Videoüberwachung am Arbeitsplatz

Eberhard Kiesche // Matthias Wilke

HIER LESEN SIE:

- welche Überwachungsmöglichkeiten neue digitale Videotechnik bietet
- welche rechtlichen Grundlagen für die Videoüberwachung insbesondere am Arbeitsplatz gelten und als Mindestanforderungen durch Regelungen der Belegschaftsvertretung nicht unterschritten werden dürfen
- warum eine heimliche Videoüberwachung immer verboten ist und auch die unverdeckte Videoüberwachung am Arbeitsplatz stets die streng begrenzte Ausnahme sein muss
- welche Regelungsaspekte für Betriebs- und Dienstvereinbarungen zu beachten sind

Diebstahl, tätliche Angriffe auf Mitarbeiter, Sachbeschädigung und andere leider auch an Arbeitsplätzen vorkommende oder zumindest mögliche Straftaten liefern die Begründung dafür, dass nicht mehr nur in öffentlichen Einrichtungen, sondern zunehmend auch im Arbeitsumfeld Videosysteme zur Abschreckung und Beweissicherung eingesetzt werden – zum Beispiel auf dem dunklen Parkplatz oder in besonders schützenswürdigen Bereichen wie Rechenzentrum, Kassenbereich oder Laderampe. Immer und überall ist diese „Big-Brother"-Methode jedoch nicht zulässig – und eine Kontrolle der Arbeitsleistung mit Hilfe von Videokameras vom Bundesarbeitsgericht (BAG) sogar verboten worden.[1]

Jede Form der Beobachtung von Menschen durch Kameras stellt einen Eingriff in deren verfassungsmäßig geschützte allgemeine Persönlichkeitsrechte dar. Dabei steht das berechtigte Bedürfnis der Betroffenen nach Wahrung der Intimsphäre dem stetig wachsenden Sicherheitsbedürfnis entgegen.

Der Einsatz von Videoüberwachung bedeutet deshalb für jedes Unternehmen, für jeden Mitarbeiter oder auch Kunden immer einen Widerspruch zwischen einerseits dem Wunsch, vor kriminellen Attacken geschützt zu werden und andererseits der Forderung, persönliche Freiräume und Intimsphäre gewahrt zu wissen. Anders ausgedrückt: Man möchte sich zwar sicher, aber nicht kontrolliert oder überwacht fühlen.

Damit ist die Einführung einer Videoüberwachung in Betrieb oder Behörde gerade auch für eine Belegschaftsvertretung immer ein besonders heikles Thema, das offene und klare Argumente und vor allem eine zweifelsfreie rechtliche Absicherung braucht.

Neue Technik für die Videoüberwachung

In der Vergangenheit wurden für eine Videoüberwachung eigene geschlossene Übertragungssysteme aus Kameras, fest verlegten Kabeln, Beobachtungsschirmen und meist noch Aufzeichnungssystemen aufgebaut. Diese ► analoge Closed-Circuit-Television-Technik (CCTV) wird auch nach wie vor in vielen Betrieben eingesetzt. Vermehrt ist jedoch ein Übergang zur ► digitalen CCTV-Technik zu beobachten.

DIE AKTUELLE MELDUNG

Am 15.11.2007 hat der Bundestag das EU-Abkommen mit den USA über die Weitergabe von Fluggastdaten beschlossen. Das war zwar umstritten, aber man durfte doch davon ausgehen, dass die Abgeordneten wussten was sie taten. Dass das nicht der Fall war, kam erst zwei Wochen später raus. In das Gesetz war nämlich – so berichtete FR-Online am 28.11.2007 – eine Änderung des § 27 Bundespolizeigesetz eingeschmuggelt worden. Darin wurde der Passus „spätestens nach zwei Tagen" durch „spätestens nach dreißig Tagen" ersetzt.

