Videoüberwachung in Unternehmen – rechtliche Möglichkeiten und Grenzen

Von Rechtsanwalt Dr. Ulrich Dieckert

Foto: PCS

Nicht nur die öffentliche Hand macht von der modernen Videoüberwachungstechnik Gebrauch. Noch häufiger ist der Einsatz in Unternehmen, die sich durch diese Technik sowohl nach außen als auch nach innen schützen wollen. Dabei sind die Anwendungsbereiche so vielfältig, wie die Tätigkeitsfelder des modernen Wirtschaftslebens. Zum Standard gehört mittlerweile die kameraunterstützte Eingangskontrolle in Bürohäusern beziehungsweise Betriebsanlagen. Das Bild des Pförtners, der von zahlreichen Bildschirmen umgeben ist, ist dem Publikum bereits seit Jahren vertraut. Neben diesem klassischen Anwendungsbereich eröffnet die moderne Videoüberwachungstechnik aber auch scheinbar unbegrenzte Möglichkeiten im Inneren eines Unternehmens. Intelligente Systeme schützen beispielsweise vor Diebstahl im Lager oder kontrollieren die Abläufe in der Produktion. Schließlich wird auch vor der Kontrolle von Mitarbeitern nicht halt gemacht, was in letzter Zeit Gegenstand lebhafter Diskussionen in der Öffentlichkeit war. Dieser Beitrag befasst sich mit den rechtlichen Grenzen, die dem Einsatz der Videoüberwachungstechnik durch Gesetze und Rechtsprechung gesetzt sind. Dabei muss zwischen dem Einsatz im öffentlich zugänglichen Bereich und der Kontrolle im Inneren eines Unternehmens unterschieden werden.

Rechtsgrundlagen für den Einsatz im Außenbereich

Wer Videoüberwachungskameras für die Zutrittskontrolle oder den äußeren Objektschutz einsetzt, hat vor allen Dingen die Voraussetzungen des § 6 b Bundesdatenschutzgesetz (BDSG) zu beachten. Denn diese Vorschrift befasst sich mit der Anwendung von Videoüberwachungstechnik in sogenannten „öffentlichen Räumen“. Der Gesetzgeber versteht darunter Berei-

che, die von jedermann ohne gesonderte Zugangsberechtigung betreten werden können, wie beispielsweise das öffentliche Straßenland, Parks, Bahnhöfe, Schalterräume, Kaufhäuser etc.. Nach der Rechtsprechung zählen hierzu auch die Flächen, die an einen Betrieb unmittelbar angrenzen, entweder als Außenbereich einer Umfriedung oder als klassischer Zugangsbereich. Denn erst nach Übertreten deutlich sichtbarer Eingrenzungen beginnt der Innenbereich, der nicht mehr ohne gesonderte Zugangsberechtigung betreten werden darf.

Konsequenterweise ist die Beobachtung derartiger „Grenzbereiche" zulässig, wenn sie zur Wahrnehmung des Hausrechtes dient. Darüber hinaus können Kameras im Außenbereich positioniert werden, wenn dies zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen (vgl. § 6 b Abs. 1 BDSG). Soweit der Einsatz nicht nur zur Livebeobachtung dient (sogenanntes Monitoring), sondern die Bilder auch aufgezeichnet werden, ist gemäß Absatz 3 der Vorschrift ebenfalls die Zweckmäßigkeit, Erforderlichkeit und Verhältnismäßigkeit der Maßnahme zu prüfen.

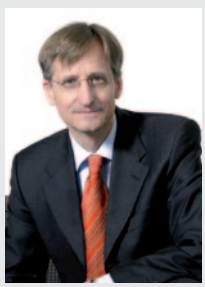
Aufgrund der Tatsache, dass durch jede Videoüberwachungsmaßnahme in Persönlichkeitsrechte der beobachteten Personen eingegriffen wird, bedarf es stets einer sorgfältigen Abwägung. So dürfen dem Betreiber keine gleichwertigen Überwachungsmittel zur Verfügung stehen, die weniger in Grundrechte eingreifen (sogenannte Erforderlichkeit). Selbst wenn es jedoch keine milderen Mittel gibt, muss das Interesse des Unternehmens am Schutz seiner Einrichtungen das Interesse der Betroffenen am Schutz ihrer Grundrechte überwiegen (sogenannte Verhältnismäßigkeit im engeren Sinne).

