Rechtmäßigkeit der Videoüberwachung und grundsätzliches Verbot der Verknüpfung mit Gesichtserkennung

Zusammenfassung: Videoüberwachung stellt immer einen erheblichen Eingriff in die Rechte und Freiheiten natürlicher Personen dar. Weitere rechtmäßige Zwecke der Videoüberwachung wie die Gefahrenabwehr Sachbeschädigung bei Fremdeigentum oder bei Übergriffen auf Personen sowie die mögliche Beweissicherung durch Aufzeichnung werden besprochen. Die Betrachtung abstrakter Fälle reicht nicht für die Beurteilung aus, es ist konkret auf den Einzelfall abzustellen. Die Verknüpfung von biometrischen Merkmalen mit Videoüberwachung ist grundsätzlich nicht erlaubt.

Der Praxisfall: Der Betreiber einer Diskothek plant einen zweiten Eingang für „VIPs“ einzurichten. Dazu soll eine Videoüberwachung mit Gesichtserkennung gekoppelt werden, damit die besonderen Gäste und Mitglieder des Clubs, eben die VIPs, nicht in der allgemeinen Warteschlange ausharren müssen. Für die Zusammenführung der Daten aus der Videoüberwachung mit den biometrischen Daten der betroffenen Personen benötigt er die Zustimmung von allen Betroffenen. Das ist jedoch schwierig, da sich über den zweiten Eingang auch Unbefugte den rascheren Eintritt verschaffen möchten, deren Einverständnis in die Koppelung der Videoüberwachung mit biometrischen Daten nicht vorliegt. Eine entsprechende Kennzeichnung ist die mindeste Voraussetzung, weiter Prüfungen sind vorzunehmen.

Videoüberwachung sorgfältig planen: In den vorangegangenen Ausgaben der Praxistipps Datenschutz wurden in der Ausgabe *03 2018 Videoüberwachung und DSGVO* sowie *Praxistipp Datenschutz 04 2018 Erlaubte Zwecke für Videoüberwachung nach DSGVO* schon darauf eingegangen, wie sorgfältig die einzelnen Schritte der Videoüberwachung geplant werden sollten, wenn man nicht Gefahr laufen möchte, dass eine bußgeldbewehrte Verletzung der Datenschutzvorschriften nach DSGVO vorliegt. Mehrere oberste Gerichte (BAG, BGH, BVerfG) haben übereinstimmend geurteilt, dass Videoüberwachung eine erhebliche Beeinträchtigung der Rechte und Freiheiten natürlicher Personen darstellt, weil sich Menschen im Wirkungskreis einer Videoüberwachung anders verhalten als sonst. Alleine diese Verhaltensänderung ist eine Einschränkung der persönlichen Freiheit, die nur geduldet werden kann, wenn andere Rechtsgüter nur mit der Videoüberwachung geschützt werden können. Daher ist dieser Eingriff in die Privatsphäre sehr sorgfältig zu planen, zu begründen, durchzuführen und zu kontrollieren.

Gefahrenabwehr Sachbeschädigung bei Fremdeigentum: Immer wieder kommt es vor, dass Eigentum von Dritten, beispielsweise Fahrzeuge von Kunden oder Beschäftigten, auf dem Gelände des Unternehmens beschädigt wird. Ob es sich dabei um beabsichtigte oder nicht beabsichtigte Beschädigungen handelt, ist für die Eigentümer und für das Unternehmen einerlei. Alle Beteiligten möchten Hinweise, mit deren Hilfe sie die Verursacher zur Verantwortung ziehen können, damit der Schaden beglichen wird. Hier ist Videoüberwachung ein beliebtes Instrument. Da in diesem Fall die berechtigten Interessen Dritter geschützt werden, kann es sich dabei durchaus um eine mögliche Bedingung für die Rechtmäßigkeit der Verarbeitung personenbezogener Daten nach Art. 6 Abs. 1 Buchstabe f DSGVO handeln.

