

Sebastian Meyer

Von der Videoüberwachung zur automatisierten Videoanalyse

Die technische Entwicklung der Videoanalyse lässt immer neue Nutzungsmöglichkeiten zu, die über eine bloße Überwachung von bestimmten Bereichen hinausgehen. Teilweise sind die neuen Möglichkeiten im Sinne des Betroffenen, wenn er sich bewusst hierfür entscheidet. Ohne aktive Einwilligung müssen die technischen Möglichkeiten aber gegen die Beeinträchtigungen der Rechte des Betroffenen abgewogen werden. Am Beispiel der Rechtslage in Deutschland werden einige neue Nutzungsmöglichkeiten bewertet.

Collection: Conference Proceedings IRIS 2015

Category: Articles

Field of law: Data Protection

Region: Germany

Citation: Sebastian Meyer, Von der Videoüberwachung zur automatisierten Videoanalyse, in: Jusletter IT 26. Februar 2015 – IRIS

Inhaltsübersicht

- 1 Einleitung
- 2 Rechtliche Ausgangslage in Deutschland
 - 2.1 Videoüberwachung im öffentlichen Raum
 - 2.2 Videoüberwachung außerhalb des privaten Raumes
 - 2.3 Ablauf der Interessenabwägung
- 3 Technische Möglichkeiten der Videoüberwachung
 - 3.1 Kameraattrappen
 - 3.2 Kameras ohne Aufzeichnung
 - 3.3 Kameras mit Aufzeichnung
 - 3.4 Kameras mit Auswertung
 - 3.4.1 Videoanalyse als automatisierte Einzelfallentscheidung
 - 3.4.2 Thinking Camera als Standardbeispiel
- 4 Case Studies
 - 4.1 Videoanalyse zur Verkaufsförderung
 - 4.1.1 Blickverlaufsanalyse
 - 4.1.2 Videoanalyse der Kundenströme
 - 4.2 Videoanalyse zu Abrechnungszwecken
 - 4.2.1 Optionales Angebot statt zwingende Nutzung
 - 4.2.2 Speicherung der Daten und Zugriff auf die Daten
- 5 Literatur

1 Einleitung

[Rz 1] Seit Jahren nimmt die Zahl der Videokameras, die von öffentlichen Stellen, Unternehmen und Privatpersonen installiert werden, beständig zu.¹ Gleichzeitig bieten technische Weiterentwicklungen immer neue und bessere Einsatzmöglichkeiten. Aus Sicht des Betroffenen erhöht sich die Eingriffsintensität hierdurch immer weiter. Zum einen muss der Betroffene befürchten, dass er aufgrund der steigenden Zahl von Videokameras häufiger in den Erfassungsbereich gerät, zum anderen ist für den Betroffenen weniger erkennbar, wie und wofür die Daten verwendet werden. Wie immer bei technischen Neuerungen ist sorgsam abzuwägen, ob das, was technisch möglich ist, auch rechtlich eingesetzt werden darf. Die Abwägung muss dabei die Interessen der verantwortlichen Stelle für die Videoüberwachung berücksichtigen und diese in ein Verhältnis zu den schutzwürdigen Interessen der Betroffenen setzen. Je nach Anwendungsbereich und technischer Ausgestaltung fällt die Interessenabwägung zugunsten der verantwortlichen Stelle oder des Betroffenen aus. Auch außerhalb des Datenschutzes — also etwa bei einem fehlenden Personenbezug — sind das Allgemeine Persönlichkeitsrecht und das Recht auf informationelle Selbstbestimmung des Betroffenen gegenüber den Interessen der Stelle abzuwägen, von der die Videoüberwachung ausgeht.

2 Rechtliche Ausgangslage in Deutschland

[Rz 2] In Deutschland finden sich Regelungen für die Videoüberwachung im Bundesdatenschutzgesetz (BDSG) unter dem Stichwort «Beobachtung öffentlich zugänglicher Räume mit opto-elektronischen

¹ Vgl. Deutscher Bundestag, Drucksache 17/13071 vom 16. April 2013, wonach in London statisch jeder Bewohner pro Tag 300 Mal von einer Videokamera erfasst wird.