Gesetzeskonforme Umsetzung in der Praxis

Wie bereits dargelegt, ist der Einsatz von Kameras bei der Zutrittskontrolle regelmäßig durch das Hausrecht des Unternehmens gedeckt. Dies gilt sowohl für den Eingang in Bürogebäuden als auch die Kontrolle von Werkseinfahrten oder ähnliche Bereiche, in denen Besucherverkehr stattfindet. Denn das Interesse des Unternehmens an der Kontrolle, wer zu welchem Zweck in den Innenbereich eingelassen wird, überwiegt in der Regel die schutzwürdigen Interessen der Besucher, zumal sie meist nur für einen kurzen Augenblick ins Bild geraten. Jedoch ist der Kameraeinsatz (gegebenenfalls unterstützt durch Wechselsprechanlagen) regelmäßig auf den eigentlichen Zweck der Einlaßkontrolle zu beschränken. So wäre es beispielsweise unzulässig, die Besucher auch in Wartebereichen zu filmen, da hier in der Regel eine erhöhte soziale Interaktion stattfindet, die aus Gründen des Persönlichkeitsrechtsschutzes unbeobachtet bleiben muß.

Auch die Verwendung von Kameras zum Schutz von Umfriedungen genügt in der Regel dem Kriterium der Erforderlichkeit, wenn kein zumutbares milderes Mittel besteht. Dies wird von der Rechtsprechung mittlerweile auch dann angenommen, wenn die Alternative in personalintensiven und damit kostenträchtigen Überwachungsmaßnahmen bestünde. Allerdings ist bei der Ausrichtung der Kameras zu beachten, dass nicht in unverhältnismäßiger Weise in die Grundrechte von unbeteiligten Passanten eingegriffen wird.

Insbesondere die Außenbeobachtung von Gebäuden, die an das öffentliche Straßenland angrenzen, ist von der Rechtsprechung auf einen schmalen Streifen von maximal einem Meter begrenzt worden. Dies ist durch geeignete technische und organisatorische Maßnahmen zu gewährleisten, etwa durch feste Kameraeinstellungen oder die Ausblendung von Privatbereichen durch privat-masking oder durch die Verschleierung (Verpixeln) von Bildbereichen. Auch muss sichergestellt sein, dass der Einstellwinkel und die Ausrichtung der Kamera nicht unbefugt verändert wird, gegebenenfalls durch den Verzicht beziehungsweise die besondere Reglementierung von Fernsteuerungsfunktionen.



Der Autor, Rechtsanwalt Dr. Ulrich Dieckert, ist Partner der überörtlichen Sozietät Witt Roschkowski Dieckert, die unter anderem für die Bauwirtschaft beratend tätig ist. Dr. Dieckert hat sich im Bereich der Sicherheitstechnik auf das Thema Videoüberwachung spezialisiert und referiert hierzu auf Seminaren und Kongressen der Sicherheitsbranche. Er berät Betreiber und Errichter bei der Einführung sicherheitstechnischer Einrichtungen (zum Beispiel Entwurf von Betreiberkonzepten) und vertritt Unternehmen bei der Aushandlung von Betriebsvereinbarungen zum Thema Videoüberwachung.

