Videoüberwachung im Retail-Bereich

Rechtslagen-Vergleich

Dr. Ulrich Dieckert

Im Rahmen der Axis Roadshow 2013 stand unter anderem die Videoüberwachung im Handel aus datenschutzrechtlicher und arbeitsrechtlicher Sicht im Fokus. Dabei verglich der Autor die Rechtslagen in Deutschland, Österreich und der Schweiz.

Rechtsanwalt Dr. Ulrich Dieckert ist Partner der überörtlichen Sozietät Witt Roschkowski Dieckert, die unter anderem für die Bau- und Immobilienwirtschaft 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 Unternehmen und Errichterfirmen bei der Einführung sicherheitstechnischer Einrichtungen und vertritt diese bei Auseinandersetzungen mit Datenschützern und/oder Personalvertretern.
Er hat im Rahmen der Axis Roadshow, die im Frühjahr 2013 in Deutschland, Österreich und der Schweiz stattfand, zu Rechtsfragen der Videoüberwachung im Retailbereich referiert. Ziel des Beitrages ist es, anhand konkreter Anwendungsbeispiele einen Rechtsvergleich der drei Länder anzustellen.

Hier sind neben vielen Gemeinsamkeiten (vor allen Dingen in den Grundsätzen) einige bemerkenswerte Unterschiede im verwaltungstechnischen Umgang mit der Videoüberwachung zu verzeichnen. Ausgehend von den jeweils geltenden Rechtsgrundlagen steht die Überwachung von Kunden und sonstigen Dritten einerseits und die Überwachung von Mitarbeitern andererseits im Mitteilpunkt. Sodann werden die - durchaus unterschiedlichen - sonstigen gesetzlichen Pflichten in Bezug auf die Bilddatenbearbeitung in den drei Ländern dargelegt. Schließlich wird die Frage erörtert, inwieweit rechtmäßig beziehungsweise rechtswidrig erhobene Bilddaten vor Gericht als Beweismittel eingesetzt werden können.

Rechtsgrundsätze

Gründe für den Einsatz von Videoüberwachung im Retail-Bereich gibt es viele. Im Mittelpunkt steht der Schutz vor Diebstählen beziehungsweise Überfällen sowie vor der Beschädigung von Einrichtungen (zum Beispiel Vandalismus, Graffiti etc.). Aber auch Mitarbeiter und Kunden sollen vor Übergriffen geschützt werden. Denn allein die Tatsache einer Videoüberwachung ist zur Abschreckung potentieller Täter geeignet (sogenannte Präventionswirkung). Kommt es gleichwohl zu Sachbeschädigungen, Diebstählen beziehungsweise Übergriffen, so dienen die angefertigten Aufzeichnungen nicht nur zur Aufklärung, sondern können auch als Beweismittel für die Verfolgung rechtlicher Ansprüche eingesetzt werden (Repressionszwecke).
Daneben werden Kameras in jüngster Zeit immer häufiger dafür verwendet, Betriebsabläufe zu steuern beziehungsweise zu erfassen und Kundenbewegungen beziehungsweise Verhaltensmuster zu analysieren. Letzteres dient einer Optimierung des Personaleinsatzes beziehungsweise der Anordnung von Ware, was mit den eigentlichen Schutzzwecken nichts mehr zu tun hat. Schließlich werden Kameras in größeren Märkten beziehungsweise Einkaufszentren auch zur Überwachung von Parkplätzen, der Warenanlieferung, des Lagers sowie von Bürokomplexen eingesetzt.

Erhebung personenbezogener Daten

Aus rechtlicher Sicht ist mit dem Einsatz von Videoüberwachungstechnik regelmäßig die Erhebung, Verarbeitung und Nutzung personenbezogener Daten verbunden. Denn bereits die bloße Beobachtung einer Person, jedenfalls aber die Anfertigung von Bildaufnahmen dieser Person ermöglicht deren Identifizierung. Insofern unterfällt die Erhebung von Bilddaten in allen drei Ländern den Vorgaben der jeweiligen Datenschutzgesetze. In Deutschland ist dies das Bundesdatenschutzgesetz (BDSG), in der Schweiz das Bundesgesetz über den Datenschutz (DSG) und in Österreich das Datenschutzgesetz 2000 in der aktuellen Fassung 2012 (DSG). Alle drei genannten Gesetze haben zum Ziel, den Einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinen Persönlichkeitsrechten beeinträchtigt wird (vgl. § 1 Abs. 1 BDSG, Artikel 1 DSG-Schweiz, Artikel 1 § 1 Abs. 1 DSG-Österreich).

Dies kommt nicht von ungefähr, weil ebenfalls in allen drei Ländern die Persönlichkeits- und Freiheitsrechte der Bürger verfassungsrechtlichen Schutz genießen. In Deutschland hat das Bundesverfassungsgericht aus den Grundsätzen der Artikel 1 und 2 des Grundgesetzes in seiner Entscheidung zur Volkszählung (15.12.1983) das Grundrecht auf informationelle Selbstbestimmung abgeleitet. In der Schweiz hat dieses Grundrecht sogar Eingang in die Bundesverfassung gefunden; danach hat gemäß Artikel 13 jede Person „Anspruch auf Schutz von Missbrauch ihrer persönlichen Daten“. In Österreich ist der Anspruch auf Geheimhaltung von personenbezogenen Daten in Artikel 1 § 1 Abs. 1 DSG geregelt, was als Vorschrift mit Verfassungsrang gilt. Für alle drei Staaten gilt darüber hinaus Artikel 7 der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten (EMRK), wonach jede Person nicht nur das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation hat (vgl. Artikel 7), sondern auch das Recht auf Schutz der sie betreffenden personenbezogenen Daten (vgl. Artikel 8).

Den Verfassungsbestimmungen aller drei Länder ist des weiteren eigen, dass in Grundrechte nur durch oder aufgrund eines Gesetzes eingegriffen werden darf (siehe zum Beispiel Artikel 36 der Schweizerischen Bundesverfassung). Die einschlägige Verfassungsbestimmung in Artikel 1 § 1 Abs. 2 des DSG Österreich ergänzt, dass Beschränkungen des Anspruches auf Geheimhaltung personenbezogener Daten nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig ist und dass auch im Falle zulässiger Beschränkungen der Eingriff in das Grundrecht jeweils nur in der gelindesten, zum Ziel führenden Art vorgenommen werden darf.

Soweit es in Deutschland und in der Schweiz um die Erhebung personenbezogener Daten durch Bundesbehörden beziehungsweise durch Privatpersonen (dies umschließt auch Unternehmen) geht, gelten die bundesweit einschlägigen Regelungen des BDSG (Deutschland) beziehungsweise DSG (Schweiz). Für Organe der Länder beziehungsweise Kantone sowie für sonstige kommunale Ämter gelten in Deutschland die Landesdatenschutzgesetze und in der Schweiz die von den jeweiligen Kantonsräten beschlossenen Gesetze und Verordnungen über die Informationen im Datenschutz (sogenannte IDG beziehungsweise IDV). In Österreich gibt es eine solche Aufteilung nicht, hier gilt in allen Fällen das Datenschutzgesetz, soweit für die Ordnungs- und Strafverfolgungsbehörden nicht spezielle Regelungen aus dem Sicherheits- und Polizeigesetz beziehungsweise der Strafprozessordnung einschlägig sind. Vergleichbares gilt auch für die Ordnungs- und Strafverfolgungsbehörden in Deutschland (hier: Landespolizeigesetze) und der Schweiz.

Arbeitsrecht ist zu beachten

Soweit von den Videoüberwachungsmaßnahmen auch Mitarbeiter betroffen sind, gelten in allen drei Ländern ergänzend die einschlägigen Regeln des Arbeitsrechtes. Grundsätzlich hat der Arbeitgeber die freie Entfaltung der Persönlichkeit der im Betrieb beschäftigten Arbeitnehmer zu schützen (vgl. § 75 Abs. 2 Betriebsverfassungsgesetz - Deutschland; Artikel 328 Obligationenrecht, SR 220 - Schweiz). In Österreich ist die Videoüberwachung zum Zweck

der Mitarbeiterkontrolle an Arbeitsstätten generell untersagt (vgl. § 50 a Abs. 5 Satz 2 DSG). Auch in der Schweiz dürfen Überwachungs- oder Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, nicht eingesetzt werden (vgl. Artikel 26 Verordnung 3 zum Arbeitsgesetz).
Ein solches generelles Verbot gibt es in Deutschland nicht. Dort ist jedoch die „Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen", mitbestimmungspflichtig (vgl. § 87 Abs. 1 Nr. 6 BetrVG). Vergleichbare Mitbestimmungsrechte sind auch in der Schweiz und in Österreich geregelt, hierauf wird später noch einmal ausführlicher eingegangen.