Einrichtungen».² Schon aus dem Wortlaut der Regelung ist ersichtlich, dass es für ihre Anwendbarkeit darauf ankommt, ob der überwachte Bereich öffentlich zugänglich ist.³ Öffentlich zugänglich in diesem Sinne ist ein Bereich dann, wenn eine Widmung für den öffentlichen Verkehr gegeben ist oder nach dem erkennbaren Willen des Berechtigten eine Nutzung für die Öffentlichkeit vorgesehen ist.⁴ Auf eine Umzäunung oder Abgrenzung kommt es hierfür nicht an, auch Flächen in privatem Eigentum können in diesem Sinne öffentlich sein.⁵

[Rz 3] Basierend auf dieser Abgrenzung sind Ladenlokale beispielsweise als öffentlich zugänglicher Bereich anzusehen, ein Firmengelände dagegen nicht.⁶ Soweit ein Gelände nur für einen bestimmten Personenkreis zugänglich sein soll, ist das Kriterium der Öffentlichkeit ebenfalls nicht mehr erfüllt. Dies gilt etwa für alle Bereiche, zu deren Betreten eine Eintrittskarte erworben werden muss und schon eine Vertragsbeziehung (Mitgliedschaft) erforderlich ist.⁷ Unabhängig davon, ob es für solche Bereiche eine echte Eingangskontrolle gibt, ist das Gelände dann nicht zum Zugang für die Öffentlichkeit gedacht, sondern allenfalls für Mitarbeiter und Geschäftspartner.

[Rz 4] Für den nicht-öffentlichen Bereich kann anders als in Österreich nicht auf eigene gesetzliche Bestimmungen zur Videoüberwachung zurückgegriffen werden. Es ist insoweit anerkannt, dass die gesetzliche Regelung auch nicht analog auf andere Bereiche übertragen werden kann, da sie ausdrücklich nur für den öffentlichen Bereich geschaffen wurde.⁸ Stattdessen ist auf die allgemeinen Generalklauseln abzustellen, die für jede Form der Verarbeitung personenbezogener Daten gelten.

2.1 Videoüberwachung im öffentlichen Raum

[Rz 5] Erfolgt die Videoüberwachung nach der vorstehenden Abgrenzung im öffentlichen Raum muss in Deutschland zunächst ein berechtigter Grund für die Videoüberwachung vorliegen.⁹ Die abschließende Aufzählung nennt insoweit die Aufgabenerfüllung öffentlicher Stellen, die Wahrnehmung des Hausrechts und die Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke.¹⁰ Im nächsten Schritt muss eine Interessenabwägung erfolgen. In diesem Rahmen dürfen sich keine Anhaltspunkte dafür ergeben, dass berechtigte Interessen des Betroffenen überwiegen.¹¹

[Rz 6] Schließlich ist definiert, dass eine Videoüberwachung nur mit Kenntlichmachung und Angabe der verantwortlichen Stelle zulässig ist.¹² Hierfür wird in Deutschland üblicherweise

² HORNING/DESOL, K&R 2011, 153, 157.

³ Die Abgrenzung bei der Videoüberwachung zwischen öffentlichem und nicht-öffentlichem Raum ist dem österreichischen Datenschutzrecht fremd, da von § 50a DSG 2000 beide Bereiche gleichermaßen erfasst werden.

⁴ GOLA/SCHOMERUS, §6b Rn. 8.

⁵ SCHOLZ in Simitis, § 6b Rn. 43.

⁶ GOLA/SCHOMERUS, §6b Rn. 8.

⁷ SCHOLZ in Simitis, § 6b Rn 45.

⁸ PÖTTERS/TRAUT, RDV 2013, 132, 133.

⁹ Vgl. § 6b Abs. 1 BDSG; in Österreich stellt § 50a Abs. 2 DSG 2000 ausdrücklich auch auf rechtmäßige Zwecke der Videoüberwachung ab.

¹⁰ GOLA/SCHOMERUS, § 6b Rn. 14.

¹¹ In Österreich ist gem. § 7 Abs. 2 Nr. 3 DSG 2000 ebenfalls eine Prüfung erforderlich, ob schutzwürdige Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.