Weitere Infos unter:
www.wrd.de

Was den Einsatz in Banken und im Einzelhandel sowie in Hotels und der Gastronomie angeht, so wird dies in anderen Schwerpunktheften von Security Point behandelt. Grundsätzlich sind auch hier die Persönlichkeitsrechte der betroffenen Kunden, Besucher und Gäste zu beachten. Da es in diesen Bereichen häufig um den Schutz vor Diebstahl und Beschädigungen geht, spielen sowohl die Prävention (Abschreckung) als auch die spätere Strafverfolgung eine große Rolle. Was letztere angeht, so müssen erstellte Aufzeichnungen vor Gericht auch verwertbar sein. Dies setzt eine manipulationssichere Erstellung von Bilddatenträgern sowie eine hohe Qualität der gefertigten Aufnahmen voraus; ansonsten wird diesen vor Gericht die Anerkennung als Beweismittel versagt*. Wer also in neue Überwachungsanlagen investiert, sollte an der hierfür geeigneten Technik nicht sparen.

Werden die Bilder aufgezeichnet, so sollten Kameras, Monitore sowie das Videomanagementsystem möglichst in einem geschlossenen Netz betrieben werden, weil dies die Möglichkeiten eines Zugriffs oder Angriffs von außen verringern. Werden die Kameras über drahtlose Technik angebunden, so muss gewährleistet werden, dass die Daten nur von den eigenen Geräten empfangen werden und nicht auf den Empfangsgeräten Dritter zur Ansicht kommen. Schließlich muss das zentrale Aufnahmegerät vor Fremdzugriffen geschützt sein, insbesondere, was die spätere Weiterverarbeitung, Analyse oder Auswertung angeht. So sollte vor Inbetriebnahme der Anlage festgelegt werden, welchen Personen Zugriffsmöglichkeiten eingeräumt werden und wie Fremdeingriffe verhindert werden können (zum Beispiel durch Berechtigungsverwaltung, Zugriffsprotokollierung, Diebstahlsicherung etc.).

Ist beabsichtigt, aufgezeichnete Bilder im Falle von Straftaten an die Ermittlungsbehörden weiter zu geben, so muss hierfür sowohl organisatorisch, als auch technisch ein geregeltes Verfahren geschaffen werden. So dürfen in der Regel nur die unmittelbar mit einer kriminellen Handlung zusammenhängenden Bildsequenzen herausgegeben werden. Im Zweifelsfall sollte sich das Unternehmen aufgrund eines richterlichen Beschlusses oder aufgrund eines staatsanwaltschaftlichen Auskunftsverlangens gemäß § 161 a StPO zur Herausgabe verpflichten lassen.

Kennzeichnungs- und Informationspflichten

Wo auch immer ein Unternehmen im öffentlich zugänglichen Bereich Videoüberwachung betreibt, muss es auf diese Tatsache in geeigneter Weise hinweisen. Diese Pflicht aus § 6 b Absatz 2 BDSG kann durch das Anbringen oder Aufstellen entsprechender Schilder erfüllt werden, die neben dem Umstand der Beobachtung auch Auskunft über die verantwortliche Stelle geben. Die Schilder sind deutlich sichtbar anzubringen, damit beispielsweise Passanten selbst entscheiden können, ob sie sich einer Beobachtung aussetzen wollen oder nicht. Die Kennzeichnungspflicht gilt im Übrigen auch für Attrappen, da diese einen gleichen Überwachungsdruck ausüben, wie funktionierende Kameras.

Nach § 6 B Absatz 4 BDSG besteht eine zusätzliche Benachrichtigungspflicht, wenn durch die Videoüberwachung erhobene und gespeicherte Daten einer bestimmten Person zugeordnet werden können. Werden beispielsweise Bildsequenzen an Ermittlungsbehörden weitergereicht und hat das Unternehmen auf diesen Aufnahmen bestimmte Personen identifiziert, so sind diese von der Tatsache der Übermittlung zu informieren, wenn nicht anzunehmen ist, dass die Person darüber nicht bereits von anderer Stelle in Kenntnis gesetzt worden ist (beispielsweise durch Zeugenbefragung etc.).

