

▮ *Videoüberwachung nimmt auch am Arbeitsplatz immer mehr zu. Insbesondere wenn diese heimlich erfolgt, stellt sich die Frage, ob der Arbeitgeber/Dienstherr das darf. Persönlichkeitsrechte der betroffenen Beschäftigten sind dabei zu wahren und die Vorgaben des Datenschutzes und der Mitbestimmung des Personalrats zu beachten.*

Videoüberwachung am Arbeitsplatz

Datenschutz und Mitbestimmung

Aktuell in der öffentlichen Diskussion ist das Thema Videoüberwachung durch die heimliche Videoüberwachung bei Lidl.¹ Bei Lidl sind nicht nur die Beschäftigten im Kassenbereich heimlich überwacht worden, sondern es ist auch davon auszugehen, dass Kunden und unter Umständen auch deren Geheimzahlen bei bargeldloser Bezahlung heimlich überwacht worden sind. Vor diesem Hintergrund stellt sich wohl jeder Beschäftigte die Frage: »Was weiß mein Chef von mir?«² Dass heimliche Videoüberwachung in Betrieben und Dienststellen keine Seltenheit ist, kann auch daran abgelesen werden, dass sich Arbeitsgerichte bis hin zum BAG mit dem Thema der heimlichen Videoüberwachung beschäftigten mussten.³

Beim Einsatz von Videoüberwachung sind der Schutz der Persönlichkeitsrechte, die Vorgaben des BDSG und das Mitbestimmungsrecht des Personalrats zwingend zu beachten. Nachfolgend werden die zunehmende Videoüberwachung geschildert, die rechtlichen Grenzen einer – heimlichen – Videoüberwachung aufgezeigt und die Handlungsmöglichkeiten des Personalrats skizziert.

I. Videoüberwachung greift um sich

Der »gläserne Bürger und Beschäftigte« oder »Big brother ist watching you« scheinen das passende Negativszenario zu sein. Wobei es nicht ein »großer Bruder« ist, sondern viele »kleine Brüder« aktiv sind, die alle Bürger/Beschäftigte irgendwie überwachen. So waren nach Schätzungen der Industrie in Deutschland 1998 bei einer hohen Dunkelziffer und rasant zunehmenden Absatzzahlen bereits mehr als 500 000 Videokameras installiert.⁴ Für Liegenschaften des Bundes (Bundesministerien und BKA) hat die Bundesregierung im Jahre 2001 eine Gesamtzahl von 14.777 Kameras für 55 Liegenschaften genannt.⁵ Selbst sensible Bereiche wie Umkleidekabinen in Hallenbädern werden videoüberwacht.⁶ Heute werden gerade auch wegen der sinkenden Preise weit mehr Kameras im Einsatz sein. Denn über den Fachhandel und über Versandhäuser werden mittlerweile preisgünstig »Videowanzen« angeboten, die eine für den Bürger/Kunden und auch für Beschäftigte unauffällige Überwachung der Arbeits- und Verkaufsräume ermöglichen. Videoanlagen verfügen in der Regel über schwenkbare mit Zoom

ausgestattete Kameras, wobei die Bilder digital gespeichert werden und mit entsprechender Software ausgewertet werden können. Es kommen aber auch Kameras zum Einsatz, deren Objektiv kleiner als ein Ein-Cent-Stück und kaum zu erkennen ist.⁷ Zugespielt kann festgestellt werden: »Jetzt ist die Technik ausgereift und erschwinglich, um alle im Auge behalten zu können.«⁸

Kameras werden installiert in Banken im Bereich der Geldautomaten und Kassen, in Kaufhäusern, Parkhäusern, Fahrstühlen, Taxen oder auch an Tankstellen. Zunehmend kommen Kameras aber auch auf öffentlichen Plätzen, z.B. in Bereichen von Bahnhöfen, oder auf und an Ampeln in Städten oder an Autobahnen zum Einsatz.⁹ Mit der Verbreitung des Internets kamen aber auch Ideen auf, mit sogenannten Web-Cams die Arbeit der Beschäftigten in Behörden aufzunehmen und die Bilder im Internet für jedermann abrufbar vorzuhalten.¹⁰ Videoanlagen kommen im Rahmen sogenannter biometrischer Verfahren zum Einsatz. Mittlerweile ist die Digitalisierung und auch die Vergleichbarkeit des menschlichen Bildes so weit entwickelt, dass Zugangskontrollsysteme gezielt Personen herausfinden können.¹¹ So kann durch Speicherung und Abgleich von Bildern der Zugang zu bestimmten Bereichen oder Gebäuden gewährt oder verwehrt werden. Die technische Entwicklung geht jedoch weiter. So entwickelte die Universität Leeds die sogenannte »Thinking Camera«. Sie unterscheidet zwischen »Gut« und »Böse«. So kann sie erkennen, wie sich Menschen üblicherweise in bestimmten Situationen, wie z.B. beim Betreten eines Gebäudes oder eines Parkhauses,

1 Vgl. Der Stern, Heft 14, 27.3.2008, S. 48 ff.

2 So titelte Die Zeit, Nr. 16, 10.4.2008, S. 23 ff.

3 Vgl. z.B.: LAG Köln v. 30.8.1996 – 12 Sa 639/96 –, RDV 4/1997, 183 ff.; BAG v. 27.3.2003 – 2 AZR 51/02 –, AiB 2004, 761.

4 Vgl. LfD Niedersachsen, 15. Tätigkeitsbericht 1999/2000, abzurufen über das Internet: www.lfd.niedersachsen.de; Köppen, Datenerhebung durch Arbeitgeber und Videoüberwachung im Betrieb, FfF-Kommunikation 2/2001, S. 30.