Erleichterte Aufklärung von Sachbeschädigungen: Auch hier ist es wichtig zu unterscheiden zwischen Verhindern der Sachbeschädigung (was durch Videoüberwachung nicht gelingen kann) oder durch Verringern der Wahrscheinlichkeit, mit der die absichtliche Sachbeschädigung vorgenommen wird und der erleichterten Aufklärung einer Sachbeschädigung durch die Auswertung der Daten der Videoüberwachung. Das muss in der Zweckbestimmung auch deutlich zum Ausdruck kommen.

Gefahrenabwehr Übergriffe auf Personen: Gleiches gilt für die Gefahrenabwehr bezüglich der Übergriffe auf Personen. Vor allem in nicht-öffentlichen Bereichen, die für

ein breites Publikum auch zu Zeiten erreichbar sind, in denen keine normaler Geschäftsbetrieb mehr erfolgt, also Gastronomie, Kino, Tanzveranstaltungen usw., aber auch im öffentlichen Nahverkehr bei Straßenbahnen und Bussen, kann es immer wieder zu Verletzungen von Personen kommen. Auch hier ist zunächst unerheblich, ob es sich dabei um absichtliche Übergriffe handelt oder um unbeabsichtigte, beispielsweise bei einem Unfall in einer Straßenbahn, die scharf bremsen muss, und bei dem ein Fahrgast auf einen anderen geschleudert wird und diesen verletzt. Speziell für die Übergriffe gilt das schon mehrfach gesagte, dass sie mit einer Videoüberwachung kaum verhindert werden können, möglicherweise sich jedoch Gelegenheitstäter durch die Videoüberwachung von der Tat abhalten lassen.

Nachträgliche Beweissicherung durch Aufzeichnung: Hierbei dürfte es sich um die am häufigsten eingesetzte stichhaltige Begründung für Videoüberwachung handeln. Wie oft kommt es vor, dass im Nachhinein erst festgestellt wird, dass eine unrechtmäßige Handlung begangen wurde oder auch eine unbeabsichtigte Handlung negative Folgen hatte, und wir froh wäre man oft gewesen, sich das alles noch einmal genau ansehen zu können! Hier kann die Aufzeichnung des Geschehenen oftmals zu einer Aufklärung des genauen Hergangs beitragen, und wie oft konnten Mitarbeiter, die unberechtigt verdächtigt wurden, eine bestimmte Handlung begangen zu haben, durch derartige Aufzeichnungen schon entlastet werden!

Prüf- und Kontrollsystem einrichten: Wichtig ist hierbei aber auch, ein Prüf- und Kontrollsystem einzurichten, das außergewöhnliche Aktivitäten rechtzeitig erkennt, so dass eine zu frühe Löschung der Daten vermieden werden kann. Wenn die Daten nach einem konkreten Verdacht oder nach einer konkreten Erfordernis separiert und damit nicht im normalen Löschprozess gelöscht werden, ist dies eine erlaubte verlängerte Aufbewahrung gegenüber den ansonsten sehr strengen Löschvorgaben seitens der Aufsichtsbehörden (hierauf wird in der Folge noch näher eingegangen).

Unterstützung für logistische Abwicklung: Dies ist zwar thematisch ein Sonderfall der Videoüberwachung, kommt aber in den letzten Monaten und Jahren immer häufiger vor. Zum einen geht es tatsächlich um die Unterstützung logistischer Abläufe, sei es, dass an Einfahrtsschranken oder an Besuchereingängen Videokameras angebracht sind um zu erkennen, wer da gerade Einlass begehrt. Zum anderen können einfahrende Fahrzeuge besser an freie Plätze dirigiert werden, wenn an zentraler Stelle eine entsprechende Übersicht möglich ist.

Produktionsabläufe überwachen: Dann gibt es da noch den Fall, dass Produktionslogistik betroffen ist, also entweder mittels Kameras überwacht wird, wie die Produktionsabläufe gerade funktionieren bzw. wo gegebenenfalls Störungen zu verzeichnen sind. In diese Kategorie gehört beispielsweise auch die Beweisfindung, wer eine Schranke eines Zufahrtkontrollsystems weggefahren hat. Bei dieser Art der Videoüberwachung ist sehr genau zu prüfen, wie lange die Aufzeichnungen tatsächlich benötigt werden. Es ist niemandem damit gedient, wenn Videoaufzeichnungen, die eigentlich zu Beweiszwecken angefertigt wurden, schon gelöscht sind, bevor der zu kontrollierende Vorfall entdeckt wurde.