Löschungsverpflichtung

Schließlich hat das Unternehmen die erhobenen Bilddaten unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen (vgl. § 6 b Abs. 5 BDSG). Je nach Einsatzbereich sind die für zulässig erachteten Speicherzeiträume unterschiedlich lang. Während beispielsweise der Einzelhandel und Tankstellen ihre Aufzeichnungen im Wege eines Ringspeicherverfahrens täglich überschreiben, bewahren Banken die Aufzeichnungen an Geldautomaten bis zu sechs Wochen auf, da unberechtigte Abhebungen von Kunden oft erst nach Prüfung ihrer Kontoauszüge entdeckt werden, was eine geraume Zeit in Anspruch nehmen kann. Aufzeichnungen von Umfriedungen und Eingangsbereichen sind in der Regel spätestens nach 24 Stunden zu löschen, wenn es keine besonderen Vorkommnisse wie Einbruchsversuche, unberechtigtes Betreten, Beschädigungen gegeben hat .

Überwachung im Innenbereich

Setzt das Unternehmen die Videoüberwachung auf dem Betriebsgelände oder in seinem Bürogebäude fort, so handelt es sich hier nicht um öffentlich zugängliche Bereiche, so dass § 6 b BDSG keine unmittelbare Anwendung findet. Hier ist eine Videoüberwachung nur zulässig, wenn die Betroffenen individuell einwilligen oder die Überwachung durch eine andere

* Mehr dazu im Beitrag „Gerichtsverwertbakeit von Videobildern“ ab Seite 14.

Rechtsvorschrift erlaubt ist (vgl. § 4 Abs. BDSG). Soweit die Überwachung zur Wahrung „berechtigter Interessen“ des Unternehmens erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der Kunden oder Besucher an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, wird sich das Unternehmen auf die Generalermächtigung in § 28 Absatz 1 Nr. 2 BDSG stützen können.
So wird der Kunde oder Besucher eines Unternehmens davon ausgehen müssen, dass beispielsweise Parkflächen auf dem Betriebsgelände oder besonders sicherheitsrelevante Bereiche, wie Produktionsanlagen oder Rechenzentren, gesondert überwacht werden. In Anbetracht der Tatsache, dass ein Besucher oder Kunde in der Regel nur kurzfristig in den Erfassungsbereich einer Kamera gerät, wird die Interessenabwägung in der Regel zu Gunsten des Unternehmens ausfallen, soweit man nicht ohnehin von einer stillschweigenden Zustimmung ausgehen kann.

Arbeitnehmerdatenschutz

Von einer stillschweigenden Einwilligung kann hingegen nicht ausgegangen werden, soweit durch Kameraüberwachungsmaßnahmen Mitarbeiter des Unternehmens betroffen sind. Denn es wird unterstellt, dass selbst schriftliche Einwilligungen in einem Anstellungsverhältnis nicht völlig freiwillig erfolgen, sondern in der Regel ein gewisses Wohlverhalten des Arbeitsnehmers (auch zum Erhalt seines Arbeitsplatzes) zum Ausdruck bringen. Auch die Generalklausel in § 28 BDSG hilft hier nicht weiter, weil Mitarbeiter aufgrund ihrer permanenten Anwesenheit einem viel höheren Überwachungs- und Anpassungsdruck unterliegen, als gelegentliche Besucher von außen.
Ein wirksamer Arbeitnehmerdatenschutz lässt sich in der Regel nur herstellen, wenn das Unternehmen mit dem zuständigen Betriebsrat (falls vorhanden) eine wirksame Betriebsvereinbarung schließt. Ansonsten bleibt zu hoffen, dass der Gesetzgeber die bereits als