¹² Das Transparenzerfordernis ergibt sich aus § 6b Abs. 2 BDSG bzw. § 50d Abs. 1 DSG 2000.

ein standardisiertes Piktogramm verwendet.¹³ Inwieweit auf besondere Umstände bei der Videoüberwachung, etwa eine automatisierte Auswertung, extra hingewiesen werden muss, ist in diesem Zusammenhang noch nicht abschließend geklärt.¹⁴ Aus Transparenzgründen ist eine entsprechende Forderung im Interesse der Betroffenen aber zu befürworten. Eine Meldepflicht für Maßnahmen der Videoüberwachung existiert in Deutschland nicht.¹⁵

2.2 Videoüberwachung außerhalb des privaten Raumes

[Rz 7] Kommt die spezialgesetzliche Regelung gem. § 6b BDSG nicht zur Anwendung, so sind die allgemeinen Ermächtigungsgrundlagen zu prüfen, insbesondere die Datenerhebung für eigene Geschäftszwecke gem. § 28 BDSG. Zulässig ist danach eine Datenverarbeitung im Rahmen der Vertragserfüllung, zur Wahrung berechtigter Interessen und bei Nutzung allgemein zugänglicher Informationen. Die erste und dritte Alternative kommen bei der Videoüberwachung regelmäßig nicht in Betracht, üblicherweise ist auf die Wahrung berechtigter Interessen abzustellen. Dort ist — wie bei der Regelung zur Videoüberwachung im öffentlichen Raum — eine Prüfung vorgesehen, ob berechnigte Interessen des Betroffenen nicht überwiegen. Der Abwägungsmaßstab und der Abwägungsvorgang sind damit in beiden Konstellationen letztlich identisch.¹⁶

2.3 Ablauf der Interessenabwägung

[Rz 8] Es bietet sich an, sich im Rahmen der Interessenabwägung bei der Videoüberwachung an der allgemeinen Prüfung der Verhältnismäßigkeit einer Maßnahme zu orientieren. Demnach muss zunächst überhaupt ein legitimer Zweck vorliegen. Sodann ist auf die Geeignetheit, Erforderlichkeit und Angemessenheit einzugehen. Als legitimer Zweck genügt jeder im Gesetz vorgesehene Zweck, also die Wahrnehmung des Hausrechts oder die Wahrung berechtigter eigener Interessen. In der Literatur wird jedoch verlangt, dass der Zweck möglichst präzise definiert wird und nicht auf allgemeine Beschreibungen wie «Gefahrenabwehr» zurückgegriffen wird.¹⁷ Im nächsten Schritt ist sodann die Geeignetheit zu prüfen. Diese liegt vor, wenn die vorgesehene Maßnahme zur Erreichung des definierten Zwecks grundsätzlich tauglich ist. Demnach wäre der Einsatz von Videokameras ungeeignet, wenn eine Kontrolle vor allem nachts erfolgen soll, die Kamera aber nicht über eine ausreichende Lichtempfindlichkeit verfügt oder ohne Infrarotlicht nicht funktionsfähig ist.¹⁸

[Rz 9] Von einer Erforderlichkeit ist auszugehen, wenn kein milderes Mittel gleich geeignet ist um den angestrebten Zweck zu erreichen.¹⁹ An dieser Stelle ist beispielsweise zu diskutieren, ob

¹³ BECKER in Plath, § 6b Rn. 27.

¹⁴ HORNING/DESOL, K&R 2011, 153, 157.

¹⁵ Mangels Meldepflicht und Registrierung ähnlich § 50c DSGVO 2000 ist Information der Aufsichtsbehörden in Deutschland generell nicht vorgesehen, so dass diese nur auf Beschwerden hin tätig werden können.

¹⁶ Auch die Wahrnehmung des Hausrechts, die in § 6b BDSG explizit als Sonderfall erwähnt ist, dürfte als Unterfall der Wahrung berechtigter Interessen anzusehen sein; vgl. dazu auch SCHOLZ in Simitis, § 6b Rn. 77.

¹⁷ SCHOLZ in Simitis, § 6b Rn. 82.

¹⁸ SCHOLZ in Simitis, § 6b Rn. 87, wobei diese Kriterien unter dem Stichwort der Erforderlichkeit besprochen werden.

¹⁹ BECKER in Plath, § 6b Rn. 20; SIMITIS, § 28 Rn. 108. In Österreich ist das Gebot, immer mit den «gelindesten zur Verfügung stehenden Mitteln» zu arbeiten, ausdrücklich durch § 7 Abs. 3 DSGVO 2000 im Datenschutzrecht geregelt.

bei der Kriminalitätsbekämpfung nicht auch anderen Maßnahmen wie eine bessere Beleuchtung in Betracht kommen. Bei der Erforderlichkeit sind aber auch Kostenaspekte für die verantwortliche Stelle zu berücksichtigen. Häufigere Kontrollgänge können zwar möglicherweise zumindest ähnlich geeignet sein, wegen der damit verbundenen Kosten kann dies aber regelmäßig nicht verlangt werden.²⁰ Im Rahmen der Erforderlichkeit wird bei der Videoüberwachung teilweise auch bereits erörtert, inwieweit es notwendig ist, Videokameras mit Zoom- und Schwenkfunktionen auszustatten.²¹

[Rz 10] Die eigentliche Interessenabwägung erfolgt schließlich unter dem Stichwort der Angemessenheit.²² Es werden sowohl die Interessen der verantwortlichen Stelle als auch die Interesse des Betroffenen gegeneinander abgewogen.

