ARTIKEL 29 Datenschutzgruppe

11750/02/DE
WP 89

Stellungnahme 4/2004 zum Thema Verarbeitung personenbezogener Daten aus der Videoüberwachung

Angenommen am 11. Februar 2004

DIE GRUPPE FÜR DEN SCHUTZ DER RECHTE VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN,

eingesetzt durch Richtlinie 95/46/EG des Europäischen Parlaments und des Europäischen Rates vom 24. Oktober 1995[1],

gestützt auf Artikel 29 und Artikel 30 Absatz 1 Buchstabe a) und Absatz 3 jener Richtlinie,

gemäß den Verfahrensregeln jener Richtlinie und insbesondere der Artikel 12 und 14

HAT FOLGENDE STELLUNGNAHME ANGENOMMEN:

1. VORWORT

In den vergangenen Jahren wurden in Europa von öffentlichen und privaten Einrichtungen immer häufiger Bildaufzeichnungssysteme (Videorecorder) eingesetzt. Dieser Sachverhalt hat auf Gemeinschaftsebene und in den einzelnen Mitgliedstaaten zu einer lebhaften Diskussion über die Voraussetzungen und Einschränkungen für die Aufstellung von Anlagen für die Videoüberwachung sowie über die notwendigen Schutzvorkehrungen für die Betroffenen geführt.

Die Erfahrungen der vergangenen Jahre - auch im Anschluss an die Umsetzung der Richtlinie 95/46/EG in einzelstaatliches Recht - haben gezeigt, dass interne Fernsehüberwachungsanlagen, Kameras und noch raffiniertere Überwachungsinstrumente in den unterschiedlichsten Bereichen bereits weit verbreitet sind.

Ferner erweitert die Entwicklung marktgängiger Technologien, der Digitalisierung und der Miniaturisierung in erheblichem Maße die Möglichkeiten der Bild- und Tonaufzeichnungsgeräte, zumal im Zusammenhang mit ihrer Verbreitung über interne Netze oder das Internet.

Über den Einsatz bei Arbeitsprozessen hinaus, der von der Arbeitsgruppe bereits ausführlich behandelt wurde (*Stellungnahme 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten*[2]), kann die zunehmende Verbreitung der Videoüberwachungstechniken leicht von jedem Bürger festgestellt werden. Ferner besteht zunehmend die Tendenz, Videoüberwachungssysteme miteinander zu verknüpfen.

---

1 Amtsblatt L 281 vom 23.11.1995, S. 31, abrufbar unter: http://europa.eu.int/comm/internal_market/de/dataprot/index.htm

2 Arbeitsdokument 48, angenommen am 13. September 2001, abrufbar unter: http://europa.eu.int/comm/internal_market/de/dataprot/wpdocs/index.htm

Eine nicht erschöpfende Untersuchung der wichtigsten Anwendungen[3] zeigt, dass die Videoüberwachung ganz unterschiedlichen Zwecken dienen kann, die sich allerdings in einige wenige Kategorien zusammenfassen lassen:

1) Schutz von Einzelpersonen,
2) Schutz von Eigentum,
3) öffentliches Interesse,
4) Ermittlung, Verhütung und Verfolgung von Straftaten,
5) Beweissicherung,
6) sonstige berechtigte Interessen.

Verschiedene Bedingungen gelten auch für die Installation von Videokameras und vergleichbaren Geräten. In einigen wenigen Fällen kann der Einsatz von Videorecordern aufgrund besonderer Vorschriften der Mitgliedstaaten sogar zwingend geboten sein - so etwa in Spielkasinos -, oder aber er dient einem Zweck, dem die Verwandten der Betroffenen besonderes Gewicht beimessen - z. B. im Zusammenhang mit der Suche nach vermissten Kindern oder erwachsenen Angehörigen. Andererseits lassen sich auch ausgefallene Beispiele für solche Verwendungen - meist in Drittstaaten - aufführen: etwa Gesichtserkennungssysteme, um Bigamie zu verhindern oder die Entscheidung einer örtlichen Polizeibehörde, ohne Einwilligung der (Gefängnis-)Insassen Bilder über ihr hartes Leben im Gefängnis zu veröffentlichen.

Während also eine Videoüberwachung unter bestimmten Umständen irgendwie gerechtfertigt erscheint, gibt es auch Fälle, in denen spontan an einen Schutz durch Videokameras gedacht wird, ohne jedoch die einschlägigen Bedingungen und

---

3 Es sind verschiedene Videoüberwachungssysteme in Gebrauch:
- a) innerhalb und in der Nähe von öffentlichen oder öffentlich zugänglichen Gebäuden wie Museen, Gotteshäuser oder Denkmäler, um Straftaten oder Formen von Vandalismus zu verhindern;
- b) in Stadien oder Sporteinrichtungen, insbesondere im Zusammenhang mit bestimmten Veranstaltungen;
- c) in Beförderungseinrichtungen und im Zusammenhang mit dem Straßenverkehr zur Überwachung des Verkehrs auf Autobahnen und Schnellstraßen, oder zur Kontrolle von Geschwindigkeitsübertretungen oder Verstößen gegen die Straßenverkehrsordnung in Städten, zur Überwachung der Zugangseinrichtungen zu den Untergrundbahnen, der Tankstellen und der Fahrgasträume in Taxis;
- d) zur Vermeidung oder zur Ermittlung von gesetzwidrigen Verhaltensweisen in der Umgebung von Schulen, etwa im Zusammenhang mit Annäherungsversuchen an Minderjährige;
- e) in medizinischen Einrichtungen bei operativen Eingriffen oder zum Zweck der Fernbetreuung oder Beobachtung von Patienten auf Intensivstationen oder in Bereichen, in denen schwerkranke Patienten oder Personen in Quarantäne untergebracht sind;
- f) auf Flughäfen, auf Schiffen und in grenznahen Bereichen zur Unterbindung des Personenschmuggels oder zur Suche von als vermisst gemeldeten Minderjährigen und sonstigen Personen;
- g) bei Privatdetektiven,
- h) innerhalb oder in der Nähe von Supermärkten und Geschäften, vor allem in solchen, die Luxusgüter verkaufen, um im Falle von Straftaten Beweise liefern zu können, wie auch zum Zweck der Vermarktung von Waren oder der Profilerstellung über Verbraucher;
- i) im Umkreis von Wohnanlagen mit Eigentumswohnungen (Kondominien) aus Sicherheitsgründen oder zum Zwecke der Beweiserhebung im Falle von Straftaten;
- j) für journalistische Zwecke oder Werbezwecke, entweder über Webcams oder Online-Kameras, die für die Tourismusförderung oder Werbung eingesetzt werden, etwa im Zusammenhang mit Strandeinrichtungen und Tanzlokalen, wo Kunden und Besucher ohne vorherige Unterrichtung in regelmäßigen Abständen gefilmt werden.

Modalitäten angemessen zu erwägen. Dies hat zuweilen seinen Grund in den großen wirtschaftlichen Vorteilen, die sich für öffentliche Einrichtungen ergeben, wie etwa bessere Versicherungskonditionen bei der Verwendung von Videoüberwachungsgeräten.

Auch gibt es im Zusammenhang mit der Videoüberwachung einen psychologischen Faktor, der sie in der öffentlichen Meinung zuweilen, berechtigt oder nicht, als "unschätzbares Instrument" erscheinen lässt, das für die Aufdeckung von Straftaten nützlich ist.

Es handelt sich also um einen vielseitigen, ständig sich weiter entwickelnden Bereich, in dem bereits verschiedene Techniken verfügbar sind.

Ausgehend von teilweise unterschiedlichen Verordnungen und Regelungen wie auch von zuweilen äußerst detaillierten Bestimmungen in einzelstaatlichen Gesetzen, die einen systematischeren und aufeinander abgestimmten Ansatz erforderlich machen, soll das vorliegende Arbeitsdokument eine erste Analyse bieten.

In dem Arbeitsdokument wird auf sämtliche Überwachungsformen eingegangen, die eine Fernüberwachung von Veranstaltungen, Situationen und Vorkommnissen zum Zweck haben, dagegen nicht unmittelbar auf solche Arten, bei denen bestimmte Veranstaltungen gelegentlich oder bei bestimmten Gelegenheiten veröffentlicht werden, etwa im Zusammenhang mit dem Transparenzgebot für die Tätigkeiten von Kommunal-verwaltungen oder parlamentarischen Gremien.

Jeder Betreiber wird sodann in der Lage sein, die hier gelieferten Angaben weiter aufzuschlüsseln, sowohl nach den jeweiligen Bereichen als auch bezüglich der künftigen technologischen Entwicklungen, die von der Arbeitsgruppe untersucht werden sollen.

Die in diesem Arbeitsdokument behandelten Grundsätze gelten für die Aufzeichnung von Bildern, auch in Verbindung mit Tonaufzeichnungen oder biometrischen Daten wie etwa Fingerabdrücken[4].

Die genannten Grundsätze müssen, wo konkret anwendbar, auch in Verbindung mit der Verarbeitung personenbezogener Daten eingehalten werden, die nicht durch Videogeräte erfolgt, sondern durch andere Überwachungsformen, etwa Fernkontrollen durch Satelliten-gestützte GPS-Systeme.

Das Arbeitsdokument soll in erster Linie die Aufmerksamkeit auf den weiten Bereich von Kriterien für die Bewertung der Rechtmäßigkeit und Angemessenheit der Installation von personenbezogenen Videoüberwachungssystemen lenken.

Allerdings sind auch folgende Aspekte zu berücksichtigen:

a) Die zuständigen Behörden in den Mitgliedstaaten müssen die Videoüberwachung unter allgemeinen Gesichtspunkten beurteilen, d. h., auch im Hinblick darauf, dass sowohl ein allgemein selektives als auch systematisches Konzept für dieses Thema gefördert wird. Die starke Verbreitung von Bildaufzeichnungssystemen in

---

4 Die allgemeinere Frage der Anwendung der Richtlinie 95/46/EG auf biometrische Verfahren wird von der Arbeitsgruppe in einem separaten Dokument behandelt.