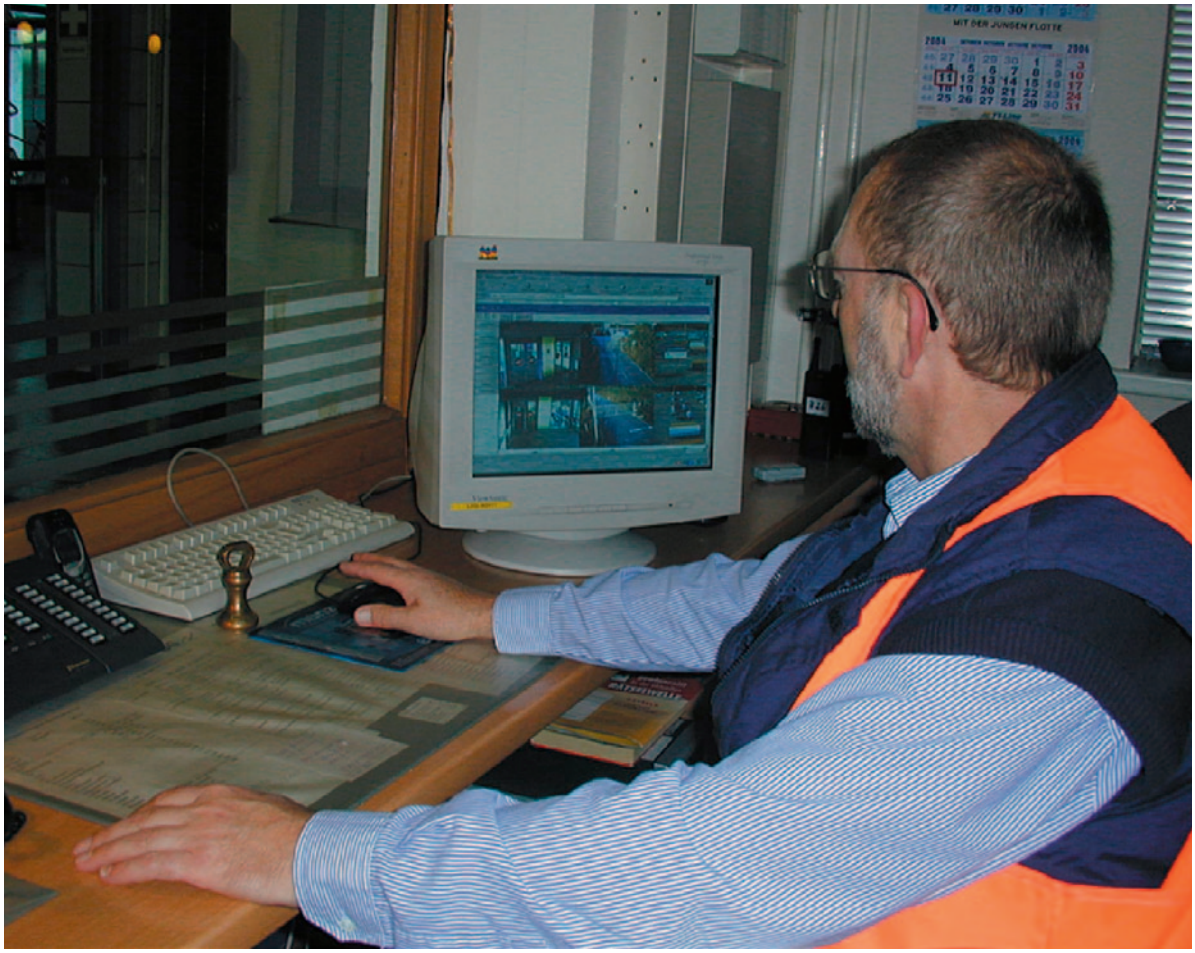


Foto: Mobotix

Die Überwachung des Einlassbereichs ist in vielen Unternehmen mittlerweile üblich.

Referentenentwurf vorliegenden Neuregelungen in Kraft setzt, die weiter unten angesprochen werden.

Betriebsvereinbarung, Vorabkontrolle

Gemäß § 87 Absatz 1 Nr. 6 Betriebsverfassungsgesetz besteht ein Mitbestimmungsrecht in Bezug auf „Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Arbeitnehmer zu überwachen". Da hierzu auch die Videoüberwachung geeignet ist, kann der Betriebsrat den Abschluss einer Vereinbarung verlangen, in der die technischen Einzelheiten der Überwachungsmaßnahme sowie Einsichts- und Kontrollrechte des Betriebsrates geregelt sind. Dies gilt übrigens sowohl für die nicht öffentlichen, als auch für die öffentlich zugänglichen Bereiche eines Unternehmens. Wird eine solche Vereinbarung geschlossen, so gilt diese als „andere Rechtsvorschrift" gemäß § 4 Absatz 1 BDSG, die den Einsatz der Videoüberwachung erlaubt.

