

Auf einen Blick Nützliche Tipps und Links

Die Entscheidung des Kammergerichtes ist grundsätzlich nachvollziehbar, weil die Bank im zu entscheidenden Fall fahrlässig mit der Absicherung ihres Tresorraumes umgegangen ist. Dabei kommt es dem Gericht gar nicht darauf an, ob eine der Maßnahmen den Raub verhindert hätte. Dem Gericht geht es nur darum, ob man den Tätern eine solch dreiste Tat nicht zumindest hätte erschweren müssen. Leider setzt sich das Gericht deshalb auch nicht mehr mit der Frage auseinander, ob die Installation einer Videoüberwachungsanlage im eigentlichen Tresorraum aus datenschutzrechtlichen Gründen überhaupt zulässig ist. Das Gericht geht offensichtlich davon aus, dass der Privatsphäre der Kunden dann Genüge getan ist, wenn diese in einem nicht überwachten Nebenraum die aus den Schließfächern herausgenommenen Behältnisse leeren bzw. füllen können. Aus hiesiger Sicht ist die vom Gericht getroffene Abwägungsentscheidung vertretbar, wenn sichergestellt ist, dass die aufgezeichneten Daten in einem „Black-Box-Verfahren“ nach kurzer Frist ungesehen gelöscht werden, wenn es keine Vorkommnisse gegeben hat.

Videoüberwachung

Neues aus Rechtsprechung und Gesetzgebung

Der Einsatz von Videoüberwachung steht immer häufiger im Fokus von Rechtsprechung und Gesetzgebung. Dabei ist eine Trendwende zu beobachten. Während die Gerichte bis vor kurzem aus datenschutz- und arbeitsrechtlichen Gründen häufig restriktiv urteilten, wird die Schutz- und Beweisfunktion dieser Technik in jüngster Zeit immer positiver beurteilt. Gleiches gilt für die Gesetzgebung. Aufgrund der wachsenden Terrorgefahr hat ein Umdenken eingesetzt, welches zu Gesetzgebungsinitiativen geführt hat, über die nachfolgend ebenfalls berichtet werden soll.

I. Aktuelle Entscheidungen zur Videoüberwachung

1. Videoüberwachung im Tresorraum einer Bank

Nach einer Entscheidung des Berliner Kammergerichtes vom 02.03.2016 kann eine Bank ihren Kunden gegenüber verpflichtet sein, potentiellen Tätern das Ausrauben von Schließfächern durch geeignete Maßnahmen zu erschweren, wie z. B. durch Installation einer Videoüberwachungsanlage im eigentlichen Schließfachraum (vgl. Kammergericht, Urteil vom 02.03.2016, 26 U 18/15).

In diesem Fall hatte ein Täter unter Vorlage eines gefälschten Passes bei einer Bank ein Schließfach angemietet. Er ließ sich sodann von einem Bankangestellten in Begleitung zweier Männer, von denen einer eine große Sporttasche bei sich hatte, in den Tresorraum führen und raubte dort, nachdem sich der Bankangestellte wieder zurückgezogen hatte, zusammen mit seinen Mittätern eine Reihe von Schließfächern aus. Eine Kundin, aus deren Schließfach dabei € 65.000,00 entwendet wurden, verklagte daraufhin die Bank auf Schadensersatz. Dieser Klage wurde von Landgericht stattgegeben, sodass die Bank beim Kammergericht Berufung einlegte. Dieses wies die Berufung mit der Begründung zurück, die Bank habe die ihr gegenüber der Kundin obliegenden Obhuts- und Aufklärungspflichten verletzt. Ein Kunde, der ein Schließfach anmiete und dort in der Regel wertvolle Dinge aufbewahre, erwarte, dass die Bank gewisse Sicherheitsvorkehrungen zum Schutz der Tresore treffe. Die Bank sei deshalb verpflichtet gewesen, Maßnahmen zu ergreifen, die es Tätern zumindest in gewissem Umfang erschweren, unter Vortäuschung lauterer Absichten Zugang zum Schließfachraum zu erlangen und dort ungehindert Schließfächer auszurauben. So wäre u. a. in Betracht gekommen,