5 Similis (Hrsg.), Kommentar zum Bundesdatenschutzgesetz, 6. Aufl., § 6b Rn. 2.

6 Vgl. Landesbeauftragter für den Datenschutz in Baden-Württemberg, 24. Tätigkeitsbericht, Ziffer 8, S. 103.

7 Der Stern (Fn. 1), S. 48.

8 Vgl. Die Zeit v. 30.12.1998, S. 2.

9 Vgl. hierzu: Weichert, Öffentliche Audio- und Videoüberwachung, DANA 1/1999, 4 ff.

10 Vgl. Edenfeld, PersR 2000, 323 ff.

11 Vgl. Bäumer, Probleme der Videoaufzeichnung und -überwachung, in: Möller/v. Zeuschwitz (Hrsg.), Videoüberwachung – Wohltat oder Plage?, S. 59.

benehmen. Weicht das Benehmen vom »Üblichen« ab, gibt das System »Alarm« und rät den Betreibern sich mit der Person näher zu befassen.¹²

Mit Videoüberwachung wird der Beschäftigte u.U. während der gesamten Arbeitszeit überwacht. Dementsprechend müssen sie sich bei jeder ihrer Bewegungen kontrolliert fühlen. Ihre Mimik und Gestik, bewusste oder unbewusste Gebärden, der Gesichtsausdruck bei der Arbeit oder bei der Kommunikation mit Vorgesetzten und Kollegen unterliegen stets der Möglichkeit dokumentierender Beobachtung. Damit entsteht ein Druck, sich möglichst unauffällig zu benehmen, setzen sich die Beschäftigten anderenfalls der Gefahr aus, später wegen etwa abweichender Verhaltensweisen Gegenstand von Kritik, Spott oder Sanktionen zu werden.¹³

Jeder, der mit offenen Augen durch die Lebens- und Arbeitswelt geht, kann die Kameras u.U. selbst entdecken oder aber er wird durch entsprechende Hinweisschilder auf diese hingewiesen. Auch die Rechtsprechung zum Thema Videoüberwachung zeigt an, dass in den Betrieben und Verwaltungen immer mehr Kameras zum Einsatz kommen. So haben nicht nur die Pförtner Bildschirme zur Kontrolle der Eingangsbereiche, sondern neben Lagerbereichen (z.B. städtische Bauhöfe) werden häufig Produktionsabläufe mit Kameras überwacht.

Auch wenn Videoüberwachung von der technischen Seite her nicht an Grenzen zu stoßen scheint, gibt es von der rechtlichen Seite jedoch Grenzen, die zwingend zu beachten sind. Denn was hilft die beste Videoaufzeichnung, wenn sie gerichtlich nicht zu verwerten ist und der Betroffene sogar erfolgreich einen Schmerzensgeldanspruch durchsetzen kann. Eine widerrechtliche Videoaufzeichnung und Weitergabe der Bilder kann zu Schadensersatz-, Beseitigungs-, Unterlassungs- und sogar zu Schmerzensgeldansprüchen führen. Der Einsatz von Videotechnik in Betrieb oder Dienststelle ist als technische Einrichtung mitbestimmungspflichtig. Und nicht zuletzt sind die datenschutzrechtlichen Vorgaben beim Videoeinsatz zu berücksichtigen.¹⁴

II. Allgemeines Persönlichkeitsrecht

Bei Videoüberwachung ist das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 in Verbindung mit Art. 1 Abs. 1 GG zu beachten. Bei diesem allgemeinen Persönlichkeitsrecht, das auch im Arbeitsleben anzuwenden ist¹⁵, handelt es sich um ein Rahmenrecht, dessen Umfang und Grenzen sich nicht eindeutig bestimmen lassen. Das allgemeine Persönlichkeitsrecht umfasst neben dem Recht am gesprochenen Wort, dem Recht am Charakterbild, dem Recht an der Ehre, dem Recht an Intim- und Privatsphäre, dem Recht auf informationelle Selbstbestimmung auch das Recht am eigenen Bild.¹⁶ Das vom BVerfG entwickelte Recht auf informationelle Selbstbestimmung findet auch auf alle Maßnahmen der Videoüberwachung Anwendung. Videoüberwachung gehört wegen der hohen Informationsdichte, die die Bildinformationen aufweisen, zu den intensivsten Formen der Erhebung, Verarbeitung und Nutzung personenbezogener

Daten.¹⁷ So gelten auch für die Videoüberwachung die vom BVerfG getroffenen Aussagen: »Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen.«¹⁸

Das Recht am eigenen Bild schützt nicht nur vor jeder Art unbefugter Verbreitung und Veröffentlichung, sondern auch vor jeder Art der unbefugten Anfertigung eines Bildes einer Person. Darunter fällt jede Art durch technische Mittel bewirkte Direktübertragung des Erscheinungsbildes einer Person, so auch die Überwachung der Arbeitnehmer bei der Arbeit durch offene oder heimliche fotografische Einzelaufnahmen, Film-, Fernseh- oder Videokameras. Der Einsatz dieser technischen Mittel kann aber zulässig sein, wenn es in erster Linie um die Beobachtung von Arbeitsprozessen geht oder aus Sicherheitsgründen (Gebäudesicherung) erfolgt.¹⁹