Das heißt im Klartext: Videoaufnahmen von Überwachungskameras auf Bahnhöfen und Flugplätzen müssen künftig nicht mehr nach 48 Stunden gelöscht werden, sondern können einen ganzen Monat lang aufbewahrt und gegebenenfalls polizeilich ausgewertet werden – eine Bestimmung die mit dem Thema Fluggastdaten gar nichts zu tun hatte und deshalb von den Abgeordneten auch schlicht übersehen worden war.

Kein Wunder also, dass der Bundesbeauftragte für den Datenschutz – nachdem er der Sache auf die Spur gekommen war – von einem Skandal sprach und damit auch die Tatsache meinte, dass dieses Sicherheitsgesetz ohne jede öffentliche Debatte von der Koalition „innerhalb eines Tages durchgewinkt worden" war.

Insbesondere die Abgeordneten der Grünen und der FDP fühlen sich nun manipuliert und hintergangen. Ob das so ist oder ob die Opposition die Sache bloß verpennt hat, wie der SPD-Innenpolitiker Wiefelspütz meint, sei mal dahin gestellt. Aber ganz sicher recht hat der Bundesbeauftragte für den Datenschutz, wenn er hier einen Trend ausmacht: Statt einem konkreten Verdacht nachzugehen, werden von den Behörden mehr und mehr Daten unabhängig von konkreten Vorwürfen gespeichert. Und der Bundestag diskutiert nicht einmal mehr darüber.

Dabei wird das erfasste Videobild digitalisiert und die Übertragung dieser Daten zur Überwachungszentrale erfolgt dann über das Netzwerk des Unternehmens oder auch über das Internet. Das digitale CCTV nutzt also die bestehende IKT-Infrastruktur – und ist damit längst nicht mehr so „geschlossen" (englisch: *closed*), wie es ihr Name sagt.

„Klare Sicht, wo besonderer Schutz gefragt ist", so lautet der Slogan eines CCTV-Systemanbieters. Und das kann man durchaus wörtlich nehmen: Die angebotenen Überwachungs- und Kontrollanlagen liefern beste Bildqualität selbst bei schwierigen Lichtsituationen, hochwertige Daten also, die mit den verschwommenen Fahndungsbildern der Vergangenheit nichts mehr gemein haben.

Außerdem verfügt die neue Technikgeneration im Gegensatz zu den herkömmlichen Systemen meist auch über steuerbare Kameras. Mit sogenannten Dome-Kameras (englisch: *dome* = Kuppel) können große Flächen im Innen- und Außenbereich rundum kontrolliert werden. Gängige Modelle verfügen über 20fach optisches und 10fach digitales Zoom und sind für den Tag-/Nacht-Einsatz geeignet.

Foto: Starfusions

Steuerbare Rundum-Kameras mit drahtloser Datenübertragung sind Stand der Technik.

Alles in allem bieten die netzwerkfähigen digitalen Kameras und Bildspeicher jedenfalls aus Sicht der Sicherheitsexperten gegenüber der traditionellen Technik, also dem klassisch verkabelten Videorecorder, erhebliche Vorteile:

- sehr viel kostengünstigerer Systemaufbau,
- vereinfachte und beschleunigte Übertragung und Auswertung der Bilddaten,
- direkte (Echtzeit-)Übertragung der Bilder an fast jeden Ort der Welt,
- einfache und gezielte Steuerung der Kameras ebenfalls von beliebigen Orten aus,
- Unterstützung der Bildaufnahme und Auswertung durch spezielle Software.

Von besonderem Interesse sind dabei neben den Kostenvorteilen vor allem zwei Aspekte:

(1) Die globale Nutzbarkeit der anfallenden Bilddaten – so will beispielsweise die Sicherheitsabteilung eines bekannten Modemarkts die Kameras von über 50 Filialen zentral in der Hauptverwaltung steuern und alle Bilder dort auch auswerten.