- dass die Bank die Echtheit des von einem Täter vorgelegten Passes durch ihr in der tatbetroffenen Filiale vorhandenes Datensystem überprüft,

- dass die Bank eine Kontrolle der von den Tätern mitgeführten, großen Sporttaschen bei Zugang zum Schließfachraum vornimmt,
- dass die Bank eine Kontrolle der von den Tätern mitgeführten Taschen nach Verlassen des Schließfachraums vornimmt,
- dass die Bank im eigentlichen Schließfachraum eine Videokamera installiert und dem Kunden zu Diskretionszwecken einen nicht überwachten Nebenraum zur Verfügung stellt,
- und dass die Bank eine Alarmanlage, die auf Erschütterungen reagiert, welche durch den Einsatz von Brechwerkzeug hervorgerufen werden, an die Schließfachschränke installiert.

2. Verwertung von Zufallsfunden aus einer Videoüberwachung

Nach einer Entscheidung des Bundesarbeitsgerichts vom 22.09.2016 (AZ: 2 AZR 848/15) kann die gerichtliche Verwertung eines „Zufallsfundes“ aus einer gemäß § 32 Abs. 1 Satz 2 BDSG gerechtfertigten verdeckten Videoüberwachung zulässig sein.

In diesem Fall ging es um die Frage, ob Videoaufnahmen vor Gericht verwendet werden dürfen. Die Arbeitsgeberin hatte zur Aufklärung von Kassendifferenzen unter Anwendung der Ausnahmenvorschrift des § 32 Abs. 1 Satz 2 BDSG nach Rücksprache mit dem Betriebsrat versteckte Kameras an den Kassen angebracht. Dabei wurde eine Leergutmanipulation festgestellt, allerdings durch eine Mitarbeiterin, welche die Arbeitgeberin gar nicht im Fokus hatte. Diese Mitarbeiterin wehrte sich sodann gegen die außerordentliche, fristlose Kündigung durch die Arbeitgeberin vor Gericht.

Das Bundesarbeitsgericht bestätigte im Revisionsverfahren die vom Landesarbeitsgericht gebilligte fristlose Kündigung. Nach Auffassung des BAG dürfen auch sogenannte „Zufallfunde“ vor Gericht verwertet werden. Gebotene Aufklärungsmaßnahmen nach § 32 Abs. 1 Satz 2 BDSG müssen sich nicht allein auf solche Beschäftigten beschränken, gegen die bereits ein konkreter Verdacht vorliegt. Zwar müsse der Kreis der Verdächtigen möglichst weit eingegrenzt werden. Es sei aber nicht nötig, Überwachungsmaßnahmen so einzuschränken, dass sie ausschließlich bereits konkret verdächtige Personen erfassen. Die heimliche Überwachung setzt allerdings voraus, dass der Arbeitgeber vorher alle anderen mildereren Möglichkeiten geprüft bzw. ergriffen hat. Dies war im vorliegenden Fall gegeben.

Ein Beweisverwertungsverbot käme nur dann in Betracht, wenn dies aufgrund einer verfassungsrechtlich geschützten Position einer Prozesspartei zwingend geboten wäre. Das Gericht habe deshalb zu prüfen, ob die Verwertung von heimlich beschafften persönlichen Daten und Ergebnissen, die sich aus diesen Daten ergeben, mit dem allgemeinen Persönlichkeitsrecht des Betroffenen vereinbar ist. Nach Auffassung des BAG war dies im vorliegenden Fall gegeben. Zwar greift eine verdeckte Videoüberwachung immer in das allgemeine Persönlichkeitsrecht des Betroffenen ein. Dieser Eingriff war aber aufgrund überwiegender Interessen der Arbeitgeberin gerechtfertigt. Diese hatte zuvor alle anderen Mittel ausgeschöpft, Unregelmäßigkeiten im Kassenbereich aufzuklären. Sie konnte sich auf die Ausnahmenvorschrift des § 32 Abs. 1 Satz 2 BDSG stützen, die genau für diese Fälle geschaffen worden ist und die auf ständiger Rechtsprechung beruht.