Will der Arbeitgeber/Dienstherr Videoüberwachung einsetzen, so führt dieses in jedem Fall zu einer Beschränkung des allgemeinen Persönlichkeitsrechts. Er kann mit dem Personalrat eine Regelung – sinnvoller Weise in Form einer Dienstvereinbarung – treffen. Mögliche Einschränkungen des Persönlichkeitsrechts bestimmen sich nach dem Grundsatz der Verhältnismäßigkeit. Danach muss eine Videoüberwachung und eine entsprechende Regelung im Rahmen einer Dienst- oder Betriebsvereinbarung **geeignet, erforderlich** und unter Berücksichtigung der gewährleisteten Freiheitsrechte **angemessen** sein, um den erstrebten Zweck zu erreichen. Geeignet ist eine Regelung (Dienstvereinbarung) dann, wenn mit ihrer Hilfe der erstrebte Erfolg gefördert werden kann. Dabei steht Arbeitgeber und Personalrat ein gewisser Beurteilungsspielraum zu. Erforderlich ist die Regelung dann, wenn kein anderes, gleich wirksames, aber das Persönlichkeitsrecht weniger einschränkendes Mittel zur Verfügung steht. Angemessen ist eine Regelung dann, wenn sie verhältnismäßig im engeren Sinn erscheint. Es bedarf hier einer Gesamtabwägung zwischen der Intensität des Eingriffs und dem Gewicht der ihn rechtfertigenden Gründe. Die Grenze der Zumutbarkeit darf hier nicht überschritten werden.²⁰

III. Regelung im BDSG

Das BDSG gilt für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten (§ 1 Abs. 2 BDSG). So ist bei Videoüberwachung eine Zulässigkeitsprüfung gemäß § 4 BDSG vorzunehmen. Zusätzlich gibt es im BDSG eine

12 Vgl. Bäumler (Fn. 11), S. 55 f.

13 Vgl. BAG v. 29.4.2004 – 2 AZR 51/02 –, DuD 2004, 750.

14 Vgl. Ahlf, Computer und Recht 1991, 424.

15 Vgl. hierzu Edenfeld (Fn. 1010), 325 f.; Ahlf (Fn. 14), 424; Kraft/Wiese/Kreutz/Oetker/Raab/Weber/Franzen, BetrVG-GK, § 75, Rn. 97 ff.

16 Vgl. GK-BetrVG, (Fn. 15), § 75 Rn. 97 ff.

17 Vgl. v. Zeszschwitz, Videoüberwachung, in: Rossnagel (Hrsg.), Handbuch Datenschutzrecht, 2003, Rn. 7.

18 BVerfG v. 15.12.1983, NJW 1984, 422.

19 Vgl. GK-BetrVG, (Fn. 15), § 75 Rn. 97.

20 Vgl. BAG (Fn. 3).

Vorgabe zur Videoüberwachung, die jedoch ausschließlich für die »Beobachtung öffentlich zugänglicher Räume« gilt.

Die Regelung zur Videoüberwachung (§ 6b BDSG) gilt sowohl für den öffentlichen Bereich des Bundes als auch den nicht-öffentlichen Bereich. Mit dieser Regelung zur Videoüberwachung wird der Anwendungsbereich des BDSG zusätzlich ausgeweitet. So fiel nach dem alten BDSG eine bloße Beobachtung (ohne Aufzeichnung) nicht in den Anwendungsbereich des BDSG, da in diesem Fall keine Datenverarbeitung »in Dateien« stattfindet. Das Anliegen des Gesetzgebers, Videoüberwachung zu regeln, wird aus der Gesetzesbegründung deutlich: »Die in weiten Bereichen durch öffentliche und nicht-öffentliche Stellen bereits durchgeführte Videoüberwachung öffentlich zugänglicher Räume erhält durch die Vorschrift eine gesetzliche Grundlage, die der Wahrung des informationellen Selbstbestimmungsrechts Rechnung trägt. Da bereits die Beobachtung selbst erfasst wird, kommt es nicht auf das Erfordernis einer anschließenden Speicherung des Bildmaterials an, um datenschutzrechtlich relevant zu sein. Die Vorschrift erfasst nur öffentlich zugängliche Räume wie etwa Bahnsteige, Ausstellungsräume oder Schalterhallen. Für nicht-öffentlich zugängliche Räume sind besondere Regelungen, beispielsweise im Rahmen eines Arbeitnehmer-Datenschutzgesetzes erforderlich.«²¹

Neben der Regelung zur Videoüberwachung selbst, kommen aber auch weitere Vorgaben des BDSG zum Tragen, wie z.B. die Regelung zur Datenvermeidung und Datensparsamkeit (§ 3a BDSG). In jedem Fall ist zu prüfen, ob eine Vorabkontrolle durchzuführen ist.²² So ist eine Vorabkontrolle dann durchzuführen, wenn Datenverarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen. Solche Risiken liegen regelmäßig vor, wenn Überwachungskameras nicht punktuell, sondern durch die verantwortliche Stelle in größerer Zahl und zentral kontrolliert eingesetzt werden. Ebenso kann die verwendete Technik (etwa bei schwenkbaren Kameras mit hoher Auflösung der gewonnenen Bilder) zu einem solchen Risiko führen.

1. Vorgaben des § 6b BDSG

In § 6b Abs. 1 BDSG ist die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) geregelt. Die Verarbeitung und Nutzung von Daten (Aufzeichnung und Speicherung) werden gesondert in § 6 Abs. 3 und 5 BDSG geregelt.

a) Beobachten

In § 6b BDSG wird unterschieden zwischen der Beobachtung (Abs. 1) und der Aufzeichnung in Form von Verarbeitung und Nutzung (Abs. 3). So genügt die reine Beobachtung, ohne dass eine Aufzeichnung der Bilder erfolgen muss, für die Anwendung des § 6b BDSG aus. Unter Beobachtung ist jede Tätigkeit zu verstehen, die darauf gerichtet ist, Geschehnisse und Personen mit Hilfe geeigneter Geräte und Einrichtungen zu überwachen.²³ Im Unterschied zum Erheben setzt Beobachten nicht notwendigerweise eine Erfassung personenbezogener Daten voraus. Dieses hat aber auch zur Folge, dass das Aufstellen oder Anbringen von Kameraattrappen, sogenannten Dummies, nicht der Regelung des § 6b BDSG unterliegt, denn Voraussetzung ist die Beobachtung mittels einer optisch-elektronischen Einrichtung.²⁴