Unternehmen sind daher gut beraten, wenn sie vor der Einführung von Videoüberwachungsmaßnahmen hinreichende konzeptionelle Überlegungen anstellen, die auch die Belange des Arbeitnehmerdatenschutzes berücksichtigen. Hierzu sind sie bereits gemäß 4 d Absatz 5 Nr. 2 BDSG verpflichtet, wonach derartige Überwachungsmaßnahmen einer Vorabkontrolle durch den zuständigen Datenschutzbeauftragten unterliegen. Ein solcher ist zu bestellen, wenn mindestens neun Mitarbeiter regelmäßig mit der automatisierten Verarbeitung personenbezogener Daten zu tun haben (vgl. § 4 f Abs. 1 BDSG). Eine Missachtung dieser Pflicht kann empfindliche Bußgelder nach sich ziehen.

Werden bei der Aufstellung eines solchen Konzeptes die Belange des Arbeitnehmerdatenschutzes von vornherein berücksichtigt, lassen sich konfrontative Auseinandersetzungen mit dem Betriebsrat bei den späteren Verhandlungen über eine Betriebsvereinbarung vermeiden. Um seine Interessen an einer effizienten Überwachung zu wahren, sollte das Unternehmen in derartigen Verhandlungen allerdings eigene Entwürfe vorlegen, denn die von den Gewerkschaften gefertigten Muster lassen es häufig an der erforderlichen Ausgewogenheit fehlen.

Kann sich das Unternehmen mit dem Betriebsrat nicht einigen, so lassen sich Betriebsvereinbarungen auch über die Einigungsstelle erzwingen. In einem solchen Verfahren wird geprüft, ob die Überwachungsmaßnahmen zweckmäßig, erforderlich und in Bezug auf die betroffenen Grundrechte der Mitarbeiter auch verhältnismäßig sind. Anlassunabhängige und örtlich wie zeitlich unbegrenzte Maßnahmen hat die einschlägige Rechtsprechung bisher regelmäßig verworfen. Der Mitarbeiter darf nicht einem permanenten Überwachungs- und Anpassungsdruck ausgesetzt sein, da dies seine Persönlichkeitsrechte unverhältnismäßig beeinträchtigt. Der Vorrang ist daher stets zielgerichteten Maßnahmen einzuräumen, die aufgrund konkreter Vorkommnisse begründet sind und nicht länger andauern, als unbedingt nötig. Näheres hierzu lässt sich einer Grundsatzentscheidung des Bundesarbeitsgerichtes aus dem Jahr 2008 entnehmen (BAG, Beschluss vom 26.08.2008, 1 ABR 16/07).

Gezielte Überwachung

Soweit das Unternehmen im eigenen Hause Unregelmäßigkeiten entdeckt, so ist es nach dem neu erlassenen § 32 Absatz 1 Satz 2 BDSG unter bestimmten Umständen auch berechtigt, gezielte Überwachungsmaßnahmen gegenüber eigenen Mitarbeitern einsetzen. Auch der Einsatz von Videoüberwachung ist jedoch nur möglich, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat, dass die Überwachung zur Aufdeckung erforderlich ist und dass die ergriffenen Maßnahmen im Hinblick auf die Persönlichkeitsrechte des Betroffenen nicht unverhältnismäßig sind.