Planer haben Hinweispflichten

Wie ebenfalls später darzulegen sein wird, kann eine Missachtung der o. a. Vorschriften in allen drei Ländern dazu führen, dass der Betrieb von Anlagen ganz oder teilweise untersagt wird und sich der Betreiber nicht unerheblichen Bußgeldern und Schadensersatzansprüchen der Betroffenen ausgesetzt sieht. Ist die gesetzwidrige Installation der Anlage auf einen Beratungsfehler der beauftragten Planer und Errichter zurückzuführen, so können diese unter Umständen in Regress genommen werden. Sie schulden zwar als Ingenieure beziehungsweise Techniker keine eigene rechtliche Beratung. Sie müssen in Erfüllung ihrer sogenannten „Sachverwalterpflichten" den Betreiber aber auf mögliche rechtliche Risiken hinweisen. Dies sollte in Form eines Bedenkenhinweises erfolgen, um sich gegen eventuelle Ansprüche des Auftraggebers abzusichern. Diesem sollte in jedem Fall empfohlen werden, in Zweifelsfragen kompetenten Rechtsrat einzuholen.

Bei der Planung, Einführung und dem Betrieb von Videoüberwachungsanlagen sind also in allen drei Ländern datenschutzrechtliche Bestimmungen zu beachten. Des Weiteren sind die Mitarbeiter beziehungsweise deren Vertretungen in geeigneter Weise zu beteiligen. Welche datenschutzrechtlichen und arbeitsrechtlichen Regelungen im Einzelfall einschlägig sind, soll nachfolgend erläutert werden.

Überwachung von Kunden und sonstigen Dritten

Wie bereits angemerkt, haben die Gesetzgeber in Deutschland, Österreich und der Schweiz unterschiedliche Ansätze gewählt, die Erfassung personenbezogener (Bild-)Daten zu regeln. Die ausführlichsten Vorschriften finden sich im neuen Abschnitt 9 a des österreichischen Datenschutzgesetzes. Dies beginnt in § 50 a Abs. 1 mit folgender gesetzlicher Definition: „Videoüberwachung bezeichnet die systematische, insbesondere fortlaufende Feststellung von Ereignissen, die ein bestimmtes Objekt (überwachtes Objekt) oder eine bestimmte Person (überwachte Person) betreffen, durch technische Bildaufnahme- oder Bildübertragungsgeräte". Des Weiteren wird gesetzgeberisch klargestellt, dass Aufnahmen aus rein touristischen oder künstlerischen Beweggründen, aber auch Filmen für ausschließlich familiäre oder persönliche Tätigkeiten nicht unter die Videoüberwachung fallen.

Im deutschen Datenschutzgesetz befasst sich bisher nur eine Regelung, nämlich der im Jahre 2001 neu eingefügte § 6 a BDSG, ausdrücklich mit der Erhebung von Bilddaten. Dabei ist der Anwendungsbereich der Vorschrift auf „öffentlich zugängliche Räume" beschränkt. Die Rechtsprechung versteht darunter Räume, die nach dem erkennbaren Willen des Berechtigten von jedermann benutzt oder betreten werden können, wie zum Beispiel öffentliche Verkehrsflächen, Parkplätze, Verkaufsräumlichkeiten, Freizeiteinrichtungen etc. Büroräume oder Lagerflächen in Unternehmen unterfallen hingegen nicht dem Anwendungsbereich der Vorschrift. Diese „nicht öffentlich zugänglichen Betriebsstätten" sollten mit dem Gesetz zum Beschäftigtendatenschutz in das BDSG eingefügt werden. Bis zu dessen Inkrafttreten muss man sich für diese Bereiche mit den allgemeinen Grundsätzen des BDSG behelfen.

Wie man am Beispiel der Schweiz sieht, ist die Bezugnahme auf allgemeine Grundsätze durchaus möglich. Denn das schweizerische DSG enthält überhaupt keine ausdrücklichen Vorschriften zur Bilddatenerhebung durch Videoüberwachungsanlagen. Hier wird lediglich zwischen der Datenbearbeitung von Bundesbehörden einerseits und privaten Personen (wozu auch Unternehmen zählen) andererseits unterschieden. Letztere dürfen Personendaten (und damit auch Bilddaten) nur bearbeiten, wenn dabei die Persönlichkeitsrechte der betroffenen Person nicht widerrechtlich verletzt werden (Artikel 12 DSG), dem Betreiber der (Bild-)Datenverarbeitung insofern Rechtfertigungsgründe zur Seite stehen (vgl. Artikel 13 DSG) und die allgemeinen Grundsätze der Datenbearbeitung wie Zweckmäßigkeit, Verhältnismäßigkeit und Transparenz (vgl. Artikel 4 DSG) beachtet werden.

Diese Grundsätze gelten auch in Deutschland und in Österreich, auch wenn sie an unterschiedlicher Stelle geregelt sind. Ohnehin ist zu konstatieren, dass die Rechtmäßigkeit der Bilddatenerhebung stets nach den gleichen Prüfungsschritten zu beurteilen ist. Alle Gesetze stellen klar, dass mit der (Bild-)Datenerhebung ein Eingriff in Persönlichkeitsrechte (beziehungsweise schutzwürdige Geheimhaltungsinteressen) verbunden ist. Ein solcher kann gleichwohl rechtmäßig sein, wenn der Betroffene seine Daten allgemein zugänglich gemacht hat und mit deren Verwendung ausdrücklich einverstanden ist oder die Erhebung anderweitig durch Gesetz erlaubt oder angeordnet ist.

Darüber hinaus ist nach allen drei Gesetzen die Erhebung zulässig, wenn dem Betreiber der Videoüberwachungsanlage überwiegende Gründe zur Seite stehen und bei der Erhebung und Verarbeitung der Daten der Grundsatz der Verhältnismäßigkeit (insbesondere Zweckmäßigkeit, Erforderlichkeit und Angemessenheit) gewahrt bleibt. Diese Grundsätze sollen nachfolgend in Bezug auf den Retail-Bereich näher beleuchtet werden.

Einwilligung in die Bilddatenerhebung durch Kunden?

Gemäß § 50 a Abs. 3 des österreichischen DSG sind schutzwürdige Geheimhaltungsinteressen nicht verletzt, wenn Bilddaten über ein Verhalten verarbeitet werden, das ohne jeden Zweifel den Schluss zulässt, dass es darauf gerichtet war, öffentlich wahrgenommen zu werden (Ziffer 2) und/oder wenn der Betroffene der Verwendung der Daten im Rahmen der Überwachung ausdrücklich zugestimmt hat (Ziffer 3). Derartige Rechtfertigungsgründe finden sich auch in Artikel 13 Abs. 1 des schweizerischen DSG (keine Persönlichkeitsrechtsverletzung bei Einwilligung des Verletzten) und § 4 Abs. 1 des BDSG. Allerdings ist nach § 4 a BDSG die Einwilligung nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist insofern auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie - soweit nach den Umständen des Einzelfalls erforderlich oder auf Verlangen - auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Auch nach Artikel 4 Abs. 5 des schweizerischen DSG ist eine Einwilligung erst gültig, wenn sie nach angemessener Information freiwillig erfolgt.

Wollte der Betreiber eines Kaufhauses die Zustimmung seiner Kunden einholen, müsste er diese also zunächst vor dem Betreten hinreichend über die Art und Weise der Videoüberwachung aufklären - was bereits aus Praktikabilitätsgründen nicht möglich ist. Von einer konkludenten Einwilligung darf jedenfalls nicht ausgegangen werden, weil die Erfassung durch Kameras - anders als zum Beispiel bei Straßenkünstlern - vom Kunden nicht gesucht, sondern eher erduldet wird. Denn einer Videoüberwachung in Geschäften kann man sich aufgrund von deren Verbreitung heute kaum noch entziehen.