b) Öffentlich zugängliche Räume

Voraussetzung für die Anwendung dieser Regelung ist die Installation der Videoüberwachungs-Anlage in »öffentlich zugänglichen Räumen«. Sowohl in der Rechtsprechung als auch in der Literatur gibt es keine Definition des Begriffs »öffentlich zugänglicher Raum«. Meistens werden, wie auch in der Gesetzesbegründung zum BDSG, nur Beispiele aufgezählt. In der Gesetzesbegründung werden »Bahnsteige, Ausstellungsräume eines Museums, Verkaufsräume oder Schalterhallen« genannt. Entscheidend für die Anwendung der Regelung ist nicht, dass es Einrichtungen (innerhalb oder außerhalb von Gebäuden) sind, die im öffentlichen Eigentum stehen, sondern dass es sich um Bereiche handelt, die ohne jede Voraussetzung von jedermann genutzt werden können.²⁵ Im Gegensatz dazu ist bei einem nicht öffentlich zugänglichen Raum der Kreis der Personen, der Zutritt hat, begrenzt. So sind Firmen- oder Werksgelände typischerweise keine öffentlich zugänglichen Räume. Davon ist in jedem Fall auszugehen, wenn durch Schilder am Werksgelände darauf hingewiesen wird, dass nur Befugten den Zutritt erlaubt ist. Im Einzelfall kann jedoch ein »Firmengelände« öffentlich zugänglicher Raum sein, wenn z.B. ein Unternehmen in seinem Eingangsbereich (Treppenhaus, Foyer) Kunstausstellungen durchführt und jede Person Zutritt hat. Hier

Redaktionshinweis

Das Seminar »Datenschutz in der arbeitsrechtlichen Praxis« am 26.8.2008 in Bad Homburg vermittelt u.a. das aktuelle Datenschutzrecht, den Beschäftigtendatenschutz, den Datenschutz im Personalratsbüro sowie die Handlungsmöglichkeiten des Personalrats beim Abschluss von Dienstvereinbarungen zum Datenschutz.

Kontakt:

ilona.hofmann@aib-wissen.de

Telefon: 069/13 30 77 – 671

21 Bundesministerium des Innern (Hrsg.), Gesetz zur Änderung des Bundesdatenschutzgesetzes und anderer Gesetze, Synopse zu den am 23.5.2001 in Kraft tretenden Änderungen (nur) des BDSG (mit Begründung des Regierungsentwurfs, BT-Drs. 14/4329 und Begründung zur Beschlussempfehlung des BT-Innenausschusses vom 4.4.2001, BT-Drs. 14/5793), Begründung zu § 6b BDSG.
22 Vgl. zur Vorabkontrolle: Schierbaum, Computer Fachwissen, 11/2001, 25 ff.
23 Vgl. Bergmann/Möhrle/Herb, Datenschutzrecht, Loseblatt, § 6b Rn. 18.
24 Vgl. Simitis (Hrsg.), (Fn. 55), § 6b Rn. 37; Däubler, Gläserne Belegschaften? Datenschutz in Betrieb und Dienststelle, 4. Auflage, S. 154.
25 Vgl. Königshofen, RDV 5/2001, 220.

ist es geradezu gewollt, dass diese Bereiche öffentlich zugänglich sind.

c) Optisch-elektronische Einrichtung

Die Kontrolle muss durch »optisch-elektronische Einrichtungen« erfolgen. Hierunter fallen wohl in erster Linie festinstallierte Videokameras und Webcams. Kameras, Ferngläser und moderne Fotoapparate sind wohl nicht mit einzubeziehen, da es sich nicht um »Einrichtungen« handelt. Denn bei Einrichtungen muss es sich um festinstallierte oder aufgestellte Überwachungssysteme handeln. Wie bereits erwähnt fallen Attrappen nicht unter diese Regelung.

d) Zulässigkeit der Video-Beobachtung

Das BDSG enthält in § 6b Abs. 1 drei Vorgaben für die Zulässigkeit von Video-Beobachtung. Diese bilden die Grundlage für die rechtmäßige Verwendung von Videoanlagen. Die Video-Beobachtung öffentlich zugänglicher Räume ist zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist.

Die Beobachtung öffentlich zugänglicher Räume ist zulässig, soweit sie **zur Aufgabenerfüllung öffentlicher Stellen** (des Bundes) erforderlich ist (§ 6b Abs. 1 Nr. 1 BDSG). Unter diese erste Zulässigkeitsvariante fallen **nicht** die nicht-öffentlichen Stellen (Privatbetriebe, Vereine, Stiftungen). Diese Regelung gilt nur für öffentliche Stellen und zwar soweit bereichsspezifische Gesetze des Bundes Regelungen zur Videoüberwachung enthalten. Mit dem Begriff »Aufgabenerfüllung« sind die gesetzlichen Aufgaben gemeint. Bereichsspezifische gesetzliche Regelungen zur Videoüberwachung gehen dem § 6b BDSG vor und sind hier nicht gemeint. D.h. die Videoüberwachung muss sich nicht direkt aus einem Gesetz ergeben, sondern es reicht aus, wenn die Videoüberwachung einen gesetzlichen Auftrag unterstützt. Unter diese Regelung fällt z.B. die Videoüberwachung, mit der die Funktionsfähigkeit öffentlich zugänglicher Räume gewährleistet werden kann, die zur Aufgabenerfüllung der öffentlichen Stellen des Bundes verwendet werden (»Gebäudesicherheit«, »Zugangskontrolle«).²⁶

Die Regelung, dass die Videoüberwachung »zur Wahrnehmung des Hausrechts zulässig« ist, richtet sich an öffentliche und nicht-öffentliche Stellen. Hierunter fallen Videobeobachtungen, die dazu dienen, die Begehung von Straftaten (Diebstahl, Sachbeschädigungen) zu verhindern oder aufzuklären. Hierzu zählt auch die Überwachung von Hausverboten. Zivilrechtlich ergibt sich das Hausrecht aus den Abwehransprüchen des Eigentümers nach §§ 859 ff, 904, § 1004 BGB. Gründe und Schranken können sich aus spezialgesetzlichen Bestimmungen wie bspw. dem Mietrecht (§ 535 BGB) oder dem Wohnungseigentümergebot (§ 21 WEG) ergeben.