öffentlichen oder privaten Bereichen darf nicht zu einer ungerechtfertigten Einschränkung der Rechte und fundamentalen Freiheiten der Bürger führen; andernfalls könnten die Bürger gezwungen werden, sich unverhältnismäßigen Datenerhebungsverfahren zu unterwerfen, mit deren Hilfe sie an zahlreichen öffentlichen und privaten Orten eindeutig identifizierbar würden.

b) Es wäre zweckmäßig, die Trends bei der Entwicklung der Videoüberwachung zu bewerten, um zu verhindern, dass die Entwicklung von Softwareanwendungen zur Gesichtserkennung und Untersuchung und Prognose gefilmter menschlicher Verhaltensweisen zu einer rücksichtslosen dynamisch-präventiven Überwachung führen - im Unterschied zur konventionellen statischen Überwachung, mit der hauptsächlich besondere Ereignisse und ihre Urheber dokumentiert werden sollen. Neue Formen der Überwachung beinhalten die automatische Aufzeichnung der Gesichtszüge von Einzelpersonen sowie ihres "anomalen" Verhaltens in Verbindung mit automatischen Warnmeldungen und Befehlsaufforderungen; dies birgt die Gefahr von Diskriminierungen.

2. INTERNATIONALE RECHTSINSTRUMENTE

a) Europäische Konvention zum Schutz der Menschenrechte und Grundfreiheiten

Der Schutz der Privatsphäre ist in Artikel 8 der Konvention der Menschenrechte (EMRK) verankert.

b) Europarat: Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Konvention Nr. 108) vom 28. Januar 1981

Der Geltungsbereich dieser Konvention beschränkt sich nicht wie die Richtlinie 95/46/EG auf Tätigkeiten des ersten Pfeilers (siehe weiter unten). Vielmehr umfasst er auch die Videoüberwachung mit der Verarbeitung personenbezogener Daten. Der mit diesem Übereinkommen geschaffene Beratende Ausschuss hat erklärt, dass Stimmen und Bilder als personenbezogene Daten zu betrachten seien, wenn sie über Einzelpersonen in der Form Auskunft geben, dass sie identifizierbar werden, und sei es auch nur auf indirekte Weise.

Der Europarat steht kurz vor der Fertigstellung eines Pakets von Leitlinien zum Schutz von Personen im Hinblick auf die Sammlung und Verarbeitung von Daten durch Videoüberwachung. In diesen Leitlinien sollen die Schutzvorkehrungen für die Betroffenen weiter spezifiziert werden, die in den Bestimmungen der Instrumente des Europarats enthalten sind.

c) Charta der Grundrechte der Europäischen Union

In der Charta der Grundrechte der Europäischen Union ist in Artikel 7 der Schutz des Privat- und Familienlebens, der Wohnung und der Korrespondenz sowie in Artikel 8 der Schutz der personenbezogenen Daten verankert.

3. ÜBERWACHUNG GEMÄSS RICHTLINIE 95/46/EG

Die besonderen Aspekte der Verarbeitung personenbezogener Informationen aus Ton- und Bilddaten wurden in verschiedenen Abschnitten der Richtlinie 95/46/EG (nachstehend "Richtlinie" genannt) ausdrücklich betont.

Die Richtlinie gewährleistet den Schutz der Privatsphäre wie auch den umfassenderen Schutz der personenbezogenen Daten unter Bezugnahme auf die Grundrechte und Grundfreiheiten natürlicher Personen (Artikel 1 Absatz 1).

Ein erheblicher Teil der Informationen, die durch Videoüberwachung gesammelt werden, betrifft bestimmte oder bestimmbare Personen, die bei ihrem Aufenthalt in der Öffentlichkeit oder in öffentlich zugänglichen Gebäuden gefilmt wurden. Diese vorübergehenden Personen müssen zwar einen geringeren Grad an Privatheit erwarten, aber nicht, dass sie völlig ihrer Rechte und Freiheiten beraubt werden, was sich auch auf ihre Privatsphäre und die Bilder von ihnen bezieht.

Hier ist auch auf das Recht des Einzelnen auf Bewegungsfreiheit einzugehen, der sich auf dem Gebiet eines Staates rechtmäßig aufhält; dieses Recht ist in Artikel 2 des Zusatzprotokolls Nr. 4 der Europäischen Konvention zum Schutz der Menschenrechte und Grundfreiheiten verankert.

Diese Bewegungsfreiheit kann nur solchen Einschränkungen unterworfen sein, die in einer demokratischen Gesellschaft unerlässlich sind und für das Erreichen bestimmter Zwecke angemessen sind. Die Bürger haben ein Recht auf Bewegungsfreiheit ohne psychologische Konditionierung ihrer Bewegungen und Verhaltensweisen, wie auch darauf, keiner ausführlichen Überwachung durch einen unverhältnismäßigen Einsatz von Videoüberwachungen durch verschiedene Stellen in zahlreichen öffentlichen oder öffentlich zugänglichen Gebäuden unterworfen zu sein, wie etwa der Aufzeichnung ihrer Bewegungen und/oder die Auslösung von Alarm durch Softwareprogramme, die ohne irgendwelches menschliches Zutun eine vermutete verdächtige Verhaltensweise einer Person automatisch "interpretieren".

Die Besonderheit und Sensibilität der Verarbeitung personenbezogener Ton- und Bilddaten werden in den einleitenden Erwägungsgründen der Richtlinie thematisiert. Zusätzlich zu den Überlegungen weiter unten über den Geltungsbereich wird in diesen Erwägungsgründen und den entsprechenden Artikeln in der Richtlinie folgendes erläutert:

a) die Richtlinie findet in Anbetracht der Bedeutung der Entwicklung der Techniken der Erfassung, Veränderung und sonstigen Verwendung personenbezogener Daten grundsätzlich auch auf Ton- und Bilddaten Anwendung (Erwägungsgrund 14);

b) die Schutzprinzipien der Richtlinie müssen für alle Informationen - auch Ton- und Bilddaten - über eine bestimmte oder bestimmbare Person gelten, indem alle Mittel berücksichtigt werden, die von dem Verantwortlichen für die Verarbeitung oder von einem Dritten eingesetzt werden könnten, um die betreffende Person zu bestimmen (Artikel 2 Buchstabe a) und Erwägungsgrund 26).

Neben den vorgenannten spezifischen Bezügen entfaltet die Richtlinie ihre Wirkungen im Rahmen ihrer einzelnen Bestimmungen, die sich insbesondere auf folgende Punkte

beziehen:

1) *Datenqualität*. Bilder müssen nach Treu und Glauben und auf rechtmäßige Weise und für festgelegte eindeutige und rechtmäßige Zwecke verarbeitet werden. Bilder sind gemäß dem Grundsatz zu verwenden, dass sie den Zwecken entsprechen, für die sie erhoben oder weiterverarbeitet werden, dafür erheblich sind und nicht darüber hinausgehen, sowie dass sie in keiner mit diesen Zweckbestimmungen nicht zu vereinbarenden Weise weiterverarbeitet werden. Sie werden nur für einen begrenzten Zeitraum aufbewahrt usw. (siehe Artikel 6).

2) *Kriterien für die Rechtmäßigkeit der Datenverarbeitung*. Auf der Grundlage dieser Kriterien muss die Verarbeitung personenbezogener Daten durch Videoüberwachung mindestens eine der in Artikel 7 aufgeführten Voraussetzungen erfüllen: Einwilligung ohne jeden Zweifel, vertragliche Festlegung, Erfüllung einer rechtlichen Verpflichtung, Wahrung lebenswichtiger Interessen der betroffenen Person, Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt, ausgewogene Interessenabwägung (Artikel 7).

Formatted:

3) Die Verarbeitung *besonderer Kategorien von Daten;* sie unterliegt den Schutzbestimmungen, die im Rahmen der Videoüberwachung für die Verwendung sensitiver Daten oder für Daten gelten, die Straftaten betreffen (vgl. Artikel 8).

4) *Unterrichtung der Betroffenen* (siehe Artikel 10 und 11),

5) *Rechte der Betroffenen*, insbesondere Recht auf Zugang zu eigenen Daten und Widerspruchsrecht gegen die Datenverarbeitung aus schutzwürdigen Gründen (siehe Artikel 12 und 14a),

6) Schutzklauseln im Zusammenhang mit *automatisierten Einzelentscheidungen* (vgl. Artikel 15),

7) *Sicherheit* der Verarbeitung (Artikel 17),

8) *Meldung von Verarbeitungen* (vgl. Artikel 18 und 19),

9) *Vorabkontrolle* von Verarbeitungen, die spezifische Risiken für die Rechte und Freiheiten der Betroffenen beinhalten können (Artikel 20) und

10) *Übermittlung von Daten an Drittstaaten* (vgl. Artikel 25 und folgende).

Die Besonderheit und Sensibilität der Verarbeitung von Bild- und Tondaten wird schließlich auch im letzten Artikel der Richtlinie gewürdigt, wonach sich die Kommission verpflichtet, insbesondere die Anwendung dieser Richtlinie auf die Verarbeitung solcher Daten zu prüfen und alle geeigneten Vorschläge zu unterbreiten, die sich unter Berücksichtigung der Entwicklung der Informationstechnologie und der Arbeiten über die Informationsgesellschaft als notwendig erweisen könnten (siehe Artikel 33).

4. EINZELSTAATLICHE BESTIMMUNGEN FÜR DIE VIDEOÜBERWACHUNG

In verschiedenen Mitgliedstaaten wurden bereits Fallstudien zu Videoüberwachungen

durchgeführt, die entweder aufgrund verfassungsmäßiger Bestimmungen[5] oder spezifischer Rechtsvorschriften oder auf Anordnungen und sonstige Entscheidungen der zuständigen einzelstaatlichen Behörden hin erfolgten[6].

In einigen wenigen Staaten gibt es auch besondere Bestimmungen für die Videoüberwachung, unabhängig davon, ob sie der Verarbeitung personenbezogener Daten dient. Gemäß diesen Vorschriften müssen Installation und Einsatz von internen Fernsehüberwachungsanlagen und vergleichbaren Geräten vorher durch eine Behörde genehmigt werden, die insgesamt oder teilweise von der nationalen Datenschutzbehörde repräsentiert werden kann. Solche Bestimmungen können sich je nach dem öffentlichen oder privaten Charakter der Körperschaft, die für den Betrieb der entsprechenden Anlagen zuständig ist, voneinander unterscheiden.

