



Videüberwachung am Arbeitsplatz

Die Videoüberwachung von Arbeitnehmern am Arbeitsplatz ist nur unter gewissen Voraussetzungen zulässig. Arbeitgeber tun gut daran, die Zulässigkeit einer solchen Videoüberwachung vorgängig sorgfältig zu prüfen. Nicht alles, was technisch möglich ist, ist auch erlaubt.

■ Von Dr. iur. Reto Fanger

Videüberwachung des Kassenraums

So hat das Bundesgericht bereits im Jahr 2009 entschieden, dass die Videoüberwachung des Arbeitnehmers nur in Ausnahmefällen wie etwa bei der Verarbeitung von Edelmetallen oder beim Anvertrauen von wertvollem Schmuck in einem Uhren- und Juwelengeschäft zulässig ist. Es fand eine verborgene Überwachung des rückwärtigen Kassenraums statt.

Ähnlich ein anderer Bundesgerichtsentscheid, der sich auf die versteckte Videoüberwachung an der Kasse bezieht und auf deren Film eine Angestellte aufgezeichnet war, wie sie Geldnoten aus der Kasse entwendet hatte.

Grundsätze zur Videoüberwachung am Arbeitsplatz

Generell ist eine Videoüberwachung des Arbeitsplatzes, die der Verhaltensüberwachung der Arbeitnehmer dient, immer unzulässig, während die Videoüberwachung aus anderen Gründen – sei es zur Wahrung der Sicherheit, zum Zweck der Leistungskontrolle oder zum Schutz vor Diebstahl – zulässig ist, vorausgesetzt, die Gesundheit der Arbeitnehmenden wird dadurch nicht gefährdet.

Der Arbeitnehmer darf dabei nicht oder nur ausnahmsweise von der Kamera erfasst sein, da sonst seine Gesundheit gefährdet werden kann. Denkbar sind Videokameras ausserhalb der Gebäude

und bei den Parkplätzen, bei Zugängen oder Eingängen, bei Durchgängen, bei gefährlichen Maschinen und Anlagen, in Tresorräumen, bei Gasinstallationen im Freien, bei Lagern mit gefährlichen oder wertvollen Gütern oder in der Schalterhalle einer Bank. Sind öffentliche Plätze betroffen, ist die Bewilligungspflicht mit der zuständigen Gemeinde vorgängig abzuklären.

Überwachung muss verhältnismässig sein

Das Verhältnismässigkeitsprinzip verlangt überdies, dass die Videoüberwachung nicht weiter geht, als dies zur Erreichung des zulässigen Zwecks notwendig ist. Grundsätzlich sollten Videoüberwachungsanlagen am Ar-



beitsplatz nur dann eingesetzt werden, wenn der angestrebte Zweck nicht durch weniger einschneidende Massnahmen erreicht werden kann. Die totale Überwachung des Arbeitsplatzes ist nicht erlaubt.

Zeitliche Beschränkungen

Denkbar sind denn auch zeitlich beschränkte Videoüberwachungen der Angestellten zu Schulungszwecken. Die Aufnahmeperiode muss so kurz wie möglich gehalten werden und darf nicht zum Zweck der Verhaltensüberwachung verwendet werden.

Allenfalls sind datenschutzfreundliche Technologien wie Privacy-Filter zu verwenden, welche die gefilmten Gesichter in Echtzeit verschlüsseln und dabei die Privatsphäre des Arbeitnehmers zu gewährleisten vermögen. Eine Videoüberwachung benötigt aber auch bei Einsatz von Privacy-Filtern einen Rechtfertigungsgrund.

Zur nötigen Transparenz

Auch muss die Videoüberwachung transparent sein, indem die Arbeitnehmenden über die Einrichtung der Videokameras informiert sein müssen. Die überwachten Bereiche sind mittels Hinweisschildern oder Piktogrammen auf Augenhöhe zu signalisieren.