Die Möglichkeit »zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke« ist erst im Laufe des Gesetzgebungsverfahrens in das BDSG aufgenommen worden. Diese Regelung gilt wie die vorherige sowohl für den öffentlichen als auch nicht-öffentlichen Bereich. Der Begriff »Wahrnehmung berechtigter Interessen« ist dem § 28 Abs. 1 Nr. 2 BDSG entlehnt, der als Basis für eine rechtmäßige Datenverarbeitung dienen kann. Was im Einzelfall ein berechtigtes Interesse ist, entscheidet nicht allein die verantwortliche Stelle im eigenen subjektiven Ermessen. Nach der Gesetzesbegründung muss das Interesse objektiv begründbar sein, was auch bedeutet, dass das Interesse des Betroffenen am Schutz seines Persönlichkeitsrechts Berücksichtigung finden muss. So kann etwa der Zweck der Diebstahlprävention keinesfalls die Überwachung von Toiletten oder Umkleidekabinen rechtfertigen.

Zusätzlich muss die Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erfolgen. Dieses bedeutet, dass im Vorfeld (vor Installation der Videoanlage) genau die Zwecke (z.B. Verhinderung von Diebstahl) festgelegt werden müssen. Diese festgelegten Zwecke, die im Grunde genommen schriftlich fixiert werden müssen (auch wenn dies im BDSG nicht direkt vorgeschrieben ist), dürfen später nicht so ohne Weiteres verändert oder erweitert werden. So kann eine Bank, die im Bereich der Geldautomaten und Selbstbedienungsterminals Kameras zur Verhinderung von Sachbeschädigung (Vandalismus) und Diebstahl einsetzt, die Daten nicht zur Messung (Beobachtung) von Kundenströmen nutzen.

Für alle drei Zulässigkeitsalternativen setzt die Zulässigkeit der Videoüberwachung weiterhin voraus, dass sie zur Erreichung der in den einzelnen Punkten genannten **Zwecke erforderlich** sind. Erforderlichkeit heißt, dass mit der Videoüberwachung das beabsichtigte Ziel auch erreicht werden kann und dass die Überwachung notwendig ist. So ist etwa in Warenhäusern immer zu prüfen, ob Diebstahl nicht durch andere Methoden zur Sicherung der Waren erreicht werden kann. Diese notwendige Prüfung ergibt sich u.a. auch aus dem Gebot der »Datenvermeidung und Datensparsamkeit«.

Die Beweislast für die konkrete und rechtzeitige Festlegung der Zwecke liegt bei der für die Videobeobachtung verantwortlichen Stelle. Kann sie keinen ausreichenden Nachweis führen, ist die Videoüberwachung unzulässig.

e) Information der Betroffenen

Findet Videoüberwachung in öffentlich zugänglichen Räumen statt, »ist der Umstand der Beobachtung durch geeignete Maßnahmen erkennbar zu machen« (§ 6b Abs. 2 BDSG). Was nun geeignete Maßnahmen sind, entscheidet die Stelle, die die Videoüberwachung einsetzt. Man wird davon ausgehen müssen, dass Schilder, die groß genug sein und gut sichtbar angebracht werden müssen, jedenfalls dann geeignete Maßnahmen sind, wenn darauf auch Piktogramme (für Fremdsprachler) und der Name der verantwortlichen Stelle angebracht

²⁶ Vgl. Simitis (Hrsg.), (Fn. 5), § 6b Rn. 46.

sind. Unter Umständen muss die »verantwortliche Stelle« dann nicht auf dem Hinweisschild angebracht werden, wenn dieses Schild direkt am Eingangsbereich des Gebäudes angebracht ist.

f) Aufzeichnung und Nutzung von Videodaten

In § 6b Abs. 3 BDSG sind über die Zulässigkeitsvoraussetzungen für die reine Videobeobachtung hinaus auch die Verarbeitung und Nutzung der im Wege der Videobeobachtung gewonnenen Daten geregelt. So kann aus der Zulässigkeit der Beobachtung nicht auch schon auf die Zulässigkeit der Verarbeitung (hierzu gehört die Speicherung und Übermittlung von Daten) und Nutzung der Daten geschlossen werden. Das heißt, dass dieses in einem gesonderten Prüfschritt festgestellt werden muss. So ist die Verarbeitung und Nutzung von Daten, die durch Videobeobachtung gewonnen worden sind, nur zulässig, »wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen überwiegen« (§ 6b Abs. 3 BDSG). Nach der Gesetzesbegründung kommt der Interessenabwägung herausragende Bedeutung zu: Schutzwürdige Interessen des Betroffenen sind in besonderer Weise berührt, wenn automatisierte Verfahren beispielsweise zum Vergrößern und Herausfiltern einzelner Personen, zur biometrischen Erkennung, zum Bildabgleich oder zur Profilerstellung eingesetzt werden oder zu solchen Zwecken verfügbar sind. Denn derartige Maßnahmen greifen in besonders gravierender Weise in das informationelle Selbstbestimmungsrecht des Betroffenen ein, so dass regelmäßig das Interesse des Betroffenen überwiegt, nicht zum Objekt automatisierter Verarbeitung gemacht zu werden. Zusätzlich ist nach der Gesetzesbegründung folgender Grundsatz zu berücksichtigen: Je leistungsfähiger die Möglichkeiten automatisierter Auswertung von Videoaufnahmen von Personen im Zuge technischer Entwicklungen werden, desto mehr Gewicht bekommt das informationelle Selbstbestimmungsrecht des Betroffenen im Rahmen des Abwägungs- und Prüfungsprozesses.