In anderen Ländern wiederum ist die Videoüberwachung derzeit noch nicht Gegenstand besonderer Gesetze. Aber die Datenschutzbehörden arbeiten daran, eine angemessene Umsetzung der allgemeinen Datenschutzrichtlinie zu gewährleisten, unter anderem durch Stellungnahmen, Leitlinien oder Verhaltenskodizes, die beispielsweise im Vereinigten Königreich bereits angenommen wurden und in Italien derzeit entwickelt werden.

Belgien	Stellungnahmen der Datenschutzbehörde, insbesondere Stellungnahme Nr. 34/1999 vom 13. Dezember 1999 bezüglich der Verarbeitung von Bildern, insbesondere durch Videoüberwachungs-systeme; Nr. 3/2000 vom 10. Januar 2000 bezüglich der Verwendung von Videoüberwachungssystemen in Eingangsbereichen von Apartmenthäusern.

5 Siehe Entscheidung Nr. 255/2002 des portugiesischen Verfassungsgerichtshofes. Darin heißt es: "Der Einsatz elektronischer Überwachungseinrichtungen und die Überwachung von Bürgern durch private Sicherheitsdienste sind eine Einschränkung des Rechts auf Privatsphäre, das in Artikel 26 der Verfassung verankert ist".

6 Mindestens in einem Land (Belgien – Rechtssache Gaia), hat der Verstoß gegen die Datenschutzgesetze im Zusammenhang mit der Aufzeichnung von Bildern vor Gericht zu einer Nichtannahme der Beweise geführt.

Dänemark	Gesetz Nr. 76 vom 1. Februar 2000 bezüglich des Verbots der Videoüberwachung. Durch dieses Gesetz wird privaten Körperschaften generell verboten, auf öffentlichen Wegen, Straßen, Plätzen oder sonstigen vergleichbaren Arealen für öffentliche Fortbewegung, Videoüberwachungen vorzunehmen. Allerdings gibt es bestimmte Ausnahmen von diesem Verbot. Entscheidung der Datenschutzbehörde vom 3. Juni 2002 bezüglich der Videoüberwachung durch eine große Gruppe von Supermärkten und Liveübertragung aus einer Kneipe in das Internet. Nach der Entscheidung der Datenschutzbehörde vom 1. Juli 2003 muss die in privat betriebenen öffentlichen Verkehrsmitteln durchgeführte Videoüberwachung verhältnismäßig sein und den Vorschriften des dänischen Datenschutzgesetzes entsprechen. Entscheidungen der Datenschutzbehörde vom 13. November 2003, die der Videoüberwachung durch Behörden gewisse Beschränkungen auferlegen.
Finnland	In Finnland gibt es keine speziellen Gesetze zur Videoüberwachung, aber in vielen verschiedenen Rechtsvorschriften Bestimmungen zur Videoüberwachung und zu sonstigen technischen Überwachungen, Beobachtungen oder Kontrollen. Anfragen zur Videoüberwachung und zum Mitschnitt von Gesprächen sind häufig und es gab einige Entscheidungen dazu. So gab der Datenschutzbeauftragte seine Stellungnahme zum Mitschnitt von Telefongesprächen bei Kundendiensten und im Arbeitsleben ab (Protokoll 1061/45/2000 und 525/45/2000). Die Datenschutzbehörde hat eine Broschüre zum Thema "Datenschutz bei der Videoüberwachung" veröffentlicht (Asiaa tietosuojasta 4/2001 Yksityisyyden suoja kameravalvonnassa http://www.tietosuoja.fi/uploads/03wamgvxuybt4ti.rtf.)

Frankreich	Gesetz Nr. 78-17 vom 6. Januar 1978 über Verarbeitungen, Dateien und Freiheiten (CNIL). Empfehlung der Datenschutzbehörde Nr. 94-056 vom 21. Juni 1994. Leitlinien der Datenschutzbehörde zur Videoüberwachung am Arbeitsplatz (http://www.cnil.fr/thematic/index.htm) und zu anderen Fragen (z.B. Webcam)[7]. Sondergesetz bezüglich der Videoüberwachung zum Zweck der öffentlichen Sicherheit in öffentlichen Bereichen: Gesetz Nr. 95-73 vom 21. Januar 1995 zu Sicherheitsfragen (geändert durch Anordnung 2000-916 vom 19. September 2000). Verordnung Nr. 96-926 vom 17. Oktober 1996 und Rundschreiben vom 22. Oktober 1996 zur Durchführung des Gesetzes Nr. 95-73 (CNIL).
Griechenland	1) Schreiben der Datenschutzbehörde Nr. 390 vom 28. Januar 2000 zur Installation eines geschlossenen Videoüberwachungssystems in der Athener Untergrundbahn; 2) Direktive Nr. 1122 vom 26. September 2000 zu geschlossenen Videoüberwachungssystemen; 3) Entscheidung Nr. 84/2002 zu geschlossenen Videoüberwachungs-systemen in Hotels.
Deutschland	Paragraph 6 des Bundesdatenschutzgesetzes aus dem Jahre 2001. Paragraph 25 Bundesgrenzschutzgesetz. Verordnungen zur Videoüberwachung durch die Polizei in den Polizeigesetzen der einzelnen Bundesländer. Im Parlament wird ein Gesetz zum Verbot der verdeckten Videoüberwachung erörtert.
Irland	Datenschutzgesetz von 1998 und 2003. Fallstudie Nr. 14/1996 (Einsatz der Videoüberwachung).

7 Siehe Jahresberichte der französischen Datenschutzbehörde CNIL.

Italien	Paragraph 134 des Datenschutzgesetzes (Gesetzesverordnung Nr. 196 vom 30. Juni 2003 (Annahme eines Verhaltenskodex). Entscheidungen der Datenschutzbehörde Garante: Nr. 2 vom 10. April 2002 (Förderung der Annahme von Verhaltenskodizes), vom 28. September 2001 (biometrische und Gesichtserkennungsverfahren in Banken) und vom 29. November 2000 (so genannte "10 Gebote der Videoüberwachung"). Präsidialerlass Nr. 250 vom 22. Juni 1999 (Regelung des Zugangs von Fahrzeugen in die Stadtzentren und Bereiche für eingeschränkten Zugang). Verordnung Nr. 433 vom 14. November 1992 und Gesetz Nr. 4/1993 (gilt für Museen, staatliche Bibliotheken und Archive). Gesetzesverordnung Nr. 45 vom 4. April 2000 (Fahrgastschiffe auf nationalen Routen). Paragraph 4 des Gesetzes Nr. 300 vom 20. Mai 1970 (so genanntes Arbeitnehmerstatut).
Luxemburg	Artikel 10 und 11 des Gesetzes vom 2. August 2002 über den Schutz von Personen in Bezug auf die Verarbeitung personenbezogener Daten.
Niederlande	Der Bericht der Datenschutzbehörde von 1997 enthält Leitlinien für die Videoüberwachung, insbesondere für den Schutz von Personen und Eigentum an öffentlichen Plätzen. Im Jahr 2004 wird eine Aktualisierung der 1997 entwickelten Leitlinien erfolgen. Im Jahre 2003 wurde in sämtlichen niederländischen Kommunen eine Ermittlung der Videoüberwachungen durchgeführt. Änderung des Strafrechts zu seiner Ausweitung auf Aufnahmen von öffentlich zugänglichen Orten ohne Unterrichtung der Öffentlichkeit angenommen; sie gilt ab dem 1. Januar 2004. Die Regierung hat eine Änderung des Kommunalverwaltungsrechts vorgeschlagen, wonach den Stadträten und Bürgermeistern die ausschließliche Zuständigkeit für bestimmte Videoüberwachungen an öffentlichen Plätzen für öffentliche Zwecke und unter bestimmten Bedingungen zugewiesen wird (etwa die Auflage, die Wirksamkeit der Videoüberwachung regelmäßig zu überprüfen).

Portugal	Gesetzesverordnung 231/1998 vom 22. Juli 1998 (private Sicherheitsmaßnahmen und Selbstschutzsysteme). Gesetz 38/98 vom 4. August 1998 (Maßnahmen im Falle von Gewaltausbrüchen bei Sportveranstaltungen). Gesetzesverordnung 263/2001 vom 28. September 2001 (Tanzlokale). Gesetzesverordnung 94/2002 vom 12. April 2002 (Sportveranstaltungen).
Schweden	Die Videoüberwachung wird insbesondere im Gesetz (1998:150) über allgemeine Videoüberwachung (an öffentlichen Plätzen) und im Gesetz (1995:1506) über verdeckte Videoüberwachung (bei polizeilichen Ermittlungen) geregelt.[8] Die allgemeine Videoüberwachung setzt in der Regel die Genehmigung durch die Provinzialverwaltung voraus. Allerdings bedarf die Überwachung etwa von Postämtern, Banken und Geschäften keiner Genehmigung. Verdeckte Videoüberwachungen müssen von einem Gericht genehmigt werden. Entscheidungen der Provinzialverwaltung können vom Justizminister angefochten werden. Digitale Videoaufzeichnungen werden als Verarbeitung personenbezogener Daten betrachtet und fallen mithin unter die Aufsicht des Datenschutzamtes, sofern sie nicht speziell im Gesetz über die allgemeine Videoüberwachung geregelt werden. Eine Untersuchungskommission hat einen Bericht über die Videoüberwachungen vorgelegt (SOU 2002:110).
Spanien	Grundgesetz (Ley organica) Nr. 4/1997 (Videoüberwachung durch Sicherheitskräfte an öffentlichen Plätzen). Königlicher Erlass (Real Decreto) Nr. 596/1999 zur Durchführung des Gesetzes Nr. 4/1997.
Vereinigtes Königreich	Der Verhaltenskodex Videoüberwachung 2000 (Informations-beauftragter) wird gegenwärtig überarbeitet.

