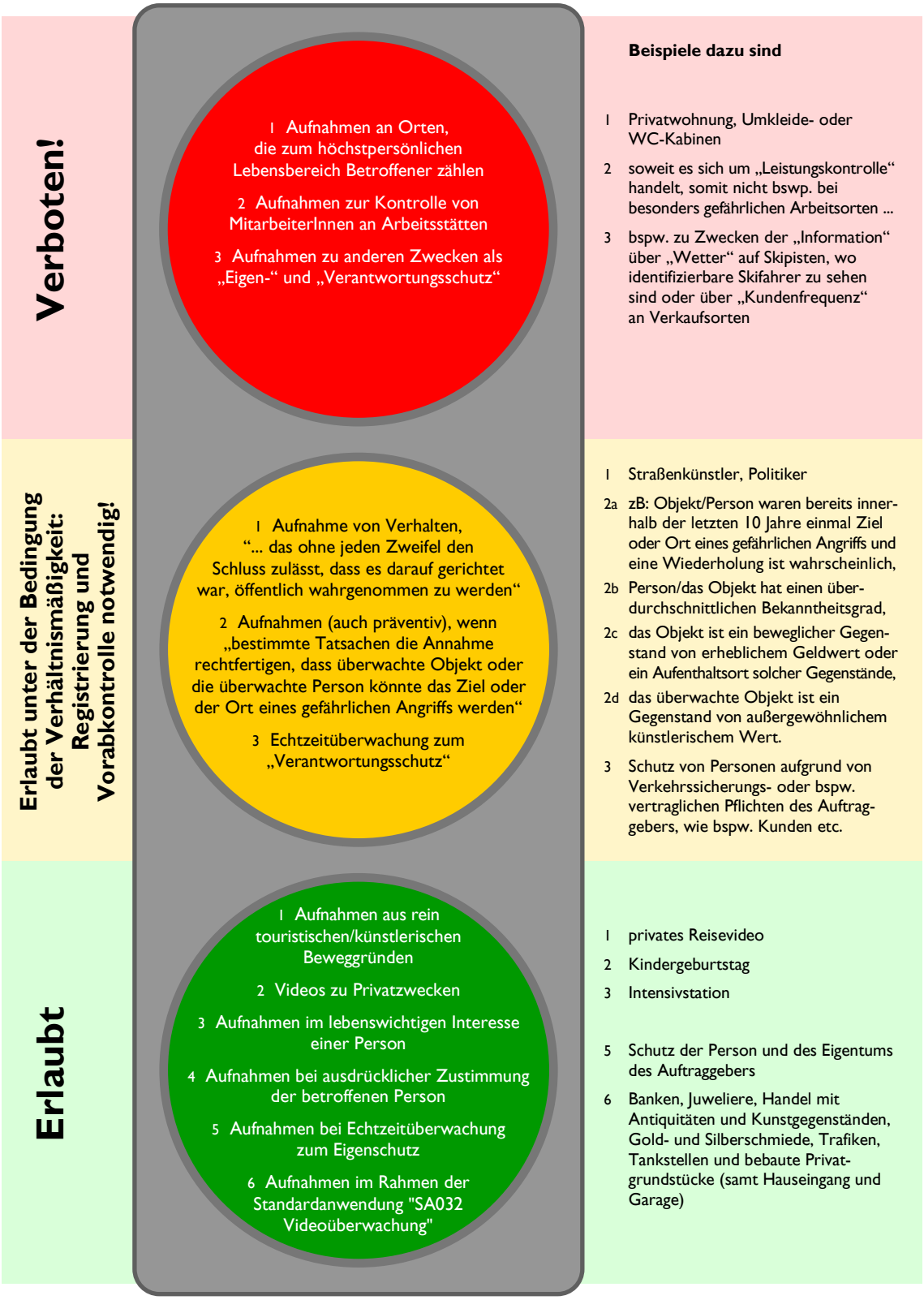

Abbildung 1: Videoüberwachung aus der Sicht des Gesetzgebers

6 Literatur

Allwinger, K. und Joshi M.A. Schillhab, 2008, Vertrauen der ÖsterreicherInnen in den Datenschutz, Juli 2008, Baden: ökonsult <http://www.oekonsult.eu/datensicherheit2008.pdf>.