FM Praxistipp

Prüfen Sie, ob Sie die aus dem Gerichtsurteil sich ergebenden Sorgfaltspflichten einhalten.

FM Praxistipp

Diese Entscheidung des BAG ist erfreulich, weil sie für die Anwendung der Ausnahmenvorschrift des § 32 Abs. 1 Satz 2 BDSG in begrüßenswerter Weise Klarheit schafft. Danach wird man künftig auch sogenannte Zufallsfunde, die bei einer verdeckten Kameraüberwachung erhoben werden, vor Gericht verwerten können. Dies setzt allerdings voraus, dass der Arbeitgeber vorher alle anderen Mittel ausgeschöpft hat, in seinem Betrieb begangene Straftaten aufzuklären. In jedem Falle empfiehlt es sich, derartige Maßnahmen mit dem Betriebsrat vorher abzustimmen.

FM Praxistipp

Bekanntlich ist die Videoüberwachung durch nicht-öffentliche Stellen nach § 6 b Abs. 1 BDSG nur zulässig, wenn sie zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Personen überwiegen. In diese Abwägungsentscheidung konnten bisher auf Seiten des Betreibers nur dessen unmittelbare Sicherheitsbedürfnisse eingestellt werden, z. B. der Schutz seines Eigentums vor Entwendung oder Beschädigung oder der Schutz seiner Beschäftigten. Die Aufrechterhaltung der allgemeinen Sicherheit und Ordnung war und ist hingegen Aufgabe der Sicherheitsbehörden, sodass derartige Aspekte bisher nicht in der Abwägungsentscheidung berücksichtigt werden durften. Dies soll sich durch das vorgelegte Gesetz ändern, was zu begrüßen ist. Denn bereits in der Vergangenheit ist es häufig vorgekommen, dass Polizeibehörden auf die Videoaufzeichnungen von Geschäften, Veranstaltern oder Verkehrsunternehmen zugreifen mussten, um in Ermangelung eigener Bilddaten Straftaten aufzuklären, die in der räumlichen Umgebung begangen worden sind. Dieses Vorgehen wird durch das Gesetz legitimiert, außerdem eröffnen sich für die Betreiber größere Spielräume, weil sie zur Rechtfertigung ihrer Videoüberwachungsmaßnahmen nunmehr auch auf allgemeine Sicherheitsaspekte verweisen dürfen.

II. Neue Gesetzgebungsinitiativen

1. Videoüberwachungsverbesserungsgesetz

Der Bundesrat hat Ende März 2017 das „Gesetz zur Änderung des Bundesdatenschutzgesetzes – Erhöhung der Sicherheit in öffentlich zugänglichen großflächigen Anlagen und im öffentlichen Personenverkehr durch optisch-elektronische Einrichtungen“ (Videoüberwachungsverbesserungsgesetz) gebilligt. Dieses wird in Kürze in Kraft treten. Mit diesem Gesetz wird der für Videoüberwachung einschlägige § 6 b des Bundesdatenschutzgesetzes in seinem Absatz 1 wie folgt ergänzt:

„Bei der Videoüberwachung von

1. öffentlich zugänglichen großflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder

2. Fahrzeugen und öffentlich zugänglichen großflächigen Einrichtungen des öffentlichen Schienen-, Schiffs- und Busverkehrs

gilt der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse.“

Mit dieser Regelung soll festgeschrieben werden, dass der Schutz von Leben, Gesundheit oder Freiheit von Personen, die sich in den o. a. Bereichen aufhalten, besonders wichtig ist. Hintergrund ist die aktuelle Bedrohungslage durch Terroristen und Straftäter, die für ihre Anschläge immer häufiger hochfrequentierte öffentlich zugängliche Plätze in ihren Fokus nehmen. Der durch das Gesetz eingeführte Schutzgedanke soll bei der nach § 6 b Abs. 1 BDSG durchzuführenden Abwägungsentscheidung über den Einsatz von Videoüberwachungsmaßnahmen durch die Betreiber von solchen Einrichtungen und im Rahmen von Überprüfungsentscheidungen der Datenschutzaussichtsbehörden berücksichtigt werden. Damit soll das Sicherheitsniveau in Deutschland insgesamt erhöht werden.

2. Datenschutz-Anpassungs- und Umsetzungsgesetz

Der Bundestag hat am 27.04.2017 das Datenschutz-Anpassungs- und Umsetzungsgesetz EU (DSAnpUG-EU) beschlossen. Wesentlicher Gegenstand des Gesetzes ist ein völlig neues Bundesdatenschutzgesetz, mit dem das deutsche Recht an die Vorgaben der EU-Datenschutz-Grundverordnung (DSGVO) angepasst werden soll. Diese EU-Verordnung wird zum 25. Mai 2018 in Deutschland unmittelbar anwendbares Recht. Das neue Datenschutzgesetz soll nun die Basis für die Anpassung weiterer deutscher Gesetze an die DSGVO sein. Es soll ebenfalls am 25. Mai 2018 in Kraft treten.

Da seitens des Bundesrates, der diesem Gesetz noch zustimmen muss, noch Änderungen und Ergänzungen zu erwarten sind, werden wir uns mit den wesentlichen Neuerungen des Gesetzes in einer der folgenden Ausgaben auseinandersetzen. Das Gesetz ist mittlerweile verabschiedet worden und wird in Kürze im Bundesgesetzblatt veröffentlicht. Was die Videoüberwachung angeht, so entspricht der neue § 4 im Wesentlichen den bisherigen Regelungen in § 6 b BDSG. In Anbetracht der Tatsache, dass die EU-Datenschutz-Grundverordnung in Bezug auf die Datenerhebung durch Videoüberwachungsgeräte keine konkre-

te Vorschrift enthält, sah sich der deutsche Gesetzgeber berechtigt an, hierfür in Fortführung der bisherigen Regelungen eine eigene Vorschrift zu erlassen. Der neue § 4 enthält dabei auch die Neuregelungen, die durch das o. a. Videoüberwachungsverbesserungsgesetz bereits in das BDSG a. F. aufgenommen werden sollen.

Ansonsten enthält das Gesetz einige Neuerungen, auf die sich vor allen Dingen die Wirtschaft einzustellen hat. So unterliegen Unternehmen künftig einer Beweislastumkehr, dass sie die datenschutzrechtlichen Vorgaben einhalten (sogenannte Rechenschaftspflicht). Bei Verstößen können hohe Bußgelder von bis zu 20 Millionen Euro oder 4 Prozent des globalen Jahresumsatzes verhängt werden, wenn europäisches Datenschutzrecht verletzt wurde. Des Weiteren können von Datenschutzverstößen betroffene Personen (z. B. Arbeitnehmer) künftig auch Schadensersatzansprüche immaterieller Art (Schmerzensgeld) geltend machen. Die Unternehmen sind weiterhin verpflichtet, bei mehr als neun Beschäftigten einen Datenschutzbeauftragten zu bestellen. Schließlich wird Beschäftigtendatenschutz umfangreicher als bisher geregelt, wobei sich der Gesetzgeber inhaltlich in dem Rahmen gehalten hat, der durch Literatur und Rechtsprechung zum bereits heute geltenden Recht entwickelt wurde. Wir werden in einer der nächsten Ausgaben über die wesentlichen Neuregelungen noch einmal gesondert berichten.

Dr. Ulrich Dieckert
Rechtsanwalt