Überwiegende Interessen des Anwenders

Nach allen drei Datenschutzgesetzen ist ein Eingriff in die Persönlichkeitsrechte/schutzwürdige Geheimhaltungsinteressen aber auch gerechtfertigt, wenn die (Bild-)Datenerhebung der Wahrnehmung berechtigter Interessen des Betreibers dient und diese die Interessen der Betroffenen überwiegen. Gemäß § 50 a Abs. 4 Ziffer 1 des österreichischen DSG ist dies unter anderem der Fall, wenn „bestimmte Tatsachen die Annahme rechtfertigen, das überwachte Objekt oder die überwachte Person könnte das Ziel oder der Ort eines gefährlichen Angriffs werden“. Das deutsche BDSG ist an dieser Stelle weniger konkret, hier wird in § 6 b auf die „Wahrnehmung des Hausrechtes“ oder die „Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke“ abgestellt. Gleiches gilt für Artikel 13 des schweizerischen DSG, in dem lediglich vom Überwiegen eines privaten oder öffentlichen Interesses die Rede ist.

In allen drei Ländern ist man sich jedoch einig, dass der Schutz vor Sachbeschädigungen, Diebstählen, betrügerischen Manipulationen und Überfällen berechtigte Interessen von Kaufhausbetreibern darstellen, die die Interessen der Kunden, die ja nur für einen kurzen Zeitraum überwacht werden, in der Regel überwiegen. In Österreich wird dabei zwischen dem sogenannten Eigenschutz (das heißt Schutz der Person und des Eigentums des Auftraggebers) und dem sogenannten „Verantwortungsschutz“ (das heißt die Wahrnahme von Verkehrssicherungspflichten in Bezug auf Besucher und Kunden) unterschieden (vgl. § 50 a Abs. 2 DSG). Auch ist die Sicherung der zu den o. a. Zwecken erhobenen Videodaten, um diese als Beweis vor Gericht verwenden zu können (sogenannte Beweissicherung), ausdrücklich im Gesetz als gerechtfertigter Zweck genannt. Dies ist zwar in den Datenschutzgesetzen Deutschland und der Schweiz nicht ausdrücklich genannt, wird jedoch von der Rechtsprechung als rechtfertigender Zweck anerkannt.

Verhältnismäßigkeit

Auch wenn die Videoüberwachung der Wahrnehmung berechtigter Interessen dient, muss der Betreiber bei deren Einsatz in allen drei Ländern das Verhältnismäßigkeitsgebot beachten. So hat nach Artikel 4 Abs. 2 des schweizerischen DSG die Bearbeitung von Personendaten nach Treu und Glauben zu erfolgen und muss verhältnismäßig sein. Gemäß § 7 Abs. 3 des österreichischen DSG setzt die Zulässigkeit einer Datenanwendung voraus, dass die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgt. Gemäß § 6 b BDSG ist die Überwachung beziehungsweise Verarbeitung der Bilddaten auch bei Wahrnehmung berechtigter Interessen nur zulässig, wenn sie erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Danach ist in allen drei Ländern vom Betreiber stets zu prüfen, ob die eingesetzten Maßnahmen geeignet sind, um die verfolgten Zwecke zu erreichen (Zweckmäßigkeit), ob die Videoüberwachung zur Zweckverfolgung erforderlich ist, also keine milderen - gleich tauglichen - Mittel bestehen (Erforderlichkeit) und ob die Videoüberwachung den Betroffenen im Einzelfall auch zumutbar ist, um überwiegende Interessen durchzusetzen (Angemessenheit).

Zweckmäßigkeit

Dass der Einsatz von Kameras zur Abwehr von Diebstählen, Sachbeschädigungen oder Übergriffen beziehungsweise zur Beweissicherung im Retail-Bereich zweckmäßig ist, dürfte unstreitig sein. Der Betreiber einer solchen Maßnahme muss sich jedoch darüber im Klaren sein, dass er die Kameras auch nur zu diesen Zwecken einsetzen darf. Eine Verwendung der erhobenen Bilddaten für andere Zwecke (zum Beispiel Marketing) wäre nach den genannten Datenschutzregelungen unzulässig. Dies setzt jedoch voraus, dass es sich tatsächlich um Bilddatenerhebung handelt. Dies könnte beim Einsatz von Kamerasystemen fraglich sein, bei denen lediglich statistische Daten erhoben werden, die nicht mehr in Bilddaten umgewandelt werden können. Beim Betrieb derartiger Systeme zum Zwecke des „People counting“ oder für Verhaltensanalysen muss jedoch darauf geachtet werden, dass keine Verknüpfung mit den gleichzeitig betriebenen Überwachungssystemen besteht.

Erforderlichkeit

Der Betreiber einer Überwachungsanlage muss sich des Weiteren stets fragen, ob es keine anderen Mittel zum Eigen- beziehungsweise Fremdschutz gibt, die den gleichen Zweck erfüllen, aber weniger in die Rechte der Betroffenen eingreifen. Insofern ist auch der verstärkte Einsatz von Aufsichtspersonal, die Einrichtung räumlicher Sperren oder die Anbringung elektronischer Warensicherungen zu erwägen. Muss die Überwachung „flächendeckend“ und „rund um die Uhr“ erfolgen, wenn auch eine Überwachung von Schwerpunkten beziehungsweise in bestimmten Zeiträumen ausreichen könnte? Müssen die Bilder wirklich gespeichert werden oder reicht nicht eine Echtzeitüberwachung (sogenanntes Monitoring) aus? Nach österreichischer Rechtslage geht man sogar davon aus, dass beim Monitoring schutzwürdige Geheimhaltungsinteressen der Betroffenen nicht verletzt sind (vgl. § 50 a Abs. 4 Ziffer 3 DSG).

Was den Retail-Bereich angeht, so wird in allen drei Ländern von der Erforderlichkeit der dort eingesetzten Kamerasysteme in der Regel ausgegangen. Das Amtsgericht Hamburg hat in einer Entscheidung vom 22.04.2008 unter anderem festgestellt, dass Videoaufzeichnungen als Beweismittel besser geeignet sind als Zeugenaussagen (zum Beispiel eines Wachmannes). Allerdings muss in allen drei Ländern auch eine hinreichend konkrete Gefahr von Übergriffen vorliegen. Dieses Merkmal ist in Anbetracht der hohen Diebstahlsraten im Einzelhandel regelmäßig gegeben.

Angemessenheit

Selbst wenn eine Videoüberwachung aber zweckmäßig und erforderlich ist, darf sie in allen drei Ländern nicht zum Einsatz kommen, wenn damit in unzumutbarer Weise in die Persönlichkeitsrechte der Betroffenen eingegriffen wird. Dies ist regelmäßig der Fall in Räumlichkeiten, in den Kommunikation beziehungsweise soziale Interaktion stattfindet (sogenannte Privatsphäre). Aus diesem Grunde sind beispielsweise gastronomische Bereiche (zum Beispiel die Stehtische vor dem Verkaufsstand einer Bäckerei) auszupixeln oder zu maskieren. Gleiches gilt für sogenannte Raucherecken, an denen Mitarbeiter oder auch Kunden ihrem Laster frönen. Absolut unzumutbar ist eine Bilddatenerhebung schließlich in Sanitär- oder Umkleideräumen, weil dort die Intimsphäre betroffen ist. Auch wenn viele Kaufhausdiebstähle in den Umkleidekabinen vorbereitet werden, darf dort also nicht gefilmt werden. In Österreich ist dies sogar ausdrücklich durch § 50 a Abs. 5 DSG (keine Überwachung des höchstpersönlichen Lebensbereiches eines Betroffenen) verboten. In allen übrigen Bereichen eines Einkaufsmarktes (zum Beispiel Eingang, Regale, Kassen) fällt die Abwägung zwischen den schutzwürdigen Interessen der Kunden einerseits und den anzuerkennenden Zwecken des Betreibers andererseits zugunsten des Letzteren aus, weil der nur kurzzeitige Eingriff in Persönlichkeitsrechte in der sogenannten Sozial- oder Geschäftsphäre in der Regel zu dulden ist.