(2) Die Unterstützung durch Auswertungssoftware – damit wird es beispielsweise möglich, Bilder immer nur dann aufzeichnen zu lassen, wenn in einem festgelegten Bereich (oder Zeitraum) genau definierte Ereignisse eintreten. So kann etwa festgelegt werden, dass das Videosystem nur die Personen erfasst, die nicht den direkten Weg von A nach B wählen oder nur die, die nach 20.00 Uhr durch einen bestimmten Flur gehen (siehe Abbildung auf Seite 10). Durch solche „intelligenten" Zonenkonzepte sollen Fehl- und Falschalarme auf ein Minimum reduziert werden.

Die neueste Generation der Videosysteme ist sogar in der Lage, Änderungen in einem Videobild nicht nur zu erkennen, sondern auch zu interpretieren. Die typischen Störgrößen wie „Schnee", Änderung der Lichtverhältnisse und vieles mehr können solche Systeme wirksam erkennen und herausfiltern.

Insbesondere im Bereich der Video-Bewegungserkennung lassen sich mit 3D-Technik mittlerweile sehr gute Resultate erzielen. Solche 3D-Systeme sind nicht nur extrem unempfindlich für Fehlalarme, es ist

sogar möglich, die exakte Position eines Objekts im Raum zu bestimmen. Bewegliche Kameras können dann automatisch verdächtige Personen ins Visier nehmen, sie verfolgen und Bewegungsabläufe in Lageplänen darstellen.

Moderne Gesichtserkennungssysteme können an vergleichsweise wenigen „Ankerpunkten" Gesichter recht zuverlässig erkennen.

Ein weiteres neues Gebiet für die Sicherheitstechnik ist die automatische Identifizierung durch Gesichtserkennung. Neben anderen biometrischen Technologien wie z.B. Fingerabdruck- oder Augenscannern (siehe dazu den Schwerpunkt „Biometrie" in CuA 1/07) wird der Gesichtserkennung künftig mehr Bedeutung zukommen. Das heißt: Wenn die entsprechenden Bildinformationen (Fotos) hinterlegt sind, erkennt das System, ob eine bestimmte Person sich gerade im Beobachtungsbereich aufhält und kann dann z.B. automatische Alarme oder das Schließen bestimmter Türen veranlassen.

Der Ruf nach solchen Techniken wird lauter – auch vor dem Hintergrund der Krawalle in Sportstadien. Bereits jetzt wird die automatische Gesichtserkennung vermehrt eingesetzt, etwa zur Personenkontrolle bei Grenzübertritten, auf Flughäfen oder auch im Zutrittsbereich besonders schützenswerter Räume in verschiedenen Unternehmen. Neben der mehr oder weniger diskreten Alarmierung beim Eindringen unerwünschter Personen in kontrollierte Zonen, erlauben die Systeme natürlich auch, auf willkommene Persönlichkeiten aufmerksam zu machen …

Die hessische Polizei hat seit März dieses Jahres bereits über eine Million Autokennzeichen mit automatischen Videokameras (sogenannten Kennzeichenlesegeräten) erfasst.[2] Der damit verbundene automatische Abgleich mit Fahndungsdatenbanken hat 300 Treffer ergeben. Ob dies eine normale Ermittlungsmethode der Polizei ist oder eine dauerhafte Rasterfahndung, die Schluss mit dem anonymen Benutzen von Straßen und Autobahnen macht, muss das Bundesverfassungsgericht entscheiden. Drei Autofahrer haben Verfassungsbeschwerde eingelegt. Eine Entscheidung wird im kommenden Jahr erwartet.[3]

Videoüberwachung – rechtliche Grundlagen

Die Videoüberwachung ist im Bundesdatenschutzgesetz (BDSG) und in einzelnen Datenschutzgesetzen der Bundesländer geregelt, wobei die Rechtsform des Arbeitgebers darüber entscheidet, ob ein Landes- oder das Bundesdatenschutzgesetz zur Anwendung kommt:

Für Behörden und Unternehmen in öffentlich-rechtlicher Trägerschaft sind entweder das Bundesdatenschutzgesetz oder die jeweiligen Landesdatenschutzgesetze bindend. Firmen in privater Trägerschaft dagegen unterliegen immer dem Bundesdatenschutzgesetz.