Weitere wichtige ordnungsrechtliche Instrumente wurden angenommen in Island (Gesetz

[8] In Schweden wird für eine allgemeine Videoüberwachung im Prinzip die Genehmigung der Provinzialverwaltung benötigt, aber es gibt eine Reihe von Ausnahmen, etwa bezüglich der Überwachung von Postämtern, Banken und Geschäften. Versteckte Videoüberwachung muss von einem Gericht genehmigt werden. Gemäß dem Gesetz über die allgemeine Videoüberwachung kann eine Entscheidung der Provinzialverwaltung vom Justizministerium im Interesse der öffentlichen Sicherheit angefochten werden. Videoaufzeichnungen mit Digitalkameras werden als eine Verarbeitung personenbezogener Daten gemäß dem schwedischen Datenschutzgesetz angesehen und fallen somit unter die Aufsicht der Datenschutzbehörde. Derzeit prüft eine Untersuchungskommission die Verwendung der Videoüberwachung zur Verbrechensvorbeugung. Unter anderem wird die Kommission das Gesetz über die allgemeine Videoüberwachung bewerten und prüfen, ob Änderungen erforderlich sind. Ferner prüft sie den Geltungsbereich des schwedischen Datenschutzgesetzes im Hinblick auf die Videoüberwachung und den möglichen Bedarf an besonderen Gesetzen für die Verarbeitung personenbezogener Daten im Zusammenhang mit der Videoüberwachung

Nr. 77/2000, Paragraph 4), in Norwegen (Gesetz Nr. 31 vom 14. April 2000, Titel VII), in der Schweiz (Empfehlung des Bundesbeauftragten für Datenschutz) und in Ungarn (Empfehlung der Datenschutzbehörde vom 20. Dezember 2000).

5. BEREICHE, FÜR WELCHE DIE RICHTLINIE 95/46/EG INSGESAMT ODER TEILWEISE NICHT GILT

Die Richtlinie gilt nicht für die Verarbeitung von Ton- und Bilddaten für Zwecke der öffentlichen Sicherheit, der Landesverteidigung, der Sicherheit des Staates oder der Tätigkeiten des Staates im Bereich des Strafrechts oder andere Tätigkeiten, die nicht unter das Gemeinschaftsrecht fallen[9]. Gleichwohl haben viele Mitgliedstaaten bei der Umsetzung der Richtlinie 95/46/EG auch solche Fragen in allgemeiner Form behandelt, dabei aber spezifische Ausnahmeregelungen vorgesehen.

A) In einigen wenigen Staaten unterliegen Datenverarbeitungen für die vorgenannten Zwecke auf jeden Fall den Schutzbestimmungen gemäß der Konvention des Europarates Nr. 108/1981 und seinen einschlägigen Empfehlungen sowie gemäß bestimmten innerstaatlichen Vorschriften (siehe Artikel 3 Absatz 2 und Erwägungsgrund Nr. 16 der Richtlinie 95/46/EG). Angesichts ihrer Besonderheiten und spezifischer Vorschriften im Zusammenhang mit Ermittlungen der Polizei- und Justizbehörden sowie zum Zwecke der Sicherheit des Staates[10] - was auch eine verdeckte Videoüberwachung bedeuten kann, also ohne Auskunft über die überwachten Örtlichkeiten - wird diese Kategorie von Datenverarbeitungen in diesem Arbeitsdokument nicht näher behandelt.

Aber die Arbeitsgruppe möchte unterstreichen, dass auch bei einer Videoüberwachung aufgrund konkreter öffentlicher Sicherheitserfordernisse oder zum Zwecke der Aufdeckung, Verhütung und Verfolgung von Straftaten, ähnlich wie bei verschiedenen anderen Verarbeitungen personenbezogener Daten, die ebenfalls nicht in den Geltungsbereich dieser Richtlinie fallen, die Vorschriften von Artikel 8 der Konvention zum Schutze der Menschenrechte und Grundfreiheiten eingehalten werden müssen, was in besonderen Bestimmungen in Verbindung und im angemessenen Verhältnis zu den *konkreten* Gefahren und *genau umrissenen* Straftaten öffentlich bekannt gemacht werden muss - zum Beispiel in Gebäuden, die solchen Gefahren ausgesetzt sind, oder im Zusammenhang mit öffentlichen Veranstaltungen, bei denen eine hohe Wahrscheinlichkeit besteht, dass es zu Straftaten kommt[11]. Auch die Folgen einer Videoüberwachung müssen mitbedacht werden - zum Beispiel, dass rechtswidrige Aktivitäten in andere Bereiche oder Sektoren abwandern; ferner müssen die für die Verarbeitung Verantwortlichen stets eindeutig benannt werden, damit die Betroffenen ihre Rechte wahrnehmen können.

Diese Bedingung hängt auch mit dem Umstand zusammen, dass die Videoüberwachung zunehmend mehr gemeinsam von Polizei und anderen staatlichen Stellen (etwa kommunalen Verwaltungen) oder privaten Einrichtungen

---

9 Siehe Erwägungsgrund Nr. 16.

10 Hier sei auf die Grundsätze verwiesen, die der Europäische Gerichtshof für Menschenrechte in seinem Urteil vom 4. Mai 2000 in der Rechtssache Rotaru vs. Rumänien aufgestellt hat.

11 Beispielsweise in Frankreich das Rundschreiben vom 22.10.1996, das sich auf abgelegene Plätze und Geschäfte bezieht, die sehr spät abends schließen.

(Banken, Sportvereinen, Verkehrsunternehmen) vorgenommen wird, was die Gefahr mit sich bringt, dass die Rollen und Zuständigkeiten der einzelnen Beteiligten in Bezug auf die auszuführenden Aufgaben verschleiert werden[12].

B) Zweitens gilt die Richtlinie nicht für Verarbeitungen, die von natürlichen Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten vorgenommen werden (siehe Artikel 3 Absatz 2 und Erwägungsgrund Nr. 12 der Richtlinie).

Während die vorgenannten Umstände etwa gelten können, wenn eine Videoüberwachung für die Fernkontrolle der Vorgänge innerhalb einer Wohnung eingesetzt wird - etwa um Einbrüche zu verhindern oder im Zusammenhang mit dem so genannten elektronischen Haushaltsmanagement -, gilt dies nicht, wenn Videoüberwachungsanlagen entweder außerhalb oder in der Nähe von privaten Gebäuden installiert werden, um Eigentum zu sichern oder Sicherheit zu gewährleisten.
In diesen Fällen dürften solche Systeme wohl nicht von einzelnen Eigentümern betrieben werden, wie dies etwa bei der Überwachung ihrer Haustüren der Fall wäre, sondern eher von verschiedenen Eigentümern auf der Grundlage einer Vereinbarung oder von einer Hauseigentümergemeinschaft, um verschiedene Eingänge und Bereiche eines Wohnblocks zu überwachen - für solche Maßnahmen würde die Richtlinie gelten.
Dass die Richtlinie bei ausschließlich persönlicher Verwendung und fehlendem Zugang Dritter zu den Daten nicht gilt, solange ein Überwachungssystem zum Nutzen einer einzigen Familie oder zur Überwachung einer einzelnen Tür, eines Landeplatzes oder eines Parkplatzes usw. eingesetzt wird, entbindet den für die Verarbeitung Verantwortlichen nicht davon, die legitimen Rechte und Interessen von Nachbarn oder Passanten zu achten. In den Mitgliedstaaten der Union werden diese Rechte und Interessen gegenwärtig unabhängig von den Datenschutzgrundsätzen durch das allgemeine bürgerliche Recht gewährleistet, mit denen persönlichen Rechte, Abbildungen, Familienleben und Privatsphäre geschützt werden; man denke etwa an das Bildfeld einer Kamera, die vor der Tür einer Etagenwohnung angebracht ist und eine systematische Aufzeichnung aller Patienten einer Arztpraxis oder Klienten einer Rechtsanwaltskanzlei gestattet, die sich auf demselben Korridor befindet; dies wäre ein gesetzwidriger Verstoß gegen das Berufsgeheimnis.

Es wird also besonders auf die Ausrichtung der Videogeräte zu achten sein, ferner auf die Notwendigkeit, Hinweise und Informationen anzubringen und die Bilder zügig - innerhalb weniger Stunden - wieder zu löschen, sofern kein Einbruchs- oder anderes Strafdelikt festgestellt wurde.

C) Schließlich lässt Artikel 9 der Richtlinie zu, dass die Mitgliedstaaten insbesondere

---

12 Eine erhebliche Gefahr liegt etwa in den Tätigkeiten einiger italienischer Kommunen, die per Videoüberwachung nachts Plätze beobachten, auf denen sich Prostituierte aufhalten. Verschiedene Kommunen haben in der Vergangenheit die - fragliche - Zuständigkeit für die Verhinderung der Prostitution geltend gemacht. Andere Gemeinden haben lediglich Anordnungen herausgegeben, wonach den Freiern untersagt wurde, in den betreffenden Vierteln zu parken oder zu fahren, und zwar unter der Androhung, bei Übertretungen entsprechende Fotografien an die Privatadresse zu senden. Die italienische Datenschutzbehörde hat diesbezüglich eine Entscheidung zur Klärung der angemessenen Modalitäten für eine Verfolgung der Übertretung der einschlägigen Bestimmungen getroffen.

im audiovisuellen Bereich (siehe Erwägungsgrund 17) für die Verarbeitung personenbezogener Daten, die allein zu journalistischen, künstlerischen oder literarischen Zwecken erfolgt, Abweichungen und Ausnahmen von einigen Bestimmungen der Richtlinie vorsehen, allerdings nur insofern sich dies als notwendig erweist, um das Recht auf Privatsphäre mit den für die Freiheit der Meinungsäußerung geltenden Bestimmungen in Einklang zu bringen[13]. In diesem Zusammenhang ist besonders bei der Aufstellung von Webcams oder Online-Kameras Sorgfalt walten zu lassen, damit keine Schwachpunkte und Lücken beim Schutz von Personen auftreten, die von einer Videobeobachtung für Werbezwecke oder zur Förderung des Fremdenverkehrs betroffen sind[14].

6. VIDEOÜBERWACHUNG UND VERARBEITUNG PERSONENBEZOGENER DATEN

In Anbetracht der verschiedenen erwähnten Situationen ist die Arbeitsgruppe der Meinung, dass auf den Sachverhalt aufmerksam gemacht werden muss, dass sich die Richtlinie 95/46/EG neben der Verarbeitung personenbezogener Daten auch auf die Sammlung von Bild- und Tondaten durch interne Fernsehüberwachungsanlagen und andere Videoüberwachungssysteme bezieht, die vollständig oder teilweise automatisch arbeiten, aber auch auf die nicht automatische Verarbeitung personenbezogener Daten, die Bestandteile von Datenbanken sind oder werden sollen.