Überwachung von Mitarbeitern

In allen drei Ländern ist man sich einig, dass bei der Videoüberwachung auf die Persönlichkeitsrechte der Arbeitnehmer in besonderem Maße Rücksicht zu nehmen ist. Denn im Gegensatz zu den nur kurzzeitig erfassten Kunden sind die Mitarbeiter durch die in den Einkaufsmärkten angebrachten Systeme einer permanenten Überwachung ausgesetzt. Die Kameras sind daher in der Regel so auszurichten, dass Mitarbeiter so wenig wie möglich, jedenfalls aber nicht frontal, ins Bild geraten. Dies geschieht am besten dadurch, dass zum Beispiel bei Arbeitsplätzen am Verkaufstresen oder an der Kasse die Aufnahmen von hinten über die Schulter des Mitarbeiters erfolgen (siehe hierzu auch die Hinweise des eidgenössischen Datenschutzbeauftragten zur Positionierung von Videokameras in Warenhäusern und in Banken).

Permanente Schreibtischarbeitsplätze sollten gar nicht erfasst oder jedenfalls ausgepixelt beziehungsweise maskiert werden. Ansonsten ist bei jeder Erfassung von Betriebsabläufen (zum Beispiel Erfassung der Packstation im Lager) eine Abwägung zwischen den Interessen des Betreibers auf Kontrolle und Beweissicherung einerseits und den Interessen des Mitarbeiters vor allzu starker Beeinträchtigung seiner Bewegungsfreiheit andererseits abzuwägen. In

Bereichen, in denen die Sicherungsinteressen des Betreibers in besonderem Maße berührt sind (zum Beispiel Tresorräume), ist eine dauernde Überwachung in der Regel gerechtfertigt.

Verbot der Verhaltenskontrolle

Selbst bei einem schonenden Einsatz von Überwachungskameras sind die damit erhobenen Aufnahmen für den Betreiber und Arbeitgeber durchaus geeignet, auch das Verhalten und die Leistung seiner Arbeitnehmer zu kontrollieren. Eine Bilddatenerhebung und Auswertung zu diesen Zwecken ist jedoch in allen drei Ländern verboten. In Österreich bringt dies § 50 a Abs. 5 Satz 2 DSG mit dem Satz „Weiters ist die Videoüberwachung zum Zweck der Mitarbeiterkontrolle an Arbeitsstätten untersagt“ auf den Punkt. Dabei handelt es sich um ein absolutes Verbot, das auch nicht durch die ausdrückliche Zustimmung des Arbeitnehmers - deren Freiwilligkeit im Arbeitsverhältnis ohnehin anzuzweifeln wäre - umgangen werden kann (vgl. Beschluss der österreichischen Datenschutzkommission vom 23.11.2012). Auch in der Schweiz sind Überwachungs- oder Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, unzulässig (vgl. Artikel 26 der Verordnung 3 zum Arbeitsgesetz). Sind derartige Systeme aus anderen Gründen (zum Beispiel zur Sicherheits- oder Leistungsüberwachung) erforderlich, sind sie so zu gestalten und anzuordnen, dass die Gesundheit und Bewegungsfreiheit der Arbeitnehmer dadurch nicht beeinträchtigt wird. Insofern ist in der Schweiz eine sogenannte „Leistungsüberwachung“ zugelassen, wobei jedoch die Verhältnismäßigkeit gewahrt werden muss (vgl. Wegleitung der SECO zur Verordnung 3 zum Arbeitsgesetz).

In Deutschland fehlt es derzeit noch an einem ausdrücklichen gesetzlichen Verbot der Verhaltenskontrolle. Denn der seit nunmehr über zwei Jahre vorliegende Gesetzentwurf zum Beschäftigtendatenschutz, wonach Daten der Videoüberwachung nicht für eine allgemeine Verhaltenskontrolle erhoben, verarbeitet oder genutzt werden dürfen (vgl. § 32 f. Abs. 2 BDSG), ist immer noch nicht in Kraft gesetzt worden. Es liegen jedoch mehrere Grundsatzentscheidungen des Bundesarbeitsgerichtes vor, wonach Überwachungsmaßnahmen nicht zu einer anlassunabhängigen Leistungs- und Verhaltenskontrolle eingesetzt werden dürfen (vgl. BAG, Urteile vom 29.06.2004 und 26.08.2008). Ansonsten können in Deutschland personenbezogene Daten eines Beschäftigten für Zwecke des Beschäftigungsverhältnisses nur erhoben, verarbeitet oder genutzt werden, wenn dies für dessen Durchführung oder Beendigung erforderlich ist (vgl. § 32 BDSG). Gleiches gilt in der Schweiz gemäß Artikel 328 b des Obligationenrechtes. Nach diesen Regelungen dürfte die Bilddatenerhebung in Bezug auf Mitarbeiter jedenfalls zur Zutrittskontrolle, zur Autorisierung und Authentifizierung sowie zur Wahrnahme von Fürsorgepflichten (zum Beispiel Sicherheit der Beschäftigten) zulässig sein.

Aufdeckung von Straftaten

In Anbetracht der Tatsache, dass mehr als 50 Prozent aller Vermögensdelikte im Retail-Bereich von Mitarbeitern begangen werden, liegt es für den Arbeitgeber nahe, Videokameras auch gezielt zur Aufdeckung derartiger Straftaten einzusetzen. Dies ist jedoch in allen drei Ländern nur in eng umschriebenen Grenzen möglich, da die Verfolgung von Straftaten in erster Linie Sache der Ordnungsbehörden ist. So dürfen in Deutschland personenbezogene Daten eines Beschäftigten zur Aufdeckung von Straftaten nur dann erhoben, verarbeitet oder genutzt werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass der Betroffene im Beschäftigungsverhältnis eine Straftat begangen hat (vgl. § 32 Abs. 1 Satz 2 BDSG). Allerdings muss auch in einem solchen Fall die Verhältnismäßigkeit gewahrt sein, insbesondere was Art und Ausmaß der Überwachung im Hinblick auf den Anlass angeht. Nach herrschender Meinung wird durch diese Vorschrift auch der heimliche Kameraeinsatz bei Verdacht von Diebstahl oder Unterschlagung legitimiert. Sollte allerdings das Gesetz zum Beschäftigtendatenschutz in seiner jetziger Form in Kraft treten, wäre dies gemäß § 32 e des Entwurfes nicht mehr zulässig.

In der Schweiz gibt es keine vergleichbaren Vorschriften. Nach Hinweisen des eidgenössischen Datenschutzbeauftragten ist der Einsatz eines Überwachungssystems durch den Arbeitgeber zur Aufdeckung von Straftaten ausnahmsweise zulässig, wenn Notstand besteht (das heißt wenn alle anderen Mittel versagt haben und akuter Handlungsbedarf besteht). Der Arbeitgeber ist aber in solchen Fällen gehalten, sobald als möglich eine eventuelle weitere Überwachung durch die zuständige Behörde bewilligen zu lassen. Dem hat eine Anzeige gegen Unbekannt voranzugehen, wonach die Überwachung dann in der Regel richterlich oder gerichtspolizeilich angeordnet wird. In Österreich gibt es keine vergleichbaren Regelungen, hier dürfte die Bilddatenerhebung zur Aufdeckung von Straftaten nur zulässig sein, wenn dies ausdrücklich durch die Ordnungsbehörden angeordnet beziehungsweise erlaubt worden ist.