In den meisten dieser Gesetze sind für den Einsatz von Überwachungskameras Mindestanforderungen definiert worden. Da sich die Landesdatenschutzgesetze stark an das Bundesdatenschutzgesetz anlehnen, hier nun die Grundsätze des § 6b BDSG zur Videoüberwachung in öffentlich zugänglichen Räumen: Werden durch die Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, ist diese über eine Verarbeitung oder Nutzung entsprechend den § 19a und § 33 zu benachrichtigen.

Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

§ 6b Bundesdatenschutzgesetz (BDSG)

[…] die Beobachtung öffentlicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie
– zur Aufgabenerfüllung öffentlicher Stellen,
– zur Wahrnehmung des Hausrechtes oder
– zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke
erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.
Der Umstand der Beobachtung und die verantwortliche Stelle sind durch geeignete Maßnahmen erkennbar zu machen.
Die Verbreitung oder Nutzung der nach Absatz 1 erhobenen Daten ist zulässig, wenn sie zur Erreichung des verfolgten Zwecks erforderlich ist, und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Für einen anderen Zweck dürfen sie nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist.

In Betrieben, Supermärkten und ähnlich „öffentlichen" Örtlichkeiten kann also die Videobeobachtung bestimmter Bereiche zulässig sein, wenn dies zur Wahrnehmung des Hausrechts oder zum Schutz beispielsweise vor Vandalismus oder Dieb-

stahl erforderlich erscheint und dadurch die Persönlichkeitsrechte der Kunden und Beschäftigten nicht übermäßig verletzt werden. Ob die Installation einer Kamera im Einzelfall rechtens ist, bedarf also immer der Abwägung und Berücksichtigung zahlreicher Kriterien (siehe dazu auch den Artikel ab Seite 13).

Der PC wird mit der entsprechenden Software zur Überwachungs- und Steuerungszentrale.

Entscheidend ist dabei auch, ob öffentlich zugängliche oder nicht zugängliche Bereiche überwacht werden sollen. Die Vorschrift des § 6b Abs. 1 BDSG allerdings regelt nur die Beobachtung öffentlich zugänglicher Räume. Bezogen auf die Videoüberwachung von Arbeitsplätzen stellt sich damit also zunächst die Frage, unter welchen Umständen diese als „öffentlich zugänglich" gelten können.[4]

Arbeitsplätze – öffentlich zugänglich?

Alle Räume, die von jedermann frei betreten werden können, sind öffentlich zugängliche Räume (u.a. Museen, Schalterhallen, Bahnsteige, Verkaufsräume, Tankstellen, Biergärten, Parkhäuser). Das Gegenteil von öffentlichen Räumen sind Bereiche, die nur bestimmten, abschließend definierten Personenkreisen (wie z.B. den Mitarbeitern eines Unternehmens) zugänglich sind, entweder, weil die Räume als solche gekennzeichnet sind oder weil bekannt ist, dass sie nicht allgemein zugänglich sind (wie z.B. ein privater Vorgarten).

In den meisten Unternehmen und Betrieben gibt es sowohl „öffentlich zugängliche" als auch „nicht-öffentliche" Räume. Als ein auf alle anderen Betriebe/Behörden zu übertragendes Beispiel kann ein Krankenhaus genommen werden: Die Eingangshalle, der Weg zur Unfallambulanz, Warteflure vor Untersuchungsräumen und ähnliche Bereiche sind im Sinne des BDSG „öffentlich". Funktionsräume, Arzt- oder Schwesternzimmer, der Operationssaal, das Labor, aber auch die Patientenzimmer sind hingegen „nicht-öffentlich". Damit ist klar: Arbeitsplätze können sich sowohl in öffentlich zugänglichen als auch in nicht-öffentlichen Räumen befinden.