Bild- und Tondateien, die sich auf bestimmte oder bestimmbare natürliche Personen beziehen, sind auch dann personenbezogene Daten,

a) wenn sie im Rahmen eines geschlossenen internen Systems verwendet und nicht mit den Personalien einer Person verknüpft werden,

b) wenn sie keine Personen betreffen, deren Gesicht gefilmt wurde, aber andere Informationen enthalten, zum Beispiel Nummernschilder oder PIN-Nummern, die in Verbindung mit der Überwachung von Geldautomaten gesammelt wurden, und zwar unabhängig
   - von den zur Verarbeitung verwendeten Medien - z.B. ortsfeste oder ortsveränderliche Videosysteme wie tragbare Videokameras für Farb- oder Schwarz-Weiß-Bilder;
   - vom benutzten Verfahren: Kabel- oder Glasfaserübertragung;
   - von der Art der Ausstattung - feststehend, umlaufend, oder ortsveränderlich;
   - von den Merkmalen der Bildaufzeichnung – z.B. kontinuierlich im Gegensatz zu diskontinuierlich, was der Fall sein kann, wenn Aufnahmen nur bei Übertretung einer Geschwindigkeitsbeschränkung gemacht werden und es sich nicht um Videoaufnahmen, sondern um fallweise, nicht systematisch aufgenommene Bilder handelt; und schließlich
   - von den Übertragungssystemen - ob also eine Verbindung mit einer zentralen Stelle besteht oder aber die Bilder zu dezentralen Terminals geschickt werden usw.

Formatted:

13 Siehe Empfehlung 1/97 der Arbeitsgruppe zum Datenschutzrecht in den Medien.

14 Eine Webkamera, die heimlich unterhalb eines Treppenaufgangs einer U-Bahn-Station in Mailand aufgestellt worden war, zeigte unmittelbar im Internet Bilder der intimen Bereiche der vorübergehenden Frauen, anscheinend bloß zu journalistischen Zwecken. Da die betroffenen Frauen nicht zu identifizieren waren, konnte die nationale Datenschutzbehörde keine Schritte dagegen unternehmen.

-

"Bestimmbarkeit" im Sinne der Richtlinie kann sich auch aus der Verknüpfung der Daten mit Informationen von Dritten ergeben, oder in den einzelnen Fällen aus der Anwendung bestimmter Techniken oder Verfahren.

Deshalb ist von den für die Daten Verantwortlichen als eine der ersten Maßnahmen zu prüfen, ob die Videoüberwachung die Verarbeitung personenbezogener Daten zur Folge hat, sich also auf bestimmbare Personen bezieht. Falls ja, dann gilt die Richtlinie ungeachtet nationaler Bestimmungen, die etwa darüber hinaus aus Gründen der öffentlichen Sicherheit eine Genehmigung vorschreiben.

Dies ist etwa bei einer Anlage der Fall, die sich entweder am Eingang oder in einer Bank befindet und die eine Identifizierung von Kunden möglich macht; andererseits kann unter bestimmten Umständen die Anwendbarkeit der Richtlinie auf Luftaufnahmen ausgeschlossen werden, die nicht hinreichend vergrößert werden können oder sonst keinerlei Informationen über natürliche Personen beinhalten - wie etwa Aufnahmen zur Ermittlung von Wasserquellen oder Abfalldeponien - oder auch auf Geräte, die großräumige Bilder vom Autobahnverkehr liefern.

7. PFLICHTEN UND GEEIGNETE VORKEHRUNGEN DER FÜR DIE DATEN VERANTWORTLICHEN

A) Rechtmäßigkeit der Verarbeitung

Auch im Hinblick auf die Vorschrift, dass eine Verarbeitung nur für rechtmäßige Zwecke erfolgen darf (vgl. Artikel 6 Buchstabe a) der Richtlinie), müssen die für die Daten Verantwortlichen vorweg prüfen, ob sich die Überwachung mit den allgemeinen und besonderen Vorschriften für den entsprechenden Bereich - Gesetze, Verordnungen, rechtlich verbindliche Verhaltenskodizes - in Einklang befindet. Solche Vorschriften können auch aus Gründen der öffentlichen Sicherheit oder aus Zwecken festgelegt werden, die sich nicht auf den Schutz personenbezogener Daten beziehen – zum Beispiel die Notwendigkeit, Ad-hoc-Genehmigungen durch spezifische Verwaltungsorgane zu erhalten und deren Anweisungen zu befolgen.

Es sind alle geeigneten Maßnahmen zu treffen, um sicherzustellen, dass die Videoüberwachung mit den Grundsätzen des Datenschutzes in Einklang steht und nicht gerechtfertigte Hinweise auf die Privatsphäre vermieden werden[15].

Diesbezüglich sind auch nachahmenswerte Verfahren zu berücksichtigen, die etwa in Empfehlungen der Aufsichtsbehörden oder Organen der Selbstkontrolle vorgelegt werden.

Ferner sind die übrigen Bestimmungen des innerstaatlichen Rechts zu prüfen - Verfassungsgrundsätze, Bestimmungen des Zivil- und Strafrechts - und insbesondere

15 Kürzlich konnten eine Bank und eine lokale Polizeidienststelle der Forderung eines Bankkunden nicht nachkommen - und zwar erklärtermaßen aus Gründen des Datenschutzes -, aus dem Film einer Kamera, die auch auf einen Geldautomaten gerichtet war, diejenigen Bilder zu extrahieren, die sich auf einen Dieb bezogen, der mit der Bankkarte des Kunden nach ihrer Entwendung unrechtmäßig Geld aus dem Geldautomaten abgehoben hatte.

solche, die sich auf das "Recht auf das eigene Bild"[16] oder die Unverletzlichkeit der Wohnung beziehen; es ist die einschlägige Rechtsprechung zu berücksichtigen, wonach etwa geurteilt wird, dass auch andere Einrichtungen als diejenigen, die sich auf eine Privatwohnung beziehen - Hotelzimmer, Büroräume, Aufenthaltsräume, Waschräume, hausinterne Telefonzellen usw. - als Privaträume zu betrachten sind.

Wo Anlagen entweder von Privatfirmen oder öffentlichen Stellen, vor allem Kommunalverwaltungen, erklärtermaßen zu Sicherheitszwecken oder zur Ermittlung, Verhütung und Verfolgung von Straftaten installiert werden, muss besondere Sorgfalt auf die Festlegung und Auskunftspflicht über solche Zwecke wie auch auf die Aufgaben verwendet werden, die von den für die Daten Verantwortlichen rechtmäßig auszuführen sind, da bestimmte öffentliche Aufgaben rechtmäßig nur von bestimmten nichtadministrativen Organen, vor allem Strafverfolgungsbehörden, wahrgenommen werden dürfen.

Dieses Problem trat insbesondere bei einigen Kommunalverwaltungen auf, die keine unmittelbare Zuständigkeit für Fragen der öffentlichen Sicherheit und Ordnung haben, aber bei Überwachungen subsidiäre Tätigkeiten ausführen. Ebenso werden Maßnahmen zur Überwachung von Delikten häufig auch zur Beweissicherung bei Straftaten herangezogen.

B) Besonderheiten, Präzisierung und Rechtmäßigkeit der Zwecke

Die für die Daten Verantwortlichen müssen sicherstellen, dass die verfolgten Zwecke weder unklar noch mehrdeutig sind, auch um genaue Kriterien an der Hand zu haben, wenn die Rechtmäßigkeit der durch die Datenverarbeitung verfolgten Zwecke zu beurteilen ist (siehe Artikel 6 Buchstabe b) der Richtlinie).

Eine solche Klarstellung ist auch im Hinblick auf die Angabe der Zwecke sowohl bei den Auskünften an die Betroffenen als auch bei der betreffenden Meldung erforderlich, aber auch im Zusammenhang mit den etwaigen Vorabprüfungen der Verarbeitung gemäß Artikel 20 der Richtlinie.

Es muss eindeutig ausgeschlossen werden, dass die aufgezeichneten Bilder - besonders im Hinblick auf die technischen Reproduktionsmöglichkeiten - zu weiteren Zwecken verwendet werden, etwa dadurch, dass die Anfertigung von Kopien ausdrücklich verboten wird.

Die relevanten Zwecke sind in einem Dokument aufzuführen, in dem auch andere wichtige Datenschutzaspekte zusammengefasst werden, etwa so wichtige Fragen wie die Angabe des Zeitpunkts der Löschung der Aufnahmen, etwaige Anträge von Betroffenen auf Zugang oder rechtmäßige Einsicht der Daten.

16 In Frankreich und Belgien beinhaltet dieses Recht die "vorherige Zustimmung".

C) Kriterien für die rechtmäßige Verarbeitung

Die für die Daten Verantwortlichen müssen nicht nur prüfen, ob die Videoüberwachung den besonderen Bestimmungen aus Abschnitt A), sondern auch mindestens einem der Kriterien entspricht, nach denen eine Verarbeitung gemäß Artikel 7 der Richtlinie rechtmäßig ist - insbesondere in Bezug auf den Schutz personenbezogener Daten.

Abgesehen von den eher seltenen Fällen, in denen eine gesetzliche Vorgabe zu befolgen ist - so wurde bereits auf Überwachungsmaßnahmen in Spielkasinos hingewiesen -, oder in denen eine Verarbeitung zum Schutze lebenswichtiger Interessen erforderlich ist, z. B. Fernüberwachung von Patienten auf Intensivstationen, müssen die für die Datenverarbeitung Verantwortlichen häufig Aufgaben im öffentlichen Interesse oder aufgrund der Tätigkeit einer staatlichen Stelle in Erfüllung bestimmter Verordnungen durchführen: z. B. Feststellung von Verkehrsübertretungen oder gewalttätigem Verhalten in öffentlichen Verkehrsmitteln in Bereichen mit hoher Kriminalität (vgl. Artikel 7 Buchstabe e) der Richtlinie). Oder die für die Verarbeitung Verantwortlichen können berechtigte Interessen wahrnehmen, sofern nicht das Interesse oder die Grundrechte und Grundfreiheiten der betroffenen Person überwiegen (siehe Artikel 7 Buchstabe f) der Richtlinie).