Mitbestimmung

In allen drei Ländern haben Arbeitgeber ihre Mitarbeiter über die Einführung von Videoüberwachungsmaßnahmen zumindest zu informieren. So hat der Betriebsinhaber nach dem österreichischen Arbeitsverfassungsgesetz dem Betriebsrat Mitteilung zu machen, welche Arten von personenbezogenen Arbeitnehmerdaten er automationsunterstützt aufzeichnet und welche Verarbeitungen und Übermittlungen er vorsieht. Dem Betriebsrat ist auf Verlangen die

Überprüfung der Grundlagen für die Verarbeitung und Übermittlung zu ermöglichen (vgl. § 91 Abs. 2 ArbVG). Auch in der Schweiz muss der Arbeitgeber dafür sorgen, dass alle in seinem Betrieb beschäftigten Arbeitnehmer ausreichend und angemessen informiert und angeleitet werden über die bei ihren Tätigkeiten auftretenden Gefahren sowie über die Maßnahmen der Gesundheitsvorsorge zu deren Verhütung (vgl. Artikel 5 der Verordnung Nr. 3 zum Arbeitsgesetz). Hierunter ist auch die Einführung von technischen Überwachungssystemen zu subsumieren. Vergleichbare Informationspflichten ergeben sich in Deutschland aus dem Betriebsverfassungsgesetz beziehungsweise dem Bundesdatenschutzgesetz.

Rechtslage in Deutschland

Insbesondere aber unterliegt die Einführung von Videoüberwachungsmaßnahmen auch der arbeitsrechtlichen Mitbestimmung. So ist in Deutschland der Betriebsrat gemäß § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz bei der Einführung und Anwendung technischer Einrichtungen, die dazu bestimmt sind, das Verhalten oder die Leistung der Beschäftigten zu überwachen, in jedem Falle zu beteiligen. Dabei reicht es aus, dass diese Einrichtungen zu einer Verhaltens- beziehungsweise Leistungskontrolle lediglich geeignet sind, was bei Videoüberwachungsanlagen stets der Fall ist. Das Mitbestimmungsrecht realisiert sich in der Regel durch den Abschluss von Betriebsvereinbarungen, die im Übrigen auch nach Datenschutzrecht eine legitimierende Rechtsgrundlage für die Datenerhebung darstellen (sogenannte „andere Rechtsvorschrift“ i. S. v. § 4 Abs. 1 BDSG). In der zwischen Arbeitgeber- und Arbeitnehmervertretung ausgehandelten Betriebsvereinbarung sind die einzuführenden Maßnahmen sowie die technischen Parameter des Überwachungssystems detailliert zu beschreiben.

Des Weiteren werden konkrete Regelungen über die Zugangs- und Zugriffsberechtigung, über die Auswertung der Daten (zum Beispiel Vier-Augen-Prinzip), über die Speicherung, Löschung sowie Nutzung und Weitergabe der Bilddaten aufgestellt. Zumeist enthalten derartige Betriebsvereinbarungen auch Bestimmungen, nach denen die beschlossenen Maßnahmen in regelmäßigen Abständen auf deren Sinnhaftigkeit überprüft werden. Erfahrungsgemäß verlangt der Betriebsrat in den Verhandlungen größere Einschränkungen des Kameraeinsatzes, als nach Datenschutzrecht möglich und aus Sicherheitsgründen geboten wäre. Kommt daher eine Einigung über den Abschluss der Vereinbarung nicht zustande, so kann in Deutschland die Einigungsstelle eingerufen werden (vgl. § 87 Abs. 2 i. V. m. § 76 Betriebsverfassungsgesetz), welche auf Antrag des Arbeitgebers die Zustimmung des Betriebsrates durch einen eigenen Spruch ersetzen kann. Sind die Parteien mit diesem Spruch nicht einverstanden, so ist eine arbeitsgerichtliche Überprüfung im Instanzenweg möglich.

Rechtslage in Österreich

In Österreich hingegen kann der Arbeitgeber die Zustimmung des Betriebsrates zur Einführung derartiger Systeme nicht erzwingen. Zwar sieht auch hier das einschlägige Arbeitsverfassungsgesetz den Abschluss von Betriebsvereinbarungen in Bezug auf „Maßnahmen zur menschengerechten Arbeitsgestaltung“ vor (vgl. § 97 Abs. 1 Ziffer 9 ArbVG). Die Zustimmung des Betriebsrates kann im Streitfall aber nur dann durch eine Entscheidung der Schlichtungsstelle ersetzt werden, wenn es um die Einführung von Systemen zur automationsunterstützenden Ermittlung, Verarbeitung und Übermittlung von personenbezogenen Daten des Arbeitnehmers geht (vgl. § 96 a Abs. 1 ArbVG). Handelt es sich hingegen um die Einführung von Kontrollmaßnahmen und technischen Systemen zur Kontrolle der Arbeitnehmer, die deren Menschenwürde berühren (können) (vgl. § 96 Abs. 1 Ziffer 3 ArbVG), ist dieser Rekurs nicht möglich. In Österreich geht die herrschende Meinung davon aus, dass Videoüberwachungsmaßnahmen in jedem Falle die Menschenwürde von Arbeitnehmern berühren, sodass der Betriebsrat im Streitfall die Einführung der Videoüberwachung blockieren kann.

Rechtslage in der Schweiz

In der Schweiz hingegen können die Arbeitnehmervertretungen noch nicht einmal den Abschluss von Betriebsvereinbarungen einfordern. Zwar stehen diesen gemäß Artikel 48 des Bundesgesetzes über die Arbeit in Industrie, Gewerbe und Handel (Arbeitsgesetz) bei „Fragen des Gesundheitsschutzes“ Mitspracherechte zu, worunter auch die Einführung von Überwachungssystemen verstanden wird. Sie haben allerdings nur die Möglichkeit, hierzu Vorschläge und Anregungen vorzubringen. Der Arbeitgeber darf die berechtigten Anliegen der Arbeitnehmer auch nicht nur lediglich zur Kenntnis nehmen. Setzt er sich über diese Bedenken und Hinweise hinweg, so hat er seine Entscheidungen den Arbeitnehmervertretungen gegenüber zu begründen. Weitere Pflichten bestehen hingegen nicht. Insofern findet eine gerichtliche Überprüfung der eingeführten Überwachungsmaßnahmen nur dann statt, wenn einzelne Arbeitnehmer hiergegen vorgehen.

Derartige Möglichkeiten stehen natürlich auch den Arbeitnehmern in Deutschland und in Österreich zur Verfügung. Wurden jedoch zuvor Betriebsvereinbarungen mit den Personalvertretungen abgeschlossen, so sind diesen Klagen in der Regel keine großen Erfolgschancen beizumessen.

Sonstige Pflichten in Bezug auf die Bilddatenbearbeitung

In Anbetracht der Tatsache, dass aufgezeichnete Daten einem besonderen Missbrauchsrisiko unterliegen, enthalten die Rechtsordnungen aller drei Länder ausführliche Regelungen darüber, wie die Weitergabe von Daten, deren Löschung, deren Schutz vor missbräuchlicher Verwendung, deren Bearbeitung durch Dritte etc. zu gestalten ist. Des Weiteren enthalten die Datenschutzgesetze Bestimmungen über Melde- und Registrierungspflichten sowie über die Durchführung von datenschutzrechlichen Vorabkontrollen. Im Detail bestehen jedoch eine Reihe von Unterschieden, auf die nachfolgend näher eingegangen werden soll.

Weitergabe von Bilddaten

In allen drei Ländern ist man sich einig, dass Videoaufzeichnungen nur in Verdachtsfällen beziehungsweise bei konkreten Anhaltspunkten ausgewertet werden dürfen. In der Schweiz ergibt sich dies aus Art. 4 Abs. 3 des Datenschutzgesetzes, wonach Personendaten nur zu dem Zweck bearbeitet werden dürfen, der bei der Beschaffung angegeben wurde, aus den Umständen ersichtlich oder gesetzlich vorgesehen ist. Ähnliches lässt sich aus § 6 Abs. 1 des DSG-Österreich ableiten. In Deutschland ist die Verarbeitung oder Nutzung der durch die Beobachtung erhobenen Daten nur zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen (vgl. § 6 b Abs. 2 BDSG).