Während es bei Einhaltung der gesetzlichen Vorgaben (siehe oben § 6b BDSG) relativ unproblematisch sein kann, einen öffentlichen Bereich ohne Arbeitsplätze mit Videotechnik zu überwachen, sind für Betriebs- oder Geschäftsräume nach der Vorstellung des Gesetzgebers „besondere Regelungen" für das Anbringen von Überwachungskameras erforderlich.[5]

Der Grund liegt auf der Hand: Der Eingriff in die Persönlichkeitsrechte eines Arbeitnehmers ist bei der Überwachung öffentlicher oder nicht-öffentlicher Betriebs-/Geschäftsräume sehr viel intensiver als in öffentlich zugänglichen Räumen. Während die überwachten Menschen in der „richtigen" Öffentlichkeit, etwa auf einem Bahnhofsvorplatz, demjenigen, der sich die Überwachungsmonitore oder Aufzeichnungen anschaut, in der Regel unbekannt sind, verhält sich dies bei einem Büro oder einem Produktionsraum natürlich anders. Hier sind die überwachten Personen durchweg bekannt, so dass es bei ihnen zu einem sehr viel stärkeren Überwachungs-, Anpassungs- und auch Einschüchterungsdruck kommen wird.

Deshalb sieht das Bundesarbeitsgericht (BAG) die „Eingriffsintensität" beim Einsatz von Videokameras am Arbeitsplatz auch als prinzipiell unverhältnismäßig an und hält sie dort nur in Ausnahmefällen für zulässig.[6] Hierbei spielt es keine Rolle, ob etwa im Kaufhaus der Arbeitsbereich durch Kunden öffentlich zugänglich ist, wie beispielsweise der Verkaufsraum oder nicht-öffentlich wie Lager oder Tresorraum. Außerdem hat das BAG 2004 bereits festgestellt, dass ohne „besondere Regelungen", etwa im Rahmen einer Betriebs- oder Dienstvereinbarung, der Betrieb einer Videoüberwachungsanlage gar nicht zulässig ist.

Für die Überwachung öffentlicher Räume ohne Arbeitsplätze ist die Beachtung und Einhaltung des § 6b des BDSG ausreichend. Für öffentliche Räume mit Arbeitsplätzen und für nicht-öffentliche Arbeitsräume sind strengere Maßstäbe anzulegen (siehe den Kasten auf Seite 11)

Zweck, Erforderlichkeit, Interessen

Vor jeder Videoüberwachung – egal ob in öffentlichen Räumen oder nicht – muss der mit der Maßnahme angestrebte Zweck schriftlich dokumentiert werden und zwar im Rahmen der so genannten Vorabkontrolle nach § 4d Abs. 5 BDSG. Diese ist vom zuständigen betrieblichen oder behördlichen Datenschutzbeauftragten durchzuführen und zu belegen.

Im Rahmen dieser Vorabkontrolle wird überprüft, ob der konkrete Einsatz einer Videokamera im jeweiligen Einzelfall gesetzeskonform ist. Ein Unternehmen ist auch immer nur dann befugt, eine Videoüberwachung durchzuführen, wenn diese Überwachung einen konkreten Zweck erfüllt, wie beispielsweise Schutz vor Diebstahl, Vandalismus oder Produktionsstörungen.

Es genügt allerdings nicht, dass es einen solchen Zweck gibt, um die Zulässigkeit einer Videoüberwachung zu begründen. Die Überwachung muss auch „erforderlich" sein. Und das ist nur dann der Fall, wenn der festgelegte Zweck mit der Video-

überwachung überhaupt erreicht werden kann. Das kann und darf übrigens durchaus hinterfragt und bezweifelt werden, denn zumindest für die offiziell genannten Zwecke taugt das Mittel der Videoüberwachung durchaus nicht immer. Und selbst wenn es im Prinzip geeignet erscheint, muss doch immer noch überprüft werden, ob wirklich keine andere, das Persönlichkeitsrecht weniger einschränkende technische oder organisatorische Methode zur Verfügung steht. Erst wenn beispielsweise das Vier-Augen-Prinzip (es dürfen immer nur zwei Personen z.B. einen Raum betreten), Pförtner, Sicherheitsdienst oder Taschenkontrollen nachweislich (!) keine Minderung bei z.B. Diebstählen oder Sachbeschädigungen bringen, könnte in sehr engen Grenzen, gegebenenfalls zeitlich befristet und natürlich unter Mitbestimmung der Belegschaftsvertretung eine Videoüberwachung unumgänglich sei.