Im Rahmen einer zeitlich beschränkten Videoüberwachung des Arbeitsplatzes ist es mit dem Persönlichkeitsschutz vereinbar, wenn die Angestellten nur über die ausgewählte Aufnahmeperiode informiert werden. Ausnahme von der Transparenzpflicht bildet nach Auffassung des Bundesgerichts die Überwachung bei bestehendem Deliktsverdacht, um den Erfolg der Überwachung nicht zu vereiteln.

Daten, die im Rahmen einer arbeitsrechtlich zulässigen Videoüberwachung gesammelt wurden, dürfen nur in Ausnahmefällen in Bezug auf den einzelnen Arbeitnehmer ausgewertet werden. Unzulässig wäre es demnach, wenn das Warenhaus mit Überwachungskameras, die den Dieb-

stahlschutz bezwecken, die Pausendauer des Personals überprüfen würde, während die Sichtung der Aufnahmen bei einer Häufung von Mitarbeiterdiebstählen vorgenommen werden dürfte.

Die Aufbewahrung der Aufnahmen ist zeitlich zu begrenzen. Es hängt vom jeweiligen Zweck der Überwachung ab, wie lange die Daten gespeichert werden dürfen. In der Regel hat die Löschung innert 24 bis 72 Stunden zu erfolgen.

Rechtliche Anforderungen an die Videoüberwachung am Arbeitsplatz

Bearbeitung von Personendaten durch den Arbeitgeber (Art. 3 DSGVO und Art. 328b OR)

Um Personendaten handelt es sich nach Art. 3 lit. a Datenschutzgesetz (DSG) bei Informationen immer dann, wenn sie sich auf eine bestimmte oder bestimmbar Person beziehen. Das Bearbeiten umfasst gemäss Art. 3 lit. e DSG jeden Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten.

In welcher Form?

Die Form der entsprechenden Informationen, beispielsweise als Zeichen, Wort, Bild, Ton oder deren Kombination, sowie die Beschaffenheit des Datenträgers sind dabei unerheblich, sofern sich die Angaben einer oder mehreren Personen zuordnen lassen.

Wann ist eine Person bestimmbar?

Die Bestimmtheit einer Person liegt dann vor, wenn aus der Information selbst ersichtlich ist, dass es sich genau um diese Person handelt. Bestimmbarkeit einer Person ist gegeben, wenn aufgrund zusätzlicher Informationen auf sie geschlossen werden kann, sofern die Identifizierung mit vertretbarem Aufwand möglich ist. Videoaufnahmen am Arbeitsplatz fallen bei gegebener Identifikationsmöglichkeit der Arbeitnehmenden damit ohne Weiteres unter das Datenschutzgesetz.

Für den Arbeitsvertrag erforderlich?

Gestützt auf die arbeitsrechtliche Spezialbestimmung zum DSG von Art. 328b Obligationenrecht (OR) darf der Arbeitgeber Daten über den Arbeitnehmer nur bearbeiten, soweit sie dessen Eignung für das Arbeitsverhältnis betreffen oder zur Durchführung des Arbeitsvertrags erforderlich sind. Diese Bestimmung setzt die Fürsorgepflicht des Arbeitgebers im Bereich der Datenbearbeitung um und darf als relativ zwingende Norm nicht zuungunsten des Arbeitnehmers abgeändert werden.

Erforderlich im Sinne von Art. 328b OR ist die Datenbearbeitung, wenn diese vom Arbeitgeber zur Erfüllung seiner gesetzlichen oder arbeitsvertraglichen Pflichten oder für den Vertragsvollzug benötigt werden.

PRAXISBEISPIEL



Von legitimen betrieblichen Interessen kann man ausgehen bei der Gewährleistung ungestörter betrieblicher Abläufe, der Qualitätssicherung, der Optimierung der Arbeitsorganisation und der Produktivität, beim Schutz betrieblicher Vermögenswerte, bei der Beweissicherung im Geschäftsverkehr mit Kunden, der Kontrolle der Arbeitsleistung und Weisungsbefolgung sowie beim Interesse an der Erfüllung vertraglicher und gesetzlicher Pflichten.