Zusätzlich besteht eine Benachrichtigungspflicht, wenn die durch Videoüberwachung gewonnenen Daten einer Person zugeordnet werden (§ 6b Abs. 4 BDSG).

Die durch Videoüberwachung gewonnenen 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 Abs. 5 BDSG). So werden bei einer Videoüberwachung in einem Warenhaus zur Vermeidung von Diebstählen die Daten jeden Abend gelöscht werden müssen, da die Aussicht, Personen durch nichtzeitnahe Auswertungen von Aufzeichnungen zu fassen, so gut wie ausgeschlossen ist.

2. Nicht öffentlich zugängliche Räume

Sollen nicht öffentlich zugängliche Räume überwacht werden, gilt nicht der § 6b BDSG, sondern es gelten die allgemeinen Vorgaben des BDSG. So sind, wenn die Be-

schäftigten²⁷ von der Videoüberwachung betroffen sind, vor allem die § 28 BDSG und der § 4 Abs. 2 BDSG von Bedeutung. Nach § 4 Abs. 2 BDSG sind personenbezogene Daten beim Betroffenen zu erheben.²⁸ Dieser Grundsatz ist ein unmittelbarer Ausfluss des Volkszählungsurteils und des informationellen Selbstbestimmungsrechts. Der Betroffene soll wissen, wer was wann über ihn sammelt, speichert und verarbeitet. Deshalb sind grundsätzlich personenbezogene Daten beim Betroffenen selbst und nicht hinter seinem Rücken oder sonst ohne sein Wissen zu erheben. »Beim Betroffenen« bedeutet mit seiner Kenntnis und seiner Mitwirkung.²⁹ Schon allein durch diese Vorgabe ist eine heimliche Videoüberwachung von Beschäftigten ausgeschlossen.

Nach § 28 BDSG ist das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke zulässig

- wenn es der Zweckbestimmung des Vertragsverhältnisses oder vertragsähnlichen Vertrauensverhältnisses mit dem Betroffenen dient,
- soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt.

Eine Videoüberwachung eines Beschäftigten wird man nicht aus der Zweckbestimmung seines Arbeitsvertrages herleiten können. Zugleich ist das schutzwürdige Interesse des Beschäftigten gerade bei dieser Überwachungstechnik hier höher anzusiedeln als das Interesse des Arbeitgebers (verantwortliche Stelle). So wird ein Beschäftigter in der Regel von Videoüberwachung nur dann betroffen sein können, wenn es z.B. um Überwachung von Kaufhäusern, Museen, Schwimmbädern, Parkhäusern, Parkplätzen geht. Diese Videoaufzeichnung ist dann meist eine unbeabsichtigte Nebenfolge anderer Zweckbestimmungen. In diesen Fällen wird man z.B. durch den Abschluss einer Dienstvereinbarung die Nutzung und Auswertung der Beschäftigtendaten regeln bzw. unterbinden. Besonders sensible Bereiche müssen generell von Videoüberwachung freigehalten werden. Hierzu zählen z.B. Einzelbüros, Umkleidekabinen, Sanitärbereiche sowie Untersuchungsräume in Kliniken und Praxen.³⁰

²⁷ In § 12 BDSG ist für die Verarbeitung personenbezogener Daten der Beschäftigten im öffentlichen Bereich des Bundes ein Verweis enthalten: »Werden personenbezogene Daten für frühere, bestehende oder zukünftige dienst- oder arbeitsrechtliche Rechtsverhältnisse erhoben, verarbeitet oder genutzt, gelten anstelle der §§ 13 bis 16, 19 bis 20 der § 28 Abs. 1 und 3 Nr. 1 sowie die §§ 33 bis 35, auch soweit personenbezogene Daten weder automatisiert verarbeitet noch in nicht automatisierten Dateien verarbeitet oder genutzt oder dafür erhoben werden.« Werden Besucher/Bürger von der Videoüberwachung erfasst, gelten für den öffentlichen Bereich des Bundes die §§ 13 ff. BDSG.

²⁸ In § 4 Abs. 2 BDSG sind Ausnahmen vorgesehen, die jedoch beim Videoeinsatz in Bezug auf Beschäftigte nicht zum Tragen kommen.

²⁹ Vgl. Goia/Schomerus, Bundesdatenschutzgesetz, 9. Aufl., § 4 Rn. 21.

³⁰ Vgl. v. Zezschwitz, (Fn. 17), Rn. 97

IV. Recht am eigenen Bild gemäß KUG

Neben dem allgemeinen Persönlichkeitsrecht und den Vorgaben des BDSG kann auch das sogenannte Kunsturhebergesetz (KUG)³¹ zur Anwendung kommen. Das Recht am eigenen Bild ist in den §§ 22-24 KUG geregelt und versetzt den Abgebildeten in bestimmten Grenzen in die Lage, über die Verbreitung seines Bildnisses zu entscheiden. Es handelt sich um ein Persönlichkeitsrecht zum Schutz ungewollter Darstellung, woraus sich die Unzulässigkeit einer Veröffentlichung des Bildes einer Person schon dann ergibt, wenn sie ohne Einwilligung des Abgebildeten geschieht. Vor diesem Hintergrund kann in der Regel die Einstellung von Bildern der Mitarbeiter auf die unternehmenseigene oder behördeneigene Homepage nur mit Einwilligung des Beschäftigten erfolgen. Die Herstellung von Bildern, also die Videoüberwachung als solche, wird vom Wortlaut der §§ 22f. KUG nicht erfasst.³² D.h. das KUG erfasst nicht das Entstehen, Speichern, Verändern oder Nutzen von Bildern. Hier sind dann das allgemeine Persönlichkeitsrecht bzw. die Vorgaben des BDSG zu beachten.