SEMINAR ZUM THEMA

Gläserne Belegschaften – Seminar auch zum Thema Videoüberwachung mit Prof. Dr. Wolfgang Däubler und Matthias Wilke vom 3. bis 5. Juni 2008 in Kassel.

www.dtb-kassel.de

Dabei muss z.B. auch hinterfragt werden, ob eine flächendeckende Einführung der Überwachungstechnik wirklich erforderlich ist oder ob es nicht genügt, an bestimmten Schwerpunkten Kameras anzubringen. Kostenaspekte dürfen angesichts der Tatsache, dass es sich um den Schutz von Grundrechten handelt, keine Rolle spielen. Dass eine Videoüberwachung unter Umständen kostengünstiger wäre, als ein Pförtner oder ein Wachdienst, ist also ausdrücklich kein Merkmal der Erforderlichkeit.[7]

Aber selbst wenn eine geplante Videoüberwachung einem nachvollziehbaren Zweck dient und auch mangels Alternativen erforderlich erscheint, kann sie immer noch rechtlich unzulässig sein. Und zwar dann, wenn die Betroffenen (Arbeitnehmer, Kunden, Patienten, Passanten) ein schutzwürdiges Interesse daran haben, dass die Videoüberwachung unterbleibt und wenn

CHECKLISTE BETRIEBSVEREINBARUNG VIDEOÜBERWACHUNG

Einsatzzwecke der Überwachung festlegen und eingrenzen (z.B. Verhinderung von Diebstahl und Sachbeschädigung, Beweissicherung, Schutz technischer Anlagen).

Ausschluss von Leistungs- und Verhaltenskontrolle sowie der Überwachung von Anwesenheiten der Beschäftigten.

Systemdokumentation und Funktionsumfang: Standorte der Aufzeichnungsgeräte und Kameras, Ausrichtung (Schwenkbereiche) und Reichweite (Zoom), Systembeschreibung

Datenschutz-Grundsätze für den Systemeinsatz: Deutlich sichtbarer Hinweis auf die Videoüberwachung und die verantwortliche Stelle im Zugangsbereich der betroffenen Räume (ggf. mehrsprachig), Verantwortlichkeiten festlegen, Art und Dauer der Speicherung der Videodaten, zugriffsberechtigte Personen, Datensicherheitsmaßnahmen, Schnittstellen, Aufbewahrung der Speichermedien, Rechte der Beschäftigten.

Aufzeichnung: Eine permanente Aufzeichnung erfolgt nicht.

Verarbeitung: Bilddaten des Videoüberwachungssystems werden ausschließlich in einem eigenständigen System verarbeitet und werden nicht an andere technische Systeme übertragen. Bilddaten des Videoüberwachungssystems werden nur innerhalb des Betriebs verarbeitet und nicht an „Dritte" im Sinne des BDSG weitergegeben (Ausnahme nur bei strafrechtlichen Delikten). Wo es möglich ist, sollten ausschließlich analoge geschlossene Systeme verwendet werden.

Auswertung: Bei Anhaltspunkten für einen strafrechtlichen Tatbestand bei Beschäftigten wird die Belegschaftsvertretung unverzüglich informiert. Die entsprechende Aufzeichnung wird ausschließlich in Anwesenheit der Belegschaftsvertretung ausgewertet (doppeltes Passwort). Die betroffenen Beschäftigten erhalten danach umgehend die Möglichkeit zur Stellungnahme.

Aufbewahrung: Eingesetzte Bilddatenträger werden durchnummeriert und mit dem Datum der Aufnahme versehen. Gespeicherte Bilddaten sind unter Verschluss zu halten.