BVerfGE, 1983, BVerfGE 65, 1 – Volkszählung, Urteil des Ersten Senats vom 15. Dezember 1983 auf die mündliche Verhandlung vom 18. und 19. Oktober 1983 – 1 BvR 209, 269, 362, 420, 440, 484/83 in den Verfahren über die Verfassungsbeschwerden, in: BVerfGE <http://www.oefre.unibe.ch/law/dfr/bv065001.html auch http://www.datenschutz-berlin.de/gesetze/sonstige/volksz.htm>.

Bornewasser, Manfred, 2005, Evaluation der Videoüberwachung: Ein Praxisbericht. Ergebnisse einer wissenschaftlichen Begleituntersuchung. In: Hempel, Leon/Metelmann, Jörg (Hg.): Bild – Raum – Kontrolle. Videoüberwachung als Zeichen gesellschaftlichen Wandels. Frankfurt, S. 235 – 272.

Bornewasser, Manfred; Schulz, Franziska, 2007, Systematische Videoüberwachung am Beispiel einer Maßnahme in Brandenburg. In: Bücking, Hans-Jörg (Hrsg.) Polizeiliche Videoüberwachung öffentlicher Räume. Duncker & Humblot. Berlin. S. 75.

Bücking, Hans-Jörg, 2007, Polizeiliche Videoüberwachung öffentlicher Räume. Duncker &Humblot. Berlin.

Cook, Thomas D.; Campbell, Donald T., 1979, Quasi-Experimentation: Design and Analysis for Field Settings. Chicago, Illionois: Rand McNally.

Ditton, Jason, 2000, Crime and the City. Public Attitudes towards Open-Street CCTV in Glasgow, in: British Journal of Criminology, Vol. 40, pp.692-709.

EDPS, 2010, Leitlinie des europäischen Datenschutzbeauftragten zur Videoüberwachung. Brüssel, 17. März 2010. (http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Supervision/Guidelines/10-03-17_Video-surveillance_Guidelines_DE.pdf)

Eifler, Stefanie; Brandt Daniela, 2005, Videoüberwachung in Deutschland. Theorie und Praxis situationsbezogener Kriminalprävention. In: Monatsschrift für Kriminologie und Strafrechtsreform. 88. Jahrgang, Heft 3. S. 158 – 173.

Elsbergen, G. v., 2007, Kriminologische Implikationen der Videoüberwachung, in: Zurawski, N. (Hg.): Surveillance Studies Perspektiven eines Forschungsfeldes, Opladen: Verlag Barbara Budrich, 103-115.

Foucault, M., 1994, Überwachen und Strafen. Die Geburt des Gefängnisses, Frankfurt/Main: Suhrkamp.

Garland, David, 2001, The Culture of Control. Crime and Social Order in Contemporary Society. Oxford University Press.

Gill, Martin; Spriggs, Angela, 2005, „Assessing the impact of CCTV“ Home Office Research Study 292. Home Office Research, Development and Statistics Directorate.

Gras, Marianne, 2005, Überwachung und Aufklärung durch Kameras. In: Northoff, Robert (Hrsg.) 1997 – 2007, Handbuch der Kriminalprävention. Fortsetzungswerk in Losblattform. Nomos Verlagsgesellschaft, Baden – Baden. Kapitel: 4.2.1.

Hempel, Leon; Töpfer, Eric, 2004, On the Threshold to Urban Panopticon? Analysing the Employment of CCTV in Eurpopean Cities and Assessing its Social and Political Impacts. Berlin.

Hempel, Leon; Metelmann, Jörg, 2005, Bild – Raum – Kontrolle. Videoüberwachung als Zeichen gesellschaftlichen Wandels. Frankfurt am Main: Suhrkamp.

Hempel, L., 2007, Zur Evaluation von Videoüberwachung – Methoden, Standards und Beispiele aus der Bewertungspraxis, in: Zurawski, N. (Hg.): Surveillance Studies Perspektiven eines Forschungsfeldes, Opladen: Verlag Barbara Budrich, 117-147.

Hempel, Leon, 2007, Zwischen globalem Trend und nationaler Varianz, Videoüberwachung in Europa. In: Bücking, Hans-Jörg (Hrsg.) Polizeiliche Videoüberwachung öffentlicher Räume. Duncker & Humblot. Berlin. S. 13.