V. Videoüberwachung bei Zugangskontrolle

Werden Videoanlagen als Zugangskontrollsysteme genutzt und werden die Systeme »als verlängertes Auge« des Pförtners eingesetzt, sind die beschriebenen Datenschutzvorgaben einzuhalten. Besondere datenschutzrechtliche Probleme werfen jedoch biometrisch angelegte Zugangskontrollsysteme³³ auf, die auf Videoüberwachung gestützt sind. Hier werden über eine Speicherung von Bildern einzelner Personen und der Festlegung von charakteristischen Merkmalen der Zutritt zu einem Gebäude oder einem bestimmten Arbeitsbereich gesteuert. Ein solches System ist ohne eine langfristig angelegte Speicherung personenbezogener Daten (Fotos) von zutrittsberechtigten Personen nicht denkbar.³⁴ In entsprechenden Systemen können personenbezogene Daten nur mit Einwilligung des Betroffenen verarbeitet und genutzt werden. Neben der Durchführung einer Vorabkontrolle sind auch die Vorgaben des § 6a BDSG einzuhalten. Denn bei diesen Zugangskontrollsystemen handelt es sich um sogenannte »automatisierte Einzelentscheidungen«. Danach dürfen Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten, die der Bewertung einzelner Persönlichkeitsmerkmale dienen, gestützt werden. Dabei ist es gleichgültig, ob diese automatisierten Einzelentscheidungen negative oder positive Folgen für den Betroffenen nach sich ziehen. Betrachtet man die Vorgaben des § 6a BDSG ist fraglich, ob entsprechende Zugangskontrollverfahren überhaupt zum Einsatz kommen dürfen.

VI. Beteiligungsrechte des Personalrates

Vor der Einführung von Videoüberwachung (in nicht-öffentlichen und auch öffentlich zugänglichen Räumen) ist der Personalrat zu informieren. Das Informationsrecht ist in § 68 Abs. 2 BPersVG und entsprechenden Vorschriften der Landespersonalvertretungsgesetze verankert, wobei die Information in der Planungsphase (»rechtzeitig«) erfolgen und zudem abschließend und vollständig sein muss. Folgende Informationen benötigt der Personalrat in jedem Fall³⁵:

- eingesetzte Geräte (Systemaufbau), etwa Kameras, u.U. Dummies, Monitore, Aufzeichnungsgeräte, Standorte der Geräte,
- zugriffsberechtigte Personen,
- bei Aufzeichnungen die Lösungsfristen, Sicherungen der Aufzeichnungen vor unberechtigtem Zugriff,
- u.U. Verbindung zu anderen DV-Systemen und
- die Vorabkontrolle und datenschutzrechtliche Stellungnahme des betrieblichen/behördlichen Datenschutzbeauftragten.

Die Praxis zeigt, dass der Personalrat selten rechtzeitig und umfassend informiert wird. So wird ihm die datenschutzrechtliche Stellungnahme häufig vorenthalten. Das heißt dann auch, dass entsprechende Fristen zur Stellungnahme nicht laufen, da keine vollständige und abschließende Information erfolgt ist. Hierauf sollte der Personalrat die Dienststelle schriftlich hinweisen und fehlende Informationen einfordern.

Neben dem Informationsrecht kommt das Mitbestimmungsrecht des Personalrats nach § 75 Abs. 3 Nr. 17 BPersVG und entsprechenden Vorschriften der Landespersonalvertretungsgesetze zum Tragen. Danach hat der Personalrat mitzubestimmen bei der Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen. Bei Videoüberwachungs-Systemen handelt es sich um mitbestimmungspflichtige technische Überwachungseinrichtungen. Dabei ist der Personalrat auch zu beteiligen, wenn lediglich Eingangs- oder Arbeitsbereiche eines Unternehmens oder Geldautomaten in Kreditinstituten überwacht werden sollen. Denn in diesen Bereichen werden sich auch die Beschäftigten aufhalten. Eine heimliche Videoüberwachung (verdeckt und ohne Wissen der Beschäftigten) ist nach der Rechtsprechung des BAG³⁶ ein unzulässiger Eingriff in die Per-

31 Das Recht am eigenen Bild ist im Gesetz betreffend das Urheberrecht an Werken der bildenden Kunst und Photographie (KUG) v. 9.1.1907 (RGBl. 7) geregelt. Durch die Neuregelung des Urheberrechts 1965 (UrhG) wurde bis auf die Paragraphen, welche den Schutz von Bildnissen zum Inhalt haben (§§ 22-24, 33, 37, 38, 42-44, 48 und 50), aufgehoben. Vgl. hierzu: Eisner/Mose, Das Recht am eigenen Bild, abrufbar über das Internet: <http://user.cs.tu-berlin.de/~uzadow/recht/raebild.html>.

32 Vgl. Ahlf, (Fn. 14), 425.

33 Bekannt geworden ist der Einsatz von Gesichtserkennungssystemen im Zoo Hannover. Hier soll durch automatisierte Gesichtserkennung bei Dauerkartenbesitzern der Zugang zum Zoo kontrolliert werden. Vgl. hierzu: Gesichtserkennung im Zoo, Computer-Fachwissen 5/2003, 33.