Löschung: Die Bilddaten werden jeweils am Tagesende spätestens mit Beginn des nächsten Arbeitstags gelöscht. Videobänder oder andere Bilddatenträger mit aufgezeichneten Delikten werden nach Wegfall ihres Zwecks gelöscht.

Rechte des Betriebs-/Personalrats: Kontroll- und Überwachungsrechte, Mitbestimmung bei Änderung (z.B. auch für Schwenk- oder Zoombereich der Kameras) und Erweiterung des Systems, Recht auf Sachverständigen.

Außerdem:

- Abschaffung des Videoüberwachungssystems, wenn andere wirksame, aber weniger stark in die Persönlichkeitsrechte eingreifende Sicherheitstechniken auf dem Markt erhältlich sind;
- Beweisverwertungsverbot bei Verletzung der Betriebs-/Dienstvereinbarung;
- Rechte und Pflichten des Kontrollpersonals (z.B. Reinigungspersonal, Techniker, Administratoren) festschreiben;
- Beschäftigte über Standort und technische Möglichkeiten informieren;
- automatisches Logbuch zu allen wichtigen Aktionen;
- Verfahren für die Lösung von Konflikten über die Anwendung dieser Vereinbarung;
- Kündigungsfristen für die Vereinbarung, befristete Geltung (z.B. bei befristeter Überwachung).

dieses Interesse höher zu bewerten ist, als das Erreichen des mit der Videoüberwachung verfolgten konkreten Zwecks.

Im Fall einer Videoüberwachung ist ein solches „schutzwürdiges Interesse" immer gegeben und zwar in Form des grundrechtlich garantierten Persönlichkeitsrechts (Recht auf Schutz der Privat-/Intimsphäre, Recht am eigenen Bild[8]). Es geht


Foto: Bexixtech

also allein um die Frage, ob dieses Interesse das „überwiegende" ist.

Die Frage der Zulässigkeit einer Videoüberwachung am Arbeitsplatz ist also für Arbeitgeber und Belegschaftsvertretung mit recht komplizierten Abwägungen verbunden. Im Artikel ab Seite 13 wird dieser Prozess der „Verhältnismäßigkeitsprüfung" ausführlich dargestellt.

Heimlich überwachen, immer unzulässig

Videoüberwachung muss, egal ob öffentlich oder nicht, durch geeignete Maßnahmen erkennbar gemacht werden, z.B. durch ein Schild mit der Aufschrift „Achtung Videoüberwachung". Heimliche oder verdeckte Aufnahmen und Beobachtungen sind immer unzulässig, auch und vor allem an Arbeitsplätzen.

Demzufolge kann eine heimliche Überwachung auch nicht etwa durch eine Betriebs-/Dienstvereinbarung oder gar die mündliche Zustimmung der Belegschaftsvertretung „abgesegnet" werden! Eine solche Vereinbarung oder Absprache wäre rechtsunwirksam, ebenso wie die dadurch gewonnenen Bilder.

Gelegentlich werden Betriebs- oder Personalräte mit der Behauptung konfrontiert, dass Angestellte von ihrem Arbeitgeber sehr wohl heimlich mit Video überwacht werden dürften, immer dann jedenfalls, wenn ein konkreter Diebstahlsverdacht bestehe. Diese Behauptung stützt sich auf eine BAG-Entscheidung aus 2003, in der unter gewissen Voraussetzungen, quasi als Notwehrreaktion, eine heimliche Überwachung für zulässig gehalten wurde.[9]

Von dieser Entscheidung muss und darf sich aber keine Belegschaftsvertretung beeindrucken lassen. Inzwischen gelten veränderte gesetzliche Grundlagen und auch das BAG hat seit damals in mehreren Entscheidungen wieder den alten Grundsatz in Kraft gesetzt: »Heimliche Videoüberwachung ist ein Eingriff in das grundgesetzlich geschützte Persönlichkeitsrecht und deshalb unzulässig«.[10]

Speichern und Löschen von Videodaten

Da die Videoüberwachung durch aufgezeichnete Bilder gegenüber der bloßen Beobachtung eines Bildschirms den schwerer wiegenden Eingriff darstellt, ist eine Aufzeichnung nur rechtmäßig, wenn der mit der Videoüberwachung verfolgte Zweck eine Aufzeichnung wirklich erfordert. Ist das der Fall und wird aufgezeichnet, dann ist das Videomaterial nach Erreichung des Aufzeichnungszwecks und damit gemäß § 121 BGB unverzüglich (soll heißen: „ohne schuldhaftes Zögern") zu löschen.