Überwachungs- und Kontrollsysteme am Arbeitsplatz (Art. 26 ArGV 3)

Nach Art. 26 Abs. 1 der Verordnung 3 zum Arbeitsgesetz (ArGV 3) dürfen Überwachungs- und Kontrollsysteme, die das Verhalten der Arbeitnehmer am Arbeitsplatz überwachen sollen, nicht eingesetzt werden.

Ausnahmen: Leistungs- und Sicherheitskontrollen

Dies gilt allerdings nicht für Leistungs- und Sicherheitskontrollen: Für diesen Zweck sind die Überwachungs- oder Kontrollsysteme aber so zu gestalten und anzuordnen, dass sie die Gesundheit und die Bewegungsfreiheit der Arbeitnehmer dadurch nicht beein-



trächtigen. Art. 26 ArGV 3 verbietet nach Auffassung des Bundesgerichts ein Überwachungssystem nur dann, wenn es allein oder vorwiegend bezweckt, das Verhalten der Arbeitnehmer an sich zu überwachen, während die Rechtslehre teilweise strengere Anforderungen aufstellt.

WICHTIGER HINWEIS



Generell kann festgehalten werden, dass die ständige und damit systematische Verhaltensüberwachung der Mitarbeitenden mit Überwachungs- und Kontrollsystemen nicht zulässig ist. Die Zulässigkeit ist hingegen zu bejahen, wenn die Videoüberwachung am Arbeitsplatz für andere Zwecke wie beispielsweise zur Leistungs- und Sicherheitskontrolle eingesetzt wird, sofern dadurch Gesundheit und Bewegungsfreiheit der Mitarbeiter nicht beeinträchtigt sind.

Rechtmässigkeit (Art. 4 Abs. 1 und 13 DSGVO)

Personendaten dürfen gemäss Art. 4 Abs. 1 DSGVO nur rechtmässig bearbeitet werden. Das Bearbeiten von Personendaten bedarf eines Rechtfertigungsgrunds, damit es nicht zu einer widerrechtlichen Persönlichkeitsverletzung kommt (Art. 13 Abs. 1 DSGVO).

Ein möglicher Rechtfertigungsgrund kann sich – wenigstens in Branchen, in denen Überwachungsverpflichtungen bestehen – bereits aus dem Arbeitsvertrag allein ergeben. In Branchen ohne Überwachungsverpflichtungen wird sich der Arbeitgeber regelmässig auf ein überwiegendes privates Interesse berufen können. Die Einwilligung des Arbeitnehmers muss somit nicht eingeholt werden und würde auch keine ausreichende Rechtfertigung darstellen (da die erforderliche Freiwilligkeit der Einwilligung im Arbeitsbereich als fraglich einzustufen ist).

Verhältnismässigkeit sowie Treu und Glauben (Art. 4 Abs. 2 DSGVO)

Videoaufnahmen am Arbeitsplatz haben gestützt auf Art. 4 Abs. 2 DSGVO dem datenschutzrechtlichen Verhält-

nismässigkeitsgrundsatz zu entsprechen und dürfen nur nach Treu und Glauben erfolgen. In Bezug auf die Auswertung der Aufnahmen bedeutet dies, dass nur diejenigen Auswertungen vorgenommen werden dürfen, welche für das Aufdecken von Missbräuchen geeignet sind, und dass der Arbeitgeber dabei diejenige Auswertungsform zu wählen hat, welche den mildesten Eingriff in die Persönlichkeitsrechte der Mitarbeiter darstellt.