In beiden Fällen, aber vor allem im letzteren, verlangt der sensible Charakter der Verarbeitung vom für die Daten Verantwortlichen eine sorgfältige Beachtung des Aufgabenbereichs, der Befugnisse und der berechtigten Interessen. Leichtfertigkeit und ungerechtfertigte Erweiterungen dieser Aufgabenbereiche und Befugnisse bei der Verarbeitung sind absolut nicht gestattet.

Besonders im Hinblick auf die Abwägung der unterschiedlichen Interessen - auch durch eine vorherige Anhörung der Betroffenen - wird man besonders darauf Acht geben müssen, dass Konflikte zwischen einem schutzwürdigen Interesse und der Installation einer Anlage oder bestimmten Datenspeicherungsmodalitäten oder anderen Verarbeitungsvorgängen entstehen können[17].

Was schließlich die Zustimmung der Betroffenen angeht, so muss diese unzweideutig sein und auf präzisen Auskünften beruhen. Die Zustimmung muss einzeln und speziell für die Überwachungstätigkeiten eingeholt werden, die Wohngebäude betreffen, in denen sich das Privatleben der Betroffenen abspielt[18].

Die Rechtmäßigkeit der Verarbeitung ist ferner unter Berücksichtigung der Bestimmungen der Richtlinie zu prüfen, die besondere Schutzmaßnahmen für Daten vorsehen, die Straftaten betreffen (siehe Artikel 8 Absatz 5) der Richtlinie)[19].

---

17 Nach Paragraph 6b des neuen bundesdeutschen Datenschutzgesetzes, das am 23. Mai 2001 in Kraft trat, ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen zulässig, wenn - unter anderem - keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

18 Besonders ist darauf zu achten, dass bei der Installation von Videoüberwachungen in Wohnanlagen u.ä. die konkrete Möglichkeit einer gültigen Einwilligung im Sinne der Richtlinie 95/46/EG Artikel 2 Buchstabe h): "jede Willensbekundung, die ohne Zwang, für den konkreten Fall und in Kenntnis der Sachlage erfolgt und mit der die betroffene Person akzeptiert, dass personenbezogene Daten, die sie betreffen, verarbeitet werden") besteht.

19 Hier kann bezüglich der Daten von Personen, die der Teilnahme an illegalen oder kriminellen Aktivitäten verdächtigt werden, auf Paragraph 8 des portugiesischen Datenschutzgesetzes verwiesen

Zusätzliche Maßnahmen und Modalitäten können sich aus einer vorläufigen Beurteilung der Verarbeitungen in Einklang mit der Vorabkontrolle ergeben, wenn die Videoüberwachungen spezifische Risiken für die Rechte und Freiheiten der Personen beinhalten können (siehe Artikel 20 der Richtlinie 95/46/EG).

Verarbeitungen mit Hilfe der Videoüberwachung müssen immer auf ausdrückliche Rechtsvorschriften gestützt sein, wenn sie durch öffentliche Organe ausgeführt werden.

D) Verhältnismäßigkeit des Einsatzes der Videoüberwachung

Der Grundsatz, wonach Daten angemessen, notwendig und verhältnismäßig zu sein haben, bedeutet zunächst, dass interne Fernseh- und vergleichbare Videoüberwachungsanlagen nur zu Hilfszwecken eingesetzt werden dürfen, nämlich

zu Zwecken, die den Rückgriff auf derartige Systeme wirklich rechtfertigen.

Der Grundsatz der Verhältnismäßigkeit bedeutet, dass diese Systeme nur eingesetzt werden dürfen, wenn sich andere Vorsorge-, Schutz- und/oder Sicherheitsmaßnahmen physischer und/oder programmgesteuerter Art, die keine Bildaufnahmen erfordern - z. B. die Verwendung von Türen mit Sicherheitsbeschlägen zur Bekämpfung von Vandalismus, den Einbau von automatischen Toren und Freigabegeräten, von Alarmsystemen mit Fernübertragung, stärkere und umfassendere Beleuchtung von Straßen usw. - zweifelsfrei als unzureichend und/oder nicht anwendbar im Hinblick auf die vorgenannten legitimen Zwecke erweisen.

Derselbe Grundsatz gilt auch für die Auswahl der angemessenen Technologie, für die Kriterien für die Benutzung der Geräte im konkreten Fall und für die Spezifizierung der Modalitäten für die Datenverarbeitung im Zusammenhang mit Zugangsregelungen und Speicherungszeiten.

Zum Beispiel sollte verhindert werden, dass Verwaltungsorgane Videoüberwachungsanlagen im Zusammenhang mit geringfügigen Verstößen installieren - etwa um einem Rauchverbot in Schulen und anderen öffentlichen Plätzen oder dem Verbot, Zigarettenstummel und Abfälle an öffentlichen Plätzen zu hinterlassen, Nachdruck zu verleihen.

Mit anderen Worten: Im Hinblick auf den verfolgten Zweck muss von Fall zu Fall der *Grundsatz der Verhältnismäßigkeit* angewandt werden, der eine Art *Pflicht der Datenminimierung* bei den für die Verarbeitung Verantwortlichen beinhaltet.

Während ein angemessenes Videoüberwachungs- und Alarmsystem als rechtmäßig angesehen werden kann, wenn etwa verschiedene Gewaltakte im Umkreis eines Fußballstadiums vorkommen oder in Randgebieten in Bussen oder in der Nähe von Bushaltestellen wiederholt Überfälle begangen werden, ist dies nicht der Fall, wenn ein System darauf eingestellt ist, entweder Beleidigungen gegen Busfahrer oder das Beschmutzen der Fahrzeuge - so in einem Antrag an eine Datenschutzbehörde begründet - zu verhindern; ebenso wenig, um Bürger zu ermitteln, die sich geringfügiger

---

werden.

Verstöße gegen behördliche Bestimmungen haben zuschulden kommen lassen, etwa das Hinterlassen von Abfalltüten außerhalb von Mülleimern oder in Bereichen, in denen Abfälle verboten sind, oder um Personen zu ermitteln, die in Schwimmhallen Gelegenheitsdiebstähle begehen.

Die Verhältnismäßigkeit ist nach noch strikteren Kriterien zu beurteilen, wenn es sich um nicht öffentlich zugängliche Gebäude handelt.

Der Austausch von Informationen und Erfahrungen zwischen den zuständigen Behörden der Mitgliedstaaten könnte diesbezüglich hilfreich sein[20].

Diese Überlegungen gelten insbesondere für den immer häufigeren Einsatz der Videoüberwachung zu Selbstverteidigungszwecken oder zum Schutz von Eigentum – vor allem bei öffentlichen Gebäuden und Dienststellen und ihrer Umgebung. Diese Form des Einsatzes erfordert eine allgemeinere Beurteilung der indirekten Folgen des massiven Rückgriffs auf Videoüberwachungsanlagen: d.h., ob die Aufstellung verschiedener Anlagen wirklich eine Abschreckung bedeutet, oder ob Straftäter und Zerstörungswütige einfach zu anderen Plätzen abwandern oder ihre Aktionsbereiche wechseln.

E) Verhältnismäßigkeit bei Videoüberwachungen

Der Grundsatz, wonach Daten angemessen, notwendig und verhältnismäßig zu sein haben, macht ferner eine sorgfältige Beurteilung der *Verhältnismäßigkeit der Modalitäten* für die Datenverarbeitungen erforderlich, die bereits als rechtmäßig eingestuft wurden.

An erster Stelle sind die *Modalitäten für Verfilmungen* zu berücksichtigen und folgende Aspekte zu beachten:

a) das Bildfeld im Verhältnis zu den verfolgten Zwecken[21] - z. B. wenn die Überwachung eines öffentlichen Platzes erfolgt, muss das Bildfeld so eingestellt sein, dass keine Details zu erkennen sind, etwa körperliche Merkmale, die für die verfolgten Zwecke keine Rolle spielen, oder keine Einblicke in nahe gelegene private Bereiche, insbesondere, wenn eine Zoom-Funktion eingebaut ist,
b) die Art der Bildaufnahmegeräte, etwa ob ortsfest oder mobil,
c) die konkreten Modalitäten des Einbaus, etwa der Standort der Kamera, die Verwendung von festen oder beweglichen Kameras usw.,
d) die Möglichkeit einer Vergrößerung von Bildern entweder bei der Aufnahme selbst

Formatted:

20 Dies würde auch eine bessere Angleichung zwischen den ordnungsrechtlichen Konzepten einerseits und den Verwaltungsentscheidungen andererseits gestatten, die zuweilen voneinander abweichen - wie dies etwas bei den Bingohallen der Fall war.

21 Beispiele für besondere Vorkehrungen, die bezüglich des Bildwinkels getroffen werden müssen, liegen in zwei Bestimmungen der italienischen Datenschutzbehörde vor: Eine Gesundheitseinrichtung plante, einen Dienst einzuführen, der es Verwandten erlaubt, Patienten, die im Koma liegen oder sich in Quarantäne oder als Schwerkranke auf einer Intensivstation befinden, über Fernverbindung ständig zu beobachten. Sie wurde darauf hingewiesen, dass die Modalitäten so beschaffen sein müssen, dass nicht gleichzeitig auch andere Patienten gesehen werden.
In einem anderen Fall wies die Datenschutzbehörde die Polizeidienststellen an, Anlagen zur Ermittlung von Geschwindigkeitsübertretungen so aufzustellen, dass lediglich die entsprechenden Autokennzeichen aufgenommen wurden, nicht aber auch das Wageninnere.

oder danach, etwa bei gespeicherten Bildern, und die Möglichkeit, Bilder von Einzelpersonen unscharf einzustellen oder ganz herauszulöschen,

e) Standbild-Funktionen,

f) die Verbindung mit einer Stelle, an die akustische oder optische Warnhinweise gesandt werden,

g) die Schritte im Anschluss an die Videoüberwachung, etwa Schließung von Eingängen, Benachrichtigung von Sicherheitskräften usw.

Zweitens sind die *Entscheidungen* zu beachten, *die hinsichtlich der Aufbewahrung von Bildern und der Aufbewahrungszeit zu treffen sind* - letztere muss ziemlich kurz sein und in Einklang mit den besonderen Merkmalen des Einzelfalles stehen.