Jørgensen, Vibeke, 2005, Der besorgte Blick der Eltern. Sozialpsychologie der Kameraüberwachung in Kindergärten. In: Hempel, Leon; Metelmann, Jörg (Hrsg.) Bild-Raum- Kontrolle. Suhrkamp.S.204.

König, G., 2007, Videoüberwachung und Datenschutz – Ein Kräftemessen, in: Jahnel, D., Siegwart, S. und Fercher, N. (Hg.): Aktuelle Fragen des Datenschutzrechts, Wien: facultas.wuv, XXX-147.

König, Robert, 2001, Videoüberwachung. Fakten, Rechtslage und Ethik. Mit dem Schwerpunkt auf generalpräventiver Videoüberwachung im öffentlichen Raum. Verlag Österreich, Wien.

Kunnert, Gerhard, 2006, Big Brother in U-Bahn, Bus und Bim. Video-aufzeichnung in öffentlichen Verkehrsmitteln aus datenschutzrechtlicher Sicht. Wien, Juridicum. (Ausgabe 2006/1) S. 42 – 50.

Marx, G. T., 1998, Ethics for the New Surveillance, The Information Society 14(3), 171-185 <http://www.slis.indiana.edu/TIS/abstracts/ab14-3/marx.html>.

Müller, Henning Ernst, 2002, Zur Kriminologie der Videoüberwachung. Monatsschrift für Kriminologie und Strafrechtsreform. H 1; S. 34.

Nogala, D., 2000, Der Frosch im heißen Wasser. Wie in der informatisierten Gesellschaft des 21. Jahrhunderts Überwachung trivialisiert wird, in: Schulzki-Haddouti, C. (Hg.): Vom Ende der Anonymität. Die Globalisierung der Überwachung, Hannover: Heinz Heise, 139-155.

Norris, C. und McCahill, M., 2006, CCTV: Beyond Penal Modernism, British Journal of Criminology, 97-118.

Peissl, W., 2005, Überwachung und Sicherheit – eine fragwürdige Beziehung, in: Nentwich, M. und Peissl, W. (Hg.): Technikfolgenabschätzung in der österreichischen Praxis Festschrift für Gunther Tichy, Wien: Verlag der Österreichischen Akademie der Wissenschaften, 73-90.

Peissl, Walter, 2007, Wie (Video-)Überwachung unser Leben Verändert. In: Reiter, Michael; Wittmann-Tiewald, Maria (Hrsg.): Goodbye Privacy-Grundrechte in der digitalen Welt. Internationales Symposium veranstaltet von der Fachgruppe Grundrechte in der Vereinigung österreichischer Richterinnen und Richter in Kooperation mit der Ars Electronica Linz.Linde Verlag Wien. S. 133- 139.

Rathenau Institute, 2002, Declaration of Amsterdam, Debating Privacy and ICT, January 17, Amsterdam.

Rothmann, Robert, 2009, Videoüberwachung als Instrument der Kriminalprävention. Eine quantitative Analyse von Akzeptanz und Sicherheitsgefühl auf ausgesuchten Wiener Kriminalitätsbrennpunkten. Masterarbeit. Wien.

Rothmann, Robert, 2010, Sicherheitsgefühl durch Videoüberwachung? Argumentative Paradoxien und empirische Widersprüche in der Verbreitung einer sicherheitspolitischen Maßnahme In: Neue Kriminalpolitik 2010/3, S. 103 – 107.

Sherman, Lawrence W.; Farrington, David P.; Welsh, Brandon C.; MacKenzie, Doris Layton, 2002, Evidence Based Crime Prevention. Routledge.

Töpfer, E., 2007, Videoüberwachung – Eine Risikotechnologie zwischen Sicherheitsversprechen und Kontrolldystopien, in: Zurawski, N. (Hg.): Surveillance Studies Perspektiven eines Forschungsfeldes, Opladen: Verlag Barbara Budrich, 33-46.

Wehrheim, Jahn, 2002, Die überwachte Stadt. Sicherheit, Segregation und Ausgrenzung. Leske & Budrich, Opladen.

Welsh, Brandon C./Farrington, David P., 2002, Crime prevention effects of closed circuit television: a systematic review. Home Office Research, Development and Statistic Directorate. London.