Inwieweit dies auch die heimliche Videoüberwachung eines Beschäftigten rechtfertigt, ist umstritten. Zwar gilt die Kennzeichnungspflicht bisher nur für Maßnahmen im öffentlich zugänglichen Bereich (vgl. § 6 b Abs. 2 BDSG), hieraus ließe sich jedoch der Schluss ableiten, dass bei Aufnahmen im nicht öffentlichen Bereich eine Information erst recht erforderlich ist, weil der mit der Überwachung verbundene Grundrechtseingriff bei den permanent anwesenden Arbeitnehmern in der Regel sogar höher ist.

Auch haben Arbeitsgerichte in der Vergangenheit entschieden, dass heimlich angefertigte Aufzeichnungen wegen des damit verbundenen Verstoßes gegen die Kennzeichnungspflicht nicht vor Gericht verwendet werden dürfen (Beweisverwertungsverbot). Andererseits hat das Bundesarbeitsgericht in einer Entscheidung aus dem Jahre 2003 die heimliche Videoüberwachung dann für zulässig gehalten, wenn der konkrete Verdacht einer strafbaren Handlung zu Lasten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachtes ausgeschöpft sind und die verdeckte Videoüberwachung das einzig verbliebene Mittel darstellt und insgesamt nicht unverhältnismäßig ist. Diese Entscheidung er-

ging jedoch zu einem Sachverhalt, der vor Inkrafttreten des § 6 b BDSG stattgefunden hat.

Reform des Arbeitnehmerdatenschutzes

Diese Streitfrage könnte sich erledigen, wenn der nunmehr vorliegende Referentenentwurf (Stand: Mai 2010) zur Regelung des Beschäftigtendatenschutzes die parlamentarischen Hürden nimmt. Nach dem neu einzuführenden § 32 f BDSG (Beobachtung nicht öffentlich zugänglicher Betriebsstätten mit optisch-elektronischen Einrichtungen) soll die Videoüberwachung von nicht öffentlich zugänglichen Betriebsgeländen, Betriebsgebäuden oder Betriebsräumen zulässig sein, wenn sie zur Zutrittskontrolle, zur Wahrnehmung des Hausrechtes, zum Schutze des Eigentums, zur Sicherheit des Beschäftigten, zur Sicherheit von Anlagen oder zur Abwehr von Gefahren für die Sicherheit des Betriebes erforderlich sind und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen des Betroffenen am Ausschluss der Datenerhebung überwiegen.

Der Arbeitgeber hat den Umstand der Beobachtung durch geeignete Maßnahmen erkennbar zu machen, auch wenn er nur Kameraattrappen installiert. Eine heimliche Videoüberwachung eines Beschäftigten soll dann zulässig sein, wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass Beschäftigte im Beschäftigungsverhältnis eine Straftat oder eine schwerwiegende Vertragsverletzung zu Lasten des Arbeitgebers begangen haben, die Erhebung zur Aufdeckung erforderlich und Art und Ausmaß der Erhebung im Hinblick auf den Zweck nicht unverhältnismäßig sind (vgl. § 32 f Absatz 2 des Gesetzentwurfes).

Die gesetzlichen Neuregelungen sind auch deshalb zu begrüßen, weil sie für diejenigen Unternehmen und ihre Beschäftigten Rechtsklarheit herbeiführen, in denen mangels des Vorhandenseins eines Betriebsrates keine Betriebsvereinbarungen geschlossen werden. Diese Lücke wurde in der Vergangenheit von bekannten Lebensmittel- und Drogeriediscountern in wenig rühmlicher Weise ausgenutzt, deren Filialbetriebe in der Regel nicht die notwendige Mitarbeiterzahl zur Bildung eines Betriebsrates aufweisen. Am Negativbeispiel Lidl dürfte auch die Regelung in § 32 f Absatz 3 des Entwurfes ausgerichtet sein, wonach die Videoüberwachung von Betriebsstätten, die überwiegend zur privaten Lebensgestaltung des Beschäftigten dienen, unzulässig ist. Der Gesetzgeber versteht hierunter beispielsweise Pausen- und Umkleideräumlichkeiten, die für Videoüberwachungsmaßnahmen in jedem Falle tabu sein müssen.