Für einen anderen Zweck dürfen die Bilddaten in Deutschland nur verarbeitet oder genutzt werden, soweit dies zur Abwehr von Gefahren für die staatliche und öffentliche Sicherheit sowie zur Verfolgung von Straftaten erforderlich ist (§ 6 b Abs. 2 Satz 2 BDSG). Danach ist eine Weitergabe der Aufzeichnungen (Übermittlung) nur zu Zwecken der polizeilichen Prävention und/oder Strafverfolgung zulässig. Gleiches gilt gemäß § 50 a Abs. 6 DSG-Österreich. Danach verletzt die Übermittlung von Videodaten an Behörden dann nicht die Geheimhaltungsinteressen der Betroffenen, wenn beim Auftraggeber der begründete Verdacht besteht, die Daten könnten eine von Amtswegen zu verfolgende gerichtlich strafbare Handlung dokumentieren. Dies schließt sogenannte „Zufallsfunde“ ausdrücklich mit ein. Die Übermittlung setzt allerdings voraus, dass die Behörden die Herausgabe als Beweismittel fordern können. Derartige Befugnisse ergeben sich in Österreich aus § 109 StPO (Sicherstellung, Beschlagnahme) beziehungsweise § 19 AVG (mitzubringende Beweismittel). In der Schweiz ergibt sich die zweckgebundene Weitergabe von Bilddaten aus den allgemeinen Grundsätzen in Art. 4 Abs. 3 DSG (siehe oben).

Protokollierungs- und Löschungspflichten

Nach § 50 DSG Österreich ist jeder Verwendungsvorgang einer Videoüberwachung beim Bearbeiter zu protokollieren. Alle Zugriffe und Verwendungen sind mit Angabe des Ortes und der Zeit, der Art der Verwendung und der Person des Verwenders zu erfassen und zu dokumentieren. Derart konkrete Protokollierungspflichten sehen die deutschen und schweizerischen Datenschutzregelungen nicht vor.

In allen drei Ländern ist man sich jedoch einig, dass aufgezeichnete Daten spätestens dann zu löschen sind, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen einer weiteren Speicherung entgegenstehen (vgl. z. B. § 6 b Abs. 5 BDSG). In der Schweiz wird die Löschungspflicht aus den Zweckbindungsgrundsätzen aus Art. 4 Abs. 3 DSG abgeleitet, ohne dass konkrete Löschungsfristen vorgegeben werden. Dies ist in Österreich anders, wonach aufgezeichnete Daten spätestens nach 72 Stunden zu löschen sind (vgl. § 50 DSG). Ausnahmen ergeben sich, wenn der Beweis zu sichern ist (Abspeichern der relevanten Sequenz) oder wenn die Daten an Sicherheitsbehörden gemäß § 50 a Abs. 6 zu übermitteln sind. Will ein Unternehmen die Daten länger speichern, so ist dies gegenüber der Datenschutzkommission (DSK) als Aufsichtsbehörde ausführlich zu begründen. Eine längere Frist wird von der DSK in der Regel nur akzeptiert, wenn dies aus besonderen Gründen zur Zweckerreichung regelmäßig erforderlich ist.

Maßnahmen zum Schutz der Daten

Nach allen drei Datenschutzgesetzen müssen Personendaten vom Betreiber durch angemessene technische und organisatorische Maßnahmen gegen unbefugtes Bearbeiten geschützt werden (vgl. § 9 BDSG, § 15 DSG-Österreich, Art. 7 DSG-Schweiz). Insbesondere hat der Bearbeiter die Daten vor Missbrauch, Verlust, Beschädigung zu schützen, das heißt die Vertraulichkeit, die Verfügbarkeit und die Integrität der Daten sicherzustellen. Einzelheiten hierzu sind in Deutschland in einer Anlage zu § 9 BDSG und in der Schweiz in den Art. 8 und 9 der VDSG (Verordnung zum DSG) geregelt. Dies betrifft bei automatisierter Bearbeitung von Daten insbesondere die Zutrittskontrolle, die Zugangskontrolle, die Weitergabekontrolle, die Speicherkontrolle, die Benutzer- und Zugriffskontrolle sowie die Eingabekontrolle. In Österreich sind diese Maßnahmen in Abs. 2 von § 14 DSG geregelt.

Alle drei Datenschutzgesetze enthalten auch Vorschriften über die sogenannte Auftragsdatenverarbeitung. Danach muss der Auftraggeber sicherstellen, dass der mit der Bearbeitung beauftragte Dritte sämtliche Regelungen über die Datensicherheit in eigener Person gewährleistet (vgl. § 11 BDSG, §§ 10 und 11 DSG Österreich und Art. 10 a DSG Schweiz). Dem Dritten sind also sämtliche datenschutzrechtlichen Pflichten vertraglich zu übertragen, wobei der Auftraggeber für Pflichtverletzungen des Dritten haftbar bleibt. In Deutschland und in Österreich sind Vereinbarungen zwischen dem Auftraggeber und dem Dienstleister über die nähere Ausgestaltung ihrer Pflichten schriftlich festzuhalten.

Melde- und Registrierungspflichten, Vorabkontrolle

Was die Melde- und Registrierungspflichten sowie die sogenannte datenschutzrechtliche Vorabkontrolle angeht, so findet man in den drei Ländern derzeit noch unterschiedliche Regelungen.

Rechtslage in Deutschland

Gemäß § 4 d Abs. 1 BDSG sind Verfahren automatisierter Datenverarbeitungen vor ihrer Inbetriebnahme von den Betreibern der zuständigen Aufsichtsbehörde zu melden. Dabei handelt es sich in Deutschland um die jeweiligen Landesdatenschutzbeauftragten, deren Befugnisse in § 38 BDSG geregelt sind. Eine Meldepflicht entfällt jedoch, wenn das Unternehmen einen Beauftragten für den Datenschutz bestellt hat. Hierzu sind alle nicht öffentlichen Stellen verpflichtet, bei denen mehr als neun Personen ständig mit der automatisierten Verarbeitung von personenbezogenen Daten beschäftigt sind (vgl. § 4 f Abs. 1 BDSG). Dies dürfte bei Unternehmen aus dem Retail-Bereich regelmäßig der Fall sein.

Soweit automatisierte Verarbeitungen besondere Risiken für die Rechte und Freiheiten der Betroffenen aufweisen, ist durch den Datenschutzbeauftragten vor Beginn der Verarbeitung gemäß § 4 d Abs. 5 eine sogenannte Vorabkontrolle durchzuführen. Besondere Risiken sind insbesondere dann gegeben, wenn die Verarbeitung der Daten geeignet ist, die Persönlichkeit der Betroffenen zu bewerten einschließlich seiner Fähigkeiten, seiner Leistung oder seines Verhaltens. Dies ist bei der Auswertung von Videodaten in der Regel möglich, sodass der Betrieb von Videoüberwachungsanlagen stets einer innerbetrieblichen Vorabkontrolle unterliegt. Die Unternehmen haben mit anderen Worten die von ihnen bestellten Datenschutzbeauftragten in jedem Falle vorher mit der Sache zu befassen, bevor eine Videoüberwachungsanlage in Betrieb geht. Sind sich Unternehmen und Datenschutzbeauftragte über die Rechtmäßigkeit der Maßnahmen nicht einig, so kann sich der betriebliche Datenschutzbeauftragte zur weiteren Klärung an die Aufsichtsbehörde wenden.

Rechtslage in Österreich

In Österreich unterliegen Videoüberwachungen grundsätzlich der Meldepflicht bei der zentralen Datenschutzkommission zum Zwecke der Registrierung im dort geführten Datenverarbeitungsregister. Die über das Internet zu erfolgende Meldung hat Folgendes mindestens zu enthalten: Daten des Auftraggebers, Zweck der zu registrierenden Datenanwendung und ihre Rechtsgrundlagen, konkrete Örtlichkeit der Videoüberwachung, Ausführungen zur Verhältnismäßigkeit, Angaben zum Systemablauf, Angaben zu Hinweisschildern etc. Eine Meldung ist mangelhaft, wenn Angaben fehlen, offenbar unrichtig, unstimmig oder so unzureichend sind, dass diejenigen, die in das Register Einsicht nehmen, keine hinreichenden Informationen über die Wahrung ihrer schutzwürdigen Geheimhaltungsinteressen erhalten. Nach derzeitiger Rechtslage sind Videoüberwachungen dann von der Meldepflicht ausgenommen, wenn es sich um Fälle der Echtzeitüberwachung handelt (sogenanntes Monitoring) oder wenn eine Speicherung auf einem analogen Speichermedium erfolgt (vgl. § 50 c Abs. 2 DSG-Österreich).
Nicht anmeldepflichtig sind des Weiteren Überwachungsmaßnahmen, die einer sogenannten „Standardanwendung“ entsprechen. Hierbei handelt es sich um Videoüberwachungsmaßnahmen in öffentlich zugänglichen Bankräumlichkeiten, bei Juwelieren, Gold- und Silberschmieden, Handel mit Antiquitäten und Kunstgegenständen, Tabak-Trafiken, Tankstellen und bebauten Privatgrundstücken. Nach der jüngst aktualisierten Standard- und Musterverordnung 2004 setzt dies allerdings voraus, dass die Videoüberwachung verschlüsselt vorgenommen wird und eine Löschung der Daten nach 72 Stunden erfolgt.