34 Vgl. v. Zezschwitz, (Fn. 17), Rn. 95.

35 Vgl. Altwater/Hamer/Ohnesorg/Peiseler, BPersVG, 5. Aufl., § 68 Rn. 18e ff.

36 Vgl. BAG, Urteil v. 7.10.1987, ArbUR 1987, 415. Das BAG hat in einem konkreten Einzelfall auch die heimliche Videoüberwachung für zulässig gehalten; vgl. BAG v. 27.3.2003, ArbUR 2003, 187.

sönlichkeitsrechte, wenn keine überwiegenden schutzwürdigen Interessen des Arbeitgebers ersichtlich sind. Dieses schutzwürdige Interesse des Arbeitgebers muss dann genau dargelegt und begründet werden. Es reicht nicht aus, dass er pauschal auf zunehmende Diebstähle hinweist. Somit können Dienststelle und Personalrat eine heimliche Kameraüberwachung nicht über die Mitbestimmung regeln. In jedem Fall muss der Personalrat (bei nicht verdeckter Kameraüberwachung) mitbestimmen. Geschieht dies nicht, liegt eine unzulässige Videoüberwachung vor, wobei die so gewonnenen Erkenntnisse einem Verwertungsverbot unterliegen und somit in einem arbeitsgerichtlichen Verfahren nicht verwertet werden können.³⁷ Zudem kann eine nicht durch vorrangige betriebliche Interessen gerechtfertigte und unter Verstoß gegen das Mitbestimmungsrecht des Personalrats durchgeführte Videoüberwachung die Zahlung von Schmerzensgeld nach sich ziehen.³⁸

Vor diesem Hintergrund sollte der Personalrat im Rahmen seines Mitbestimmungsrecht prüfen, ob es nicht andere Sicherungsmethoden als Kameraüberwachung gibt. Dieses ergibt sich für den Arbeitgeber schon aus dem Gebot der Datenvermeidung und Datensparsamkeit des § 3a BDSG. Sollte trotzdem eine Videoüberwachung (nicht heimliche) erforderlich sein, sollte auf eine Aufzeichnung verzichtet werden. Ist auch dieses nach der entsprechenden Prüfung notwendig, muss eine enge Zweckbestimmung und Zweckbindung der Videoüberwachung in einer Dienstvereinbarung festgelegt werden (eingesetzte Technik, »Standorte« der Kameras und Aufzeichnungsgeräte, Lösungsfristen, zugriffsberechtigte Personen). Eckpunkte einer Dienstvereinbarung zur Videoüberwachung sind:

1. Gegenstand und Geltungsbereich

persönlich und sachlich

2. Zweckbestimmung

genaue und abschließende Eingrenzung des Verwendungszwecks sowie Ausschluss der Überwachung der Beschäftigten

3. Von der Kameraüberwachung betroffene Bereiche

abschließende Festlegung der betroffenen Bereiche und Dokumentationen anhand von Skizzen (Grundrisse der Gebäude) in einer Anlage zur Dienstvereinbarung; auf diesen Skizzen muss klar eingezeichnet werden, welche Flächen von der jeweiligen Kamera überwacht werden

4. Dokumentation des Videoüberwachungssystems

abschließende Dokumentation des Systems in Anlagen zur Dienstvereinbarung

4.1 Geräte (Hardware)

Auflistung aller Geräte mit »Standorten«

4.2 Systembeschreibung

Dokumentation des Leistungsumfangs

4.3 Position und Reichweite der Kameras

Dokumentation der Position und der tatsächlichen Reichweite der Kameras anhand von Skizzen

4.4 Zugriffsberechtigte Personen

abschließende Festlegung der zugriffsberechtigten Personen (zu den Aufzeichnungsgeräten und zu den Bändern)

4.5 Schnittstellen

Ausschluss von Schnittstellen zu andern DV-Systemen

5. Aufzeichnungen

wenn Aufzeichnungen erforderlich sind, genaue Festlegung des Zeitraums des Umfangs und des Umgangs mit den Aufzeichnungen

6. Aufbewahrung der Videobänder (Speichermedien)

sichere Aufbewahrung der Videobänder (bzw. der Aufzeichnungsmedien)

7. Rechte der Beschäftigten

Information aller Beschäftigten über die Videoüberwachung und Demonstration der Reichweite und der technischen Möglichkeiten des Systems mit Beginn der Videoüberwachung

8. Rechte des Personalrats

Kontroll- und Überwachungsrechte

9. Änderung und Erweiterung des Systems

Änderungen und Erweiterungen unterliegen der Mitbestimmung des Personalrats

10. Meinungsverschiedenheiten

bei nicht zu lösenden Meinungsverschiedenheiten kommt das Regelungsverfahren nach dem Personalvertretungsrecht zu Anwendung

11. Abschaffung des Kameraüberwachungssystems

Abschaffung, wenn andere Sicherungsmethoden auf dem Markt sind

12. Inkrafttreten und Kündigung

Abschluss der Dienstvereinbarung für zwei Jahre ohne Nachwirkung

Zusätzlich sollte die Dienstvereinbarung befristet (für z.B. maximal zwei Jahre) abgeschlossen werden, damit die Dienststellenseite auch weiterhin nach alternativen Sicherungsmethoden suchen muss, die nicht so stark in die Persönlichkeitsrechte eingreifen wie die Videoüberwachung.

**Bruno Schierbaum
BTQ Niedersachsen
Oldenburg**

Literaturhinweis

Wolfgang Däubler, Thomas Klebe, Peter Wedde, Thilo Weichert
Bundesdatenschutzgesetz
Basiskommentar zum BDSG
2., überarbeitete Auflage
ISBN: 978-3-7663-3210-3, € 39,90

Dieses Buch ist direkt zu beziehen über Buch & Mehr
Telefon: 069/9520530
E-Mail: service@buchundmehr.de
www.buchundmehr.de

³⁷ So das LAG Mannheim, Urteil v. 6.5.1998, RDV 1/2000, 127.

³⁸ Vgl. Arbeitsgericht Frankfurt am Main, Urteil v. 26.9.2000, RDV 4/2001, 190.