Während in einigen wenigen Fällen ein System genügt, das eine Visualisierung von Bildern, die darüber hinaus nicht aufgezeichnet werden, nur in internem Rahmen gestattet - etwa bei den Ladenkassen in Supermärkten, kann es in anderen Fällen - zum Beispiel zum Schutz von privaten Gebäuden - gerechtfertigt sein, die Bilder für einige Stunden zu speichern oder erst nach Ablauf eines Tages oder spätestens nach Ablauf einer Woche automatisch zu löschen. Eine Ausnahme von dieser Regel wäre natürlich im Falle eines Alarms oder einer Anfrage gegeben, die besondere Beachtung erfordert; in solchen Fällen gibt es berechtigte Gründe, kurzzeitig Entscheidungen etwa der Polizei oder der Justizbehörden abzuwarten.

Als weitere Beispiele lassen sich Systeme nennen, die das unerlaubte Eindringen von Fahrzeugen in Stadtzentren und Verkehrsbereiche mit eingeschränktem Zugang überwachen sollen; hier dürfen Bilder nur im Falle einer Übertretung gespeichert werden.

Die Frage der Verhältnismäßigkeit muss ferner beachtet werden, wenn längere Speicherungsfristen für notwendig gehalten werden, die aber die Dauer von einer Woche nicht überschreiten sollten[22] - zum Beispiel bei Bildern aus der Videoüberwachung, die etwa für die Identifizierung von Personen herangezogen werden, die ein Bankgebäude vor einem Raubüberfall frequentiert haben.

Drittens sind diejenigen Fälle zu beachten, in denen eine *Identifizierung von Personen* durch die Verknüpfung von Aufnahmen ihres Gesichts mit anderen Informationen ihrer aufgezeichneten Verhaltensweisen oder Tätigkeiten - etwa im Falle einer Verknüpfung von Bildern und Tätigkeiten von Kunden einer Bank zu einer leicht feststellbaren Zeit.

Diesbezüglich muss der eindeutige Unterschied zwischen einer zeitweiligen Speicherung von Bildern aus der Videoüberwachung durch Geräte am Eingang einer Bank und der weitaus indiskreteren Anlage von Datenbanken beachtet werden, die auch Fotografien und Fingerabdrücke enthalten, die von den Bankkunden mit Ihrem Einverständnis selbst geliefert werden.

Schließlich sind diejenigen Entscheidungen zu beachten, die bezüglich der *möglichen Weitergabe der Daten an Dritte* (die grundsätzlich keine Einrichtungen sein sollen, die mit der Videoüberwachung nichts zu tun haben) als auch ihrer teilweisen oder gar

---

22 Die dänische Datenschutzbehörde vertrat den Standpunkt, dass Videoaufzeichnungen nur für kurze Zeit, d.h. höchstens 30 Tage, gespeichert werden dürften.

vollständigen Offenlegung im Ausland oder im Internet zu treffen sind; dies ist im Hinblick auf die Bestimmungen bezüglich des angemessenen Schutzniveaus zu prüfen (vgl. Artikel 25 ff. der Richtlinie).

Der Grundsatz, wonach Bilddaten notwendig und verhältnismäßig zu sein haben, gilt selbstverständlich auch für die Kombination von Informationen, die sich in der Hand verschiedener Verantwortlicher für Videoüberwachungsanlagen befinden.

Mit den vorgenannten Schutzmaßnahmen soll auch auf der operationellen Ebene der Grundsatz umgesetzt werden, auf den die innerstaatlichen Rechtsvorschriften einiger weniger Staaten Bezug nehmen, nämlich der *Grundsatz der Mäßigung bei der Verwendung personenbezogener Daten*, d.h. die Vermeidung oder möglichst weit gehende Einschränkung der Verarbeitung personenbezogener Daten.

Dieser Grundsatz muss in sämtlichen Bereichen gelten; dabei ist zu beachten, dass viele Zwecke ohne den Rückgriff auf personenbezogene Daten erreicht werden können, oder aber durch den Einsatz von wirklich anonymen Daten, auch wenn es anfangs so erscheint, als sei eine Verwendung personenbezogener Informationen erforderlich.

Die vorgenannten Überlegungen gelten auch bei gerechtfertigten Rationalisierungsmaßnahmen[23] oder notwendigen Verbesserungen der Dienstleistungen für die Verbraucher[24].

F) Unterrichtung der Betroffenen

Die Transparenz und Angemessenheit beim Einsatz von Videoüberwachungsanlagen bedingt eine angemessene Unterrichtung der Betroffenen gemäß Artikel 10 und 11 der Richtlinie.

Die Betroffenen sind darüber zu informieren, dass eine Videoüberwachung stattfindet, selbst wenn sich diese auf öffentliche Ereignisse, Veranstaltungen oder Werbemaßnahmen (Webcams) bezieht. Sie sind ausführlich darüber zu informieren, welche Stellen überwacht werden.

Es ist nicht notwendig, den genauen Standort des Überwachungsgeräts anzugeben, aber die Umstände der Überwachung müssen eindeutig bekannt gemacht werden.

Die Auskünfte - auch bezüglich der *Verfilmungsmodalitäten* - müssen in einem vernünftigen Abstand zu den überwachten Plätzen angebracht werden, und nicht, wie in einigen wenigen Fällen geschehen, wo eine Anbringung von Informationen in einem Abstand von 500 Metern vom überwachten Bereich als akzeptabel betrachtet wurde.

Die Informationen müssen also gut sichtbar angebracht sein und können in knapper Form

---

23 Dies kann etwa der Fall sein, wenn in einem Supermarkt die Anzahl der Kassen berechnet werden soll, die in Abhängigkeit von der Anzahl der hereinströmenden Kunden gleichzeitig geöffnet sein müssen, oder wenn die Einkaufsrouten der Kunden in einem Supermarkt optimiert werden sollen.

24 Um den Zugang zu einem Arbeitsplatz oder zu einem bestimmten Verkehrsmittel, der Identitätskontrollen erforderlich macht, zu erleichtern, dürften Personalausweise mit Fotografie, unter Umständen auch auf computererkennbarem Trägermaterial, ausreichend sein, ohne Gesichts-erkennungssysteme zu installieren.

erfolgen, vorausgesetzt, dass sie alles Wesentliche enthalten. Dazu können auch Piktogramme gehören, die sich im Zusammenhang mit Videoüberwachungen und Rauchverboten bereits bewährt haben; sie können sich unterscheiden, je nachdem, ob die Aufnahmen gespeichert werden oder nicht. Auf jeden Fall müssen die Zwecke der Videoüberwachung und der zuständige Verantwortliche angegeben werden. Die Größe der Informationshinweise muss den einzelnen Standorten angepasst sein[25].

Besondere, wohlbegründete Einschränkungen der Informationsvorschriften sind nur in den Fällen gestattet, die in Artikel 10, 11 und 13 der Richtlinie genannt werden - zum Beispiel zeitweilige Einschränkung bei Daten, die im Verlaufe von Ermittlungen gesammelt werden, die rechtmäßig von Strafverteidigern durchgeführt werden, oder sonst im Zusammenhang mit dem Recht auf Verteidigung stehen, sofern die Erteilung von Auskünften das Erreichen der verfolgten spezifischen Zwecke behindern würde.

Schließlich ist zu überlegen, wie die entsprechenden Informationen auch blinden Personen am besten übermittelt werden.

G) Weitere Voraussetzungen

Im Zusammenhang mit solchen zusätzlichen Vorschriften, Vorkehrungen und Schutzmaßnahmen, auf die in den Datenschutzgesetzen verwiesen wird, und die vorstehend im dritten Abschnitt zusammengefasst wurden, und im Hinblick darauf, dass die Verarbeitung personenbezogener Daten gemeldet werden muss und einer Überwachung durch eine unabhängige Behörde gemäß Artikel 18, 19 und 28 der Richtlinie unterliegt, möchte die Arbeitsgruppe insbesondere auf folgende Aspekte hinweisen:

a) Einer noch festzulegenden begrenzten Anzahl natürlicher Personen muss der Zugang zu den aufgezeichneten Bildern oder ihre Einsichtnahme gestattet werden, und zwar ausschließlich für die Zwecke, die durch eine Videoüberwachung verfolgt werden, oder zur Wartung der entsprechenden Geräte und Prüfung ihrer Funktionsfähigkeit; andererseits kann dies auch aufgrund des Antrags eines Betroffenen auf Zugang zu seinen Daten oder aufgrund einer rechtmäßigen Anordnung der Polizei- oder Justizbehörden zu Ermittlungszwecken erfolgen.

   Wenn eine Videoüberwachung lediglich zur Verhütung, Aufdeckung oder Verfolgung von Straftaten eingesetzt wird, kann sich in vielen Fällen eine Lösung durch Verwendung von zwei Zugangsschlüsseln - einem in der Hand des Verantwortlichen für die Verarbeitung und einem anderen bei der Polizeibehörde - als zweckmäßig erweisen, um sicherzustellen, dass Bilder - unbeschadet des legitimen Rechts der Betroffenen, während der kurzen Zeit der Bildspeicherung auf Antrag einen Zugang zu ihren Daten zu erhalten - lediglich von Polizeibeamten eingesehen werden.

b) Um Situationen zu vermeiden, wie sie in Artikel 17 der Richtlinie genannt werden, müssen geeignete Schutzmaßnahmen getroffen werden, unter anderem die Verbreitung von Informationen, die für den Schutz des Rechts der Betroffenen, der Dritten oder der für die Verarbeitung Verantwortlichen sowie im Hinblick auf eine Verhinderung von Manipulationen, Änderungen oder Zerstörung von Daten und

25 Dies könnte als "gestufter" Ansatz bezeichnet werden.

entsprechenden Beweisen zweckmäßig sind.

c) Die Qualität der aufgezeichneten Bilder ist ebenfalls von grundlegender Bedeutung - vor allem, wenn das Speichermedium wiederholt verwendet wird, was die Gefahr von Fehlern oder gar der völligen Löschung der früher aufgezeichneten Bilder mit sich bringt.

d) Schließlich ist es sehr wichtig, dass die konkret an der Videoüberwachung beteiligten Mitarbeiter angemessen ausgebildet werden und lernen, welche Schritte zu unternehmen sind, um die einschlägigen Vorschriften zu erfüllen. Auch die Ausbildung der Kontrolleure und Mitarbeiter im Hinblick auf die einschlägigen Risiken und Verfahren für die korrekte Ermittlung der abgebildeten Einzelpersonen kann als sinnvolle Maßnahme betrachtet werden.