Verknüpfung mit Gesichtserkennung grundsätzlich untersagt: Weil die Technik es ermöglicht, wird immer öfter eine Videokamera auch dazu genutzt, eine Person über die so genannten Gesichtserkennung eindeutig zu identifizieren. Dabei werden biometrische Daten verarbeitet. Die DSGVO definiert „biometrische Daten“ (als) mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten“ (Art. 4 Abs. 1 Nummer 14 DSGVO). Nach Art. 9 Abs. 1 DSGVO ist die Verarbeitung biometrischer Daten zur eindeutigen Identifizierung einer natürlichen Person grundsätzlich untersagt.

Videoüberwachung mit Gesichtserkennung in wenigen Ausnahmen möglich: Allerdings gibt es einige wenige im Gesetz (Art. 9 Abs. 2 DSGVO) erlaubte Verarbeitungen von biometrischen Daten, also vom Einsatz der Gesichtserkennung im Zusammenhang mit Daten aus der Videoüberwachung. Die wichtigste Ausnahme steht dort

in Abs. 1 Buchstabe a). Demnach ist diese Art der Verarbeitung dann erlaubt, wenn die betroffene Person in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt hat und die Zwecke, für die die Gesichtserkennung eingesetzt werden sollen, sind nach Unionsrecht oder nationalem Recht auch dahingehend untersagt, dass selbst bei Vorliegen einer Einwilligung diese Daten nicht verarbeitet und genutzt werde dürfen. Es bleibt daher abzuwarten, ob und wie die europäische oder nationale Gesetzgebung solche Regelungen trifft, dass selbst eine Einwilligung in die Verarbeitung dieser Daten unwirksam ist. Derzeit sind derartige Regelungen noch nicht bekannt.

Erläuterungen zum Praxisfall: Bei dem geplanten Vorhaben des Betreibers der Diskothek kommen gleich mehrere kritische Aspekte zum Vorschein. Zunächst ist zu prüfen, ob die vorgesehenen Zwecke nicht auch ohne die Videokameras erreicht werden können. Aber selbst wenn das so wäre, muss zunächst die Frage der Rechtmäßigkeit der Maßnahme gestellt werden. Handelt es sich um ein berechtigtes Interesse des Verantwortlichen? Da die Schaffung eines zweiten Eingangs für Mitglieder keinen Verstoß gegen geltendes Recht darstellt, kann das angenommen werden. Ob der Einsatz der Kameras zur Identifikation der Berechtigten erforderlich ist, kann eher verneint werden. Denn ein zweiter Eingang ohne dort aufgestelltes Personal ist nicht geplant, die Videoüberwachung ist als Unterstützung gedacht, außerdem sollen die Berechtigten auf besondere Weise begrüßt werden. Aber auch dieses Ansinnen kann auf andere Weise erreicht werden, beispielsweise durch den Einsatz eines Ausweises oder einer eindeutigen Markierung, die nur Mitglieder haben. So wurde am Ende des Prüfprozesses auf den Einsatz der Kameras verzichtet.

Eberhard Häcker, Ensdorf

Der Autor Eberhard Häcker ist Geschäftsführer der TDSSG GmbH – Team Datenschutz Services – und seit vielen Jahren als Externer Datenschutzbeauftragter und Datenschutzberater tätig. Seine Fachaufsätze erscheinen regelmäßig in unterschiedlichen Publikationen. Außerdem ist er Geschäftsführer der HäckerSoft GmbH, die unter anderem mit der Datenschutzsoftware DATSIS und der Lernplattform Optilearn (Pflichtschulungen für Datenschutzbeauftragte) am Markt aktiv ist. Sein Lieblingsprojekt ist datenschutzkabarett.de.