Der Vollbetrieb einer Videoüberwachung darf unmittelbar nach Abgabe der Meldung aufgenommen werden, wenn der Auftraggeber in der Meldung zusagt, die Videoüberwachungsdaten zu verschlüsseln und durch Hinterlegung des einzigen Schlüssels bei der DSK sicherzustellen, dass eine Auswertung nur im begründeten Anlassfall durch eine bestimmte Stelle stattfindet. Dies ist für den Retail-Bereich in der Regel nicht praktikabel, weil die ständigen Vorkommnisse einer Aufklärung vor Ort erfordern. Insofern bedarf es bei der Videoüberwachung durch Kaufhäuser und Supermärkte in der Regel einer „händischen“ Vorabkontrolle durch die DSK, weil die Videoaufzeichnungen im Zweifel immer auch sensible Daten, jedenfalls aber strafrechtlich relevante Daten enthalten können, was eine Prüfung durch die DSK erforderlich macht (vgl. § 18 Abs. 2 i. V. m. § 20 DSG).

Insofern sollten sich die Unternehmen bei der Anmeldung ihrer beabsichtigten Videoüberwachung Mühe geben. Ergibt die Prüfung durch die DSK eine Mangelhaftigkeit der Meldung, so ist dem Auftraggeber innerhalb von zwei Monaten nach deren Eingang die Verbesserung unter Setzung einer angemessenen Frist aufzutragen. Wird dem Verbesserungsauftrag nicht entsprochen, ist die Registrierung unter Hinweis auf die beanstandeten Punkte schriftlich abzulehnen. Wird die Anwendung dann vom Auftraggeber förmlich beantragt, erfolgt die Ablehnung durch Bescheid der DSK, gegen den kein Rechtsmittel mehr gegeben ist.

Das zentrale Registrierungsverfahren steht in Österreich in der Kritik, weil die DSK die Flut von Registrierungsanträgen kaum noch bewältigen kann. Aus diesem Grunde ist beabsichtigt, durch eine entsprechende Gesetzesänderung eine Vorabkontrolle nach dem deutschen Muster durch bei den Unternehmen angesiedelte Datenschutzbeauftragten durchführen zu lassen.

Rechtslage in der Schweiz

Auch in der Schweiz müssen Datensammlungen gemäß Artikel 11 a DSG grundsätzlich angemeldet werden, wenn besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet werden. Nach herrschender Meinung ist dies bei Videodaten aber nicht der Fall, sodass in der Schweiz - anders als in Deutschland und Österreich - eine Anmeldung nicht erforderlich ist. Auch sieht das DSG-Schweiz staatliche Vorabkontrollen für privaten Datenverarbeitungen nicht vor. Gleiches gilt für die betrieblich bestellten Datenschutzbeauftragten, denen eine solche Aufgabe durch das DSG nicht zugewiesen ist. Allerdings prüft der betriebliche Datenschutzbeauftragte nach Artikel 12 b der Verordnung zum DSG die Bearbeitung von Personendaten und empfiehlt Korrekturmaßnahmen, wenn er feststellt, dass Datenschutzvorschriften verletzt wurden. Insofern ist auch in der Schweiz zu empfehlen, den betrieblichen Datenschutzbeauftragten vor Einführung der Videoüberwachung in die Planung mit einzubeziehen, um spätere Streitigkeiten zu vermeiden.

Sanktionen und zivilrechtliche Ansprüche

Die Verletzung von Datenschutzbestimmungen gilt bei vielen Unternehmen immer noch als „Kavaliersdelikt“. Um dem zu begegnen, sehen die Datenschutzgesetze in allen drei Ländern Sanktionsmöglichkeiten durch die zuständigen Behörden vor. Darüber hinaus können die Betroffenen nach dem Zivilrecht Unterlassungs- und sogar Schadensersatzansprüche gegen die Betreiber rechtswidriger Überwachungsmaßnahmen geltend machen.

Befugnisse der Datenschutzbeauftragten

Die Kompetenzen der nationalen Datenschutzbeauftragten fallen in den drei Ländern unterschiedlich aus. So kann der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) nach Aufklärung von streitigen Sachverhalten lediglich Empfehlungen abgeben. Wird diesen Empfehlungen nicht gefolgt oder diese von den Betreibern abgelehnt, so kann er die Angelegenheit dem Bundesverwaltungsgericht zum Entscheid vorlegen (Artikel 29 DSG). Auch in Österreich kann die Datenschutzkommission im Falle eines begründeten Verdachtes (etwa aufgrund einer Anzeige von Betroffenen) konkret Datenanwendungen auf die Verletzung geschützter Rechte überprüfen. Wird den sodann von der DSK ausgesprochenen Empfehlungen nicht entsprochen, so kann die DSK von Amts wegen Strafanzeige erstatten oder bei schwerwiegenden Verstößen durch Auftraggeber des privaten Bereichs Klage vor dem zuständigen Gericht erheben (vgl. § 30 DSG Österreich).
Die weitere Verfolgung der Verstöße obliegt daher den Gerichten, wonach die Strafgerichte gemäß § 52 DSG bei Übertretungen der Schutzbestimmungen Strafen erlassen können. Grobe Verwaltungsübertretungen sind danach mit Geldstrafe bis zu 25.000 Euro zu ahnden. Wer Daten ermittelt, verarbeitet oder übermittelt, ohne seine Meldepflicht erfüllt zu haben oder eine Datenanwendung auf eine von der Meldung abweichende Weise betreibt, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 10.000 Euro geahndet wird. Datenanwendung in Gewinn- oder Schädigungsabsicht können in Österreich sogar mit Freiheitsstrafe bis zu einem Jahr bestraft werden.

In Deutschland kann die Aufsichtsbehörde (dabei handelt es sich um die jeweiligen Landesdatenschutzbeauftragten) gemäß § 38 BDSG nicht nur streitige Sachverhalte aufklären, sondern auch Maßnahmen zur Beseitigung festgestellter technischer oder organisatorischer Mängel anordnen. Bei schwerwiegenden Verstößen/Mängeln (insbesondere Persönlichkeitsrechtsverletzungen) kann die Aufsichtsbehörde sogar den Einsatz einzelner Verfahren untersagen, wenn die Verstöße/Mängel trotz Verhängung eines Zwangsgeldes nicht in angemessener Zeit beseitigt sind. Darüber hinaus stellt die unbefugte Erhebung, Verarbeitung und Übermittlung personenbezogener Daten eine Ordnungswidrigkeit dar, die von der Aufsichtsbehörde gemäß § 43 BDSG mit Bußgeldern bis zu 300.000 Euro geahndet werden kann.

Schadensersatzansprüche der Betroffenen

Gemäß Artikel 15 DSG-Schweiz richten sich Klagen zum Schutz der Persönlichkeit nach den Artikeln 28, 28 a sowie 28 e des schweizerischen Zivilgesetzbuches. Danach kann die klagende Partei insbesondere verlangen, dass die Datenverarbeitung gesperrt wird, keine Daten an Dritte bekannt gegeben oder die Personendaten berichtigt oder vernichtet werden. Ansprüche Privater wegen Verletzung ihrer Rechte auf Geheimhaltung, auf Richtigstellung oder auf Löschung gegen Rechtsträger, die in Form des Privatrechtes eingerichtet sind, sind auf dem Zivilrechtsweg geltend zu machen (vgl. § 32 Abs. 1 DSG). Danach hat ein Auftraggeber, der Daten schuldhaft entgegen den Bestimmungen des DSG verwendet hat, dem Betroffenen den erlittenen Schaden nach den allgemeinen Bestimmungen des bürgerlichen Rechts zu ersetzen (vgl. § 33 Abs. 1 DSG). Diese sehen einen Schadensersatzanspruch unter anderem dann vor, wenn rechtswidrig und schuldhaft in die Privatsphäre eines Menschen eingegriffen oder Umstände aus der Privatsphäre eines Menschen offenbart oder verwertet werden (vgl. § 1328 a AGBG - Schweiz).