Am sinnvollsten dürfte es sein, die Videoaufnahmen automatisiert, etwa durch Selbstüberschreiben zurückliegender Aufnahmen, unkenntlich zu machen. In jedem Fall gilt: Sobald Videoaufzeichnungen zur Erreichung ihres Zwecks nicht mehr benötigt werden, sind sie zu löschen.

Sollte es ausnahmsweise zur Videoüberwachung an Arbeitsplätzen kommen, ist die Zustimmung der Arbeitnehmervertretung einzuholen, etwa durch eine Betriebs- oder Dienstvereinbarung. In jedem Fall sind die Beschäftigten „durch geeignete Maßnahmen" darüber zu informieren, dass eine Videoüberwachung an ihrem Arbeitsplatz stattfindet. Das kann die deutlich sichtbar angebrachte Kamera mit einem zusätzlichen Hinweisschild sein (eine mündliche Information aber wäre nicht ausreichend).

Eine heimliche Überwachung ist immer und in jedem Fall verboten. Ebenso sind Videokameras zur Kontrolle der Arbeitsleistung nie erlaubt, da eine solche Kontrolle (wenn überhaupt) immer auf anderen, die Persönlichkeitsrechte weniger beeinträchtigenden Wegen erreicht werden kann.

Autoren

Dr. Eberhard Kiesche, Arbeitnehmerorientierte Beratung (AoB), Bremen, eberhard.kiesche@t-online.de; **Matthias Wilke**, Datenschutz- und Technologieberatung (dtb), Kassel, fon 0561 7057570, info@dtb-kassel.de

Lexikon

analog ▶ (ähnlich, entsprechend) wird heute meist als Gegenbegriff zu „digital" benutzt und meint soviel wie kontinuierlich oder stufenlos; die Zeit, eine Tonschwingung, ein Verlauf von Weiß zu Schwarz usw. sind eigentlich stufenlos; wenn ein Medium (Ton-/Videoband, Foto) diese Stufenlosigkeit nachbilden kann, spricht man von einer analogen Darstellung

digital ▶ (englisch: *digit* = Finger, Ziffer) Darstellung beliebiger Dinge und Abläufe in Form von Zahlen (z.B. Tonschwingungen in Zahlenwerten oder Buchstaben als Schlüsselziffern); erst die Digitalisierung erlaubt die Verarbeitung letztlich beliebiger Informationen mit Computern

Fußnoten

1 Vergl. BAG vom 29.6.2004 – 1 ABR 21/03.
2 www.focus.de/magazin vom 19.11.2007
3 www.tagesschau.de vom 21.11.2007
4 BAG vom 29.6.2004 – 1 ABR 21/03; siehe auch Wilke in Arbeitsrecht im Betrieb 2006, Seite 31
5 Vergl. Bundestags-Drucksache 14/4329, Seite 38
6 Vergl. BAG vom 21.8.1990 – 1 AZR 567/89
7 Vergl. BAG vom 29.6.2004 – 1 ABR 21/03; siehe H. Grimberg: „Video-Überwachung am Arbeitsplatz" in CF 2/05
8 § 22 Kunsturhebergesetz (KUG)
9 BAG vom 27.3.2003 – 2 AZR 51/02
10 Vergl. M. Wilke: „Dürfen Arbeitgeber ihre Angestellten mit Videoanlagen beobachten?" in Arbeitsrecht im Betrieb 2006, ab Seite 31 und P. Wedde: „Heimliche Video-Überwachung von Arbeitnehmern – zulässig?" in CF 1/07