Zweckbindung (Art. 4 Abs. 3 DSGVO)

Der Grundsatz der Zweckbindung nach Art. 4 Abs. 3 DSGVO verlangt, dass die Videoaufnahmen am Arbeitsplatz nur für diejenigen Zwecke verwendet werden dürfen, welche bei der Beschaffung den Mitarbeitern bekannt gegeben wurden. Diesem Grundsatz kommt der Arbeitgeber durch den Erlass eines Überwachungsreglements und durch die regelkonforme Datenbearbeitung nach.

Transparenz (Art. 4 Abs. 4 DSGVO)

Die Überwachung und deren Zweck müssen für die Arbeitnehmer nach Art. 4 Abs. 4 DSGVO erkennbar sein, sodass der Arbeitgeber sie vorgängig über Art, Umfang und Zweck der Überwachung zu informieren hat, sei dies mittels Mitarbeiterhandbuch oder Nutzungsreglement. Die Informationspflicht der Mitarbeiter ergibt sich zusätzlich auch aus dem Erkennbarkeitsgebot.

Arbeitnehmerrechte (Betroffenenrechte)

Die betroffenen Mitarbeiter haben in Anwendung des Auskunftsrechts nach Art. 8 DSGVO das Recht, vom Arbeitgeber Auskunft darüber zu verlangen, ob bzw. welche Daten über sie in welcher Form bearbeitet werden.

GERICHTSENTSCHEIDE



Gemäss bundesgerichtlich bestätigten Entscheiden aus dem Kanton Zürich ist der Arbeitnehmer zur fristlosen Kündigung berechtigt, wenn er durch den Arbeitgeber in unzulässiger Weise mittels Videokameras überwacht wird.

Daneben ist der Arbeitnehmer auch durch Art. 179^{quater} StGB (Verletzung des Geheim- oder Privatbereichs durch Aufnahmegeräte) geschützt, da nach Auffassung des Bundesgerichts der nicht öffentlich zugängliche Arbeitsplatz zur Privatsphäre gehört. Dementsprechend kann der betroffene Mitarbeiter strafrechtliche Ansprüche gegenüber den Verantwortlichen geltend machen.

WICHTIGER HINWEIS



Mitarbeiter, die sich in ihrer Persönlichkeit verletzt fühlen, haben – gestützt auf Art. 15 DSGVO in Verbindung mit Art. 28 ZGB (Persönlichkeitsverletzung) – die Möglichkeit, gegen den Arbeitgeber eine Zivilklage zu erheben. Ein betroffener Mitarbeiter kann überdies verlangen, dass die Datenbearbeitung gesperrt wird, keine Daten an Dritte bekannt gegeben oder die Personendaten berichtigt oder vernichtet werden (Art. 15 Abs. 1 DSGVO).

Ein betroffener Mitarbeitender kann ausserdem über das Arbeitsinspektorat des Kantons seines Arbeitsorts die Verletzung von Art. 26 ArGV 3 geltend machen, wenn er beispielsweise seine Gesundheit als gefährdet einstuft, weil er an seinem Arbeitsplatz videoüberwacht wird.

Reputationsrisiko für Unternehmen

Auch wenn Datenschutzverstösse nur selten gerichtlich durchgesetzt werden, finden sie dennoch regelmässig ein breites mediales Echo. Dies hat zur Folge, dass sich Unternehmen nicht nur mit allfälligen rechtlichen Sanktionen auseinandersetzen müssen, sondern – abgesehen von den bereits genannten rechtlichen Anforderungen an die Zulässigkeit – unbedingt auch mögliche Reputationsverluste in den Entscheid zur Einführung einer Videoüberwachung am Arbeitsplatz einbeziehen sollten.

AUTOR



Dr. iur. Reto Fanger ist Rechtsanwalt (ADVOKATUR FANGER – Anwaltsboutique für ICT-, Daten-, Medien- & Arbeitsrecht, Luzern; www.advokatur-fanger.ch), Dozent an der Hochschule Luzern und Mitorganisator des Lucerne Law & IT Summit (LITS) der Uni Luzern.