Auch in Deutschland stehen den Betroffenen Unterlassungsansprüche gemäß § 1004 i. V. m. § 823 Abs. 2 BGB i. V. m. § 6 b BDSG wegen Verstoßes gegen datenschutzrechtliche Regelungen zu. Kommt der Betreiber entsprechenden Aufforderungen nicht nach, so können die Betroffenen Entschädigungsansprüche aus § 823 Abs. 2 BGB i. V. m. Artikel 1 und 2 des Grundgesetzes wegen Verletzung von Persönlichkeitsrechten geltend machen. Das Landesarbeitsgericht Frankfurt hat einer Mitarbeiterin beispielsweise einen Entschädigungsanspruch in Höhe von 7.000,00 zugesprochen, weil deren Büroarbeitsplatz permanent durch eine Kamera an der Eingangstür des Büros überwacht worden war (vgl. Entscheidung vom 25.10.2010). Das LAG Hamm hat allerdings in einer Entscheidung vom 25.09.2012 klargestellt, dass ein Arbeitnehmer zunächst erfolglos Unterlassungsansprüche geltend machen muss, bevor ihm materieller Schadensersatz zusteht.

In Österreich sind gemäß § 32 Abs. 1 DSG Ansprüche wegen Verletzung der Rechte einer Person auf Geheimhaltung, auf Richtigstellung oder auf Löschung personenbezogener Daten ebenfalls auf dem Zivilrechtsweg geltend zu machen. Gleiches gilt für Schadensersatzansprüche, die nach den allgemeinen Bestimmungen des Bürgerlichen Rechts durchzusetzen sind (vgl. § 33 Abs. 1 DSG). Anspruchsgrundlage ist hier § 1328 a AGBG, wonach eine Schadensersatzpflicht besteht, wenn rechtswidrig und schuldhaft in die Privatsphäre eines Menschen eingriffen wird oder wenn Umstände aus der Privatsphäre eines Menschen offenbart und verwertet werden.

Gerichtsverwertbarkeit

Rechtmäßig erlangte Bilddaten

Rechtmäßig erlangte Bilddaten können vor Gericht immer als Beweismittel eingesetzt werden. Dies gilt sowohl für die Verfolgung zivilrechtlicher Ansprüche (zum Beispiel Schadensersatz wegen Sachbeschädigung oder Diebstahl) als auch für Ansprüche in arbeitsgerichtlichen Verfahren (z. B. Kündigung von Mitarbeitern wegen aufgedeckter Diebstähle). Die Verwertung im Prozess setzt allerdings voraus, dass die Bilddaten eine Identifizierung des Täters (und Beklagten) zulassen. Die richtige Auflösung, der richtige Kamerawinkel und die Qualität des eingesetzten Kamerasystems spielen hier eine wichtige Rolle. Unternehmen im Retail-Bereich sollten deshalb bei der Kameratechnik nicht an der falschen Stelle sparen. Des Weiteren muss sichergestellt sein, dass eine Manipulation der Bilder von der Aufnahme bis zur Vorlage bei Gericht technisch ausgeschlossen ist (sogenannte „geschlossene Beweiskette“). Auch hier sollten die Unternehmen Kamerasysteme verwenden, deren Software Zeitstempel vergeben und Fälschungen technisch ausschließen.

Rechtswidrig erlangte Bilddaten

Soweit Privatpersonen beziehungsweise Unternehmen Bilddaten unter der Verletzung datenschutzrechtlicher Bestimmungen erheben, gibt es in Bezug auf deren Verwertung in allen drei Ländern keine ausdrücklichen gesetzlichen Regeln. Anders als zum Beispiel nach der Rechtslage in den Vereinigten Staaten besteht kein zwingendes Beweisverwertungsverbot. Man ist sich vielmehr einig, dass eine Verwertung zumindest bei schweren Straftaten zugelassen werden sollte. So hat etwa in der Schweiz das Strafgericht Kanton Basel rechtswidrig erhobene Videoaufzeichnungen für den Nachweis einer Brandstiftung zugelassen (vgl. Entscheidung vom 09.01.2004). Ansonsten soll eine Abwägung zwischen dem Interesse der Wahrheitsfindung/Strafverfolgung einerseits gegenüber dem Interesse des Betroffenen stattfinden, dass von seinen Daten nicht in persönlichkeitsrechtsverletzender Form Gebrauch gemacht wird. Bei dieser Abwägung spielt auch eine Rolle, in welcher Weise gegen datenschutzrechtliche Bestimmungen verstoßen wurde. So dürfte eine unzulässige Überwachung in der Privat-/Intimsphäre schwerer wiegen, als zum Beispiel ein Verstoß gegen Kennzeichnungspflichten.

Die deutsche Rechtsprechung hat die Verwendung heimlicher Videoaufnahmen zur Durchsetzung von zivilrechtlichen Schadensersatzansprüchen bisher regelmäßig verneint (zum Beispiel verdeckte Überwachung einer Waschküche, OLG

Köln, Entscheidung vom 05.04.2003). In Österreich wurde die Beweisverwertung rechtswidrig erlangten Beweismittel in Zivilprozessen hingegen dann bejaht, wenn dies aufgrund einer „Notsituation“ geboten war, etwa um einem Prozessbetrug zu begegnen (vgl. OGH vom 19.10.1999).

Soweit es um die verdeckte Videoüberwachung von Arbeitnehmern geht, liegen in Deutschland unterschiedliche Entscheidungen vor. Gegen eine generelle Beweisverwertung spricht sich das Arbeitsgericht Frankfurt in einer Entscheidung vom 25.01.2006 aus, weil ansonsten der Gesetzesverstoß durch den Arbeitgeber ohne Folgen bliebe. Das Bundesarbeitsgericht hat hingegen in einer jüngsten Entscheidung vom 21.06.2012 klargestellt, dass verdeckte Aufnahmen im Ausnahmefall verwendet werden können, wenn zuvor alle anderen Möglichkeiten zum Nachweis einer Straftat erfolglos geblieben sind, sich der Arbeitgeber daher in einer notwehrähnlichen Lage befindet.

Zusammenfassung

Wie dargelegt, findet eine Videoüberwachung im Retail-Bereich nicht im „rechtsfreien Raum“ statt. Vielmehr haben die Betreiber in allen drei Ländern, das heißt in Deutschland, Österreich und der Schweiz, die einschlägigen datenschutzrechtlichen und arbeitsrechtlichen Vorschriften zu beachten. Immerhin geht es um die Erhebung und Bearbeitung personenbezogener Daten, die aufgrund des damit verbundenen Eingriffs in Persönlichkeitsrechte einem besonderen Schutz unterliegen. Insofern sollte stets eine datenschutzrechtliche Vorabkontrolle der geplanten Maßnahmen stattfinden. Auf dieser Grundlage sollte man dann in Verhandlungen mit den Vertretern der Beschäftigten eintreten, um angemessene betriebliche Regelungen zum Einsatz der Videoüberwachungstechnik zu finden.

Allerdings sollten sich die Betreiber sinnvolle sicherheitstechnische Lösungen nicht von „Bedenkenträgern“ unnötig klein reden lassen. Die einschlägigen Gesetze erlauben bei kreativer Auslegung häufig mehr, als Datenschützer und Betriebsräte denken. Hier kommt es auf Seiten der Betreiber auf sichere Rechtskenntnisse, gute Argumente und selbstbewusste Verhandlungsführung an. Im Zweifelsfall sollte stets kompetenter rechtlicher Rat eingeholt werden.