H) Die Rechte der Betroffenen

Auch besondere Merkmale der erhobenen personenbezogenen Daten setzen keineswegs die Rechte der Betroffenen außer Kraft, die in Artikel (13 und) 14 der Richtlinie festgelegt sind; vor allem nicht das Recht auf Einspruch gegen eine Verarbeitung. Die Richtlinie 95/46/EG gestattet den Betroffenen, gegen die Verarbeitung sie betreffender Daten jederzeit aus stichhaltigen, sich aus ihrer besonderen Situation ergebenden Gründen Widerspruch einzulegen[26].

Das Recht der Betroffenen auf eine Löschung ihrer Daten und die gewöhnlich kurze Speicherungsfrist der Aufnahmen schränken das Recht der Betroffenen auf Zugang zu ihren personenbezogenen Daten ein, durch die sie identifizierbar werden; doch muss dieses Recht besonders in denjenigen Fällen gewahrt werden, in denen ein Antrag so detailliert gestellt wird, dass die betreffenden Aufnahmen leicht wiedergefunden werden können. Auch muss berücksichtigt werden, dass zeitweise die Rechte Dritter zu schützen sind.

Jede Einschränkung, die mit dem Aufwand für das Wiederauffinden von Aufnahmen begründet wird, wenn ein solcher Aufwand im Hinblick auf Forschungszwecke, Kosten und Mittel angesichts der kurzen Speicherungszeit der Bilder eindeutig als unverhältnismäßig einzustufen ist, darf ausschließlich im Primärrecht verankert werden (siehe Artikel 13 Absatz 1 der Richtlinie); dabei muss das Recht der Betroffenen auf Verteidigung in Bezug auf besondere Ereignisse, die im fraglichen Zeitraum geschehen sind, angemessen berücksichtigt werden.

I) Zusätzliche Schutzmaßnahmen im Zusammenhang mit besonderen Verarbeitungen

Videoüberwachungen, aus denen die rassische Herkunft, religiöse oder politische Überzeugungen, die Gewerkschaftszugehörigkeit oder sexuelle Gewohnheiten hervorgehen (Artikel 8 der Richtlinie), sind zu verbieten.

Ohne eine erschöpfende Liste der diversen Anwendungen der Videoüberwachung anzustreben, weist die Arbeitsgruppe doch darauf hin, dass - im Grundsatz und wo

26 Sofern innerstaatliche Bestimmungen nicht anders verfügen.

angemessen, im Rahmen der Vorabprüfungen der Verarbeitungen gemäß Artikel 20 der Richtlinie - auf einige wenige Kontexte/Rahmenbedingungen stärker einzugehen ist, in denen Bilder gesammelt werden, die bestimmte oder bestimmbare Personen betreffen; diese Kontexte müssen von Fall zu Fall geprüft werden.

Gedacht ist vor allem an folgende Fälle, die sich aus den gesammelten Erfahrungen oder bereits angelaufenen Prüfungen ergeben haben:

a) Ständige Verbindung zwischen mehreren Videoüberwachungssystemen, die von verschiedenen für die Verarbeitung Verantwortlichen betrieben werden;
b) mögliche Verknüpfung von Bildern und biometrischen Daten wie etwa Fingerabdrücken (zum Beispiel an Eingängen zu Bankgebäuden);
c) Einsatz von Spracherkennungssystemen;
d) im Einklang mit den Grundsätzen der Verhältnismäßigkeit und auf der Grundlage besonderer Vorschriften Einsatz von Indexerstellungssystemen für aufgezeichnete Bilder oder für Systeme zu deren gleichzeitig automatischer Wiederherstellung, insbesondere über Kennungsdaten;
e) Gesichtserkennungssysteme, die nicht darauf beschränkt sind, maskierte Passanten zu ermitteln, etwa solche mit falschen Bärten oder Perücken, sondern gezielt verdächtige Straftäter aussuchen, zum Beispiel aufgrund der Fähigkeit des Systems, bestimmte Personen mit Schablonen oder standardisierten Identitätsbausteinen nach bestimmten auffallenden Aspekten (Hautfarbe, Augenform, Wangenknochen usw.) automatisch zu ermitteln, oder auf der Grundlage von vordefiniertem anomalen Verhalten (plötzliche Bewegungen, wiederholtes Vorbeigehen, selbst bei gegebenen Zeitintervallen, Art und Weise, ein Fahrzeug zu parken usw.). In diesem Fall ist die Hinzuziehung einer Person angebracht, auch im Hinblick darauf, dass in solchen Fällen Fehler unterlaufen können, wie auch im Zusammenhang mit nachfolgendem Punkt f) erwähnt wurde;
f) die Möglichkeit einer automatischen Verfolgung von Wegen oder der Rekonstruktion oder Prognose des Verhaltens einer Person;
g) automatisierte Entscheidungen auf der Grundlage eines persönlichen Profils oder intelligenter Analyse- und Interventionssysteme, die nichts mit den üblichen Warnmeldungen zu tun haben wie etwa beim Zugang ohne erforderliche Identitätskennzeichen zu einem Ort oder bei einem Feueralarm.

8. VIDEOÜBERWACHUNG AM ARBEITSPLATZ

Die Arbeitsgruppe hat in ihrer *Stellungnahme Nr. 8/2001 zur Verarbeitung personenbezogener Daten von Beschäftigten*, die sie am 13. September 2001 vorgelegt hatte, und in ihrem *Arbeitsdokument zur Überwachung der elektronischen Kommunikation von Beschäftigten* vom 29. Mai 2002 in allgemeinerer Form bereits auf einige Grundsätze zum Schutz der Rechte, Freiheiten und Würde der Betroffenen am Arbeitsplatz hingewiesen[27].

Zusätzlich zu den dort vorgebrachten Überlegungen und sofern sie konkret auf die Videoüberwachung übertragen werden können, ist es angebracht, darauf hinzuweisen, dass Videoüberwachungssysteme für eine Fernkontrolle von Qualität und Umfang der Arbeitstätigkeiten, die auch eine Verarbeitung personenbezogener Daten beinhalten,

27 Beide Dokumente sind unter folgender Internet-Adresse abrufbar: http://europa.eu.int/comm/internal_market/de/dataprot/index.htm

nicht als Regel erlaubt sein sollten.

Dieser Fall unterscheidet sich von Videoüberwachungssystemen, die unter Einhaltung der angemessenen Schutzmaßnahmen eingesetzt werden, um Sicherheitsvorschriften in der Produktion oder am Arbeitsplatz zu erfüllen, und ebenfalls eine Fernüberwachung - wenn auch nur indirekt - mit sich bringen[28].

Die bei der Durchführung gesammelten Erfahrungen zeigen ferner, dass eine Überwachung keine Gebäudeteile umfassen sollte, die für die private Nutzung der Beschäftigten vorgesehen sind oder nicht der Ausführung von Arbeitsschritten dienen - etwa Toiletten, Duschräume, Umkleidekabinen und Erholungsräume; ferner, dass Bilder, die ausschließlich zum Schutz des Eigentums oder zur Aufdeckung, Ermittlung und Verfolgung von schwerwiegenden Straftaten aufgezeichnet werden, nicht verwendet werden sollten, um Beschäftigte wegen geringfügiger Disziplinarvergehen zu belangen, und schließlich, dass den Beschäftigten jederzeit gestattet werden sollte, ihre Gegenforderungen unter Verwendung der aufgezeichneten Bilder vorzubringen.

Über die Videoüberwachung sind sämtliche Beschäftigten und sonstigen in den Betriebsräumen arbeitenden Personen zu unterrichten. Dazu gehören Informationen über die Identität der Kontrolleure und den Zweck der Überwachung sowie sonstige Angaben, die für eine faire Verarbeitung von Daten der Betroffenen erforderlich sind, etwa, in welchen Fällen die Aufnahmen von der Geschäftsleitung eines Unternehmens geprüft werden, die Dauer der Aufzeichnungen und Mitteilungen für den Fall, dass die Aufzeichnungen den Strafverfolgungsbehörden zur Verfügung gestellt werden. Entsprechende Informationen etwa in Form eines Symbols können im betrieblichen Bereich nicht als ausreichend betrachtet werden.

9. ZUSAMMENFASSUNG

Die Arbeitsgruppe hat dieses Arbeitsdokument verfasst, um einen Beitrag zur einheitlichen Anwendung der einzelstaatlichen Maßnahmen zu liefern, die im Bereich Videoüberwachung gemäß der Richtlinie 95/46/EG getroffen wurden.

*** * ***

In diesem Rahmen ist es von großer Bedeutung, dass die Mitgliedstaaten im Hinblick auf die Tätigkeiten von Herstellern, Dienstleistungsanbietern und Vertriebshändlern sowie Softwareentwicklern Leitlinien für die Entwicklung von Technologien, Software und technischen Geräten herausgeben, die im Einklang mit den Grundsätzen stehen, die in diesem Dokument dargelegt wurden.

---

28 In diesen Fällen muss zusätzlich zu den Überlegungen aus diesem Dokument besonders berücksichtigt werden, dass die in Tarifverträgen verankerten Rechte gewahrt bleiben müssen, die zuweilen auf der kollektiven Unterrichtung der Beschäftigten oder ihrer Gewerkschaften beruhen, d.h. neben der Information, die individuell gemäß den Datenschutzvorschriften zu erteilen ist; in anderen Fällen müssen vorab Vereinbarungen getroffen werden, auch bezüglich der Dauer der Überwachung und anderer Verfilmungsmodalitäten. In einigen wenigen Staaten ist eine Intervention durch staatliche Stellen vorgesehen, sofern zwischen den Tarifparteien keine Vereinbarung erzielt werden kann.

* * *

		Geschehen zu Brüssel, den 11. Februar 2004 Für die Arbeitsgruppe *Der Vorsitzende* Stefano RODOTA