[Rz 11] Dieses Schema kann für jede datenschutzrechtliche Prüfung der Verhältnismäßigkeit bei dem Einsatz von Systemen zur Videoüberwachung angewendet werden. Mit Blick auf das konkrete System ist aber immer zu berücksichtigen, wie technisch fortgeschritten das jeweilige System ist und ob sich hierdurch für die Betroffenen eine stärkere Beeinträchtigung ergibt als bei anderen Techniken zur Videoüberwachung.

3 Technische Möglichkeiten der Videoüberwachung

3.1 Kameraattrappen

[Rz 12] Aus Sicht des Betroffenen ist die Nutzung von Kameraattrappen vermutlich das mildeste Mittel, da tatsächlich keinerlei Aufnahmen angefertigt und übermittelt werden. Wenn es der verantwortlichen Stelle ausschließlich darum geht, ein Sicherheitsgefühl zu vermitteln oder eine abschreckende Wirkung zu erreichen, können entsprechende Attrappen unter Umständen ausreichen. Typischerweise dient die Videoüberwachung aber nicht nur der Abschreckung, sondern es sollen beispielsweise auch bereits begangene Straftaten aufgeklärt werden. In solchen Fällen ist die Nutzung einer Kameraattrappe ungeeignet. Außerdem muss in Erwägung gezogen werden, dass die Nutzung von Kameraattrappen zu einem falschen Sicherheitsgefühl führt und eine Erwartungshaltung der Betroffenen begründen kann. So hat ein Autofahrer, dem Wertgegenstände in einem Parkhaus aus dem Wagen gestohlen wurden, argumentiert, wegen der angebrachten Videokameras sei er von einem bewachten Parkplatz und besonderen Bewachungspflichten des Betreibers ausgegangen.²³

[Rz 13] Rechtlich ist weitgehend unbestritten, dass Kameraattrappen in Deutschland nicht den Anwendungsbereich von § 6b BDSG fallen, da es sich objektiv nicht um optisch-elektronische Einrichtungen im Sinne der Definition handelt. Es bleibt allerdings die Möglichkeit eines Eingriffs in das Allgemeine Persönlichkeitsrecht, das bereits bei der Installation von Attrappen berührt ist.²⁴ Die Betroffenen fühlen sich auch bei einer vermeintlichen Überwachung kontrolliert, was als Eingriff ausreicht.²⁵ Wegen des beschränkten Nutzens und der bestehenden Risiken sollte

²⁰ AG Hamburg, CR 2009, 129.

²¹ SCHOLZ in Simitis, § 6b Rn. 90.

²² SCHOLZ in Simitis, § 6b Rn. 92.

²³ AG Hannover, NJW-RR 2009, 96.

²⁴ KIRSCH, MMR-Aktuell 2011, 317919; vgl. für Österreich OGH, Urt. v. 14. Mai 1997, 7 Ob 89/97g.

²⁵ BECKER in Plath, § 6b Rn 13; vgl. auch OGH, Urt. v. 28. März 2007, 6 Ob 6/06k.

auf eine ausschließliche Nutzung von Kameraattrappen regelmäßig verzichtet werden.

3.2 Kameras ohne Aufzeichnung

[Rz 14] Eine vergleichsweise geringe Eingriffsintensität weisen Systeme auf, bei denen ausschließlich die Möglichkeit besteht, die aktuellen Bilder der Videokameras wiederzugeben.²⁶ Für die verantwortliche Stelle genügt diese Art der Videoüberwachung dann, wenn ausschließlich präventive Zwecke im Vordergrund stehen.²⁷ Eine nachträgliche Auswertung der Aufnahmen ist nicht möglich, so dass weitere denkbare Nutzungsarten ausscheiden.

[Rz 15] Die Eingriffsintensität aus Sicht des Betroffenen ist zwar höher als bei einer direkten Beobachtung, aber nicht so hoch wie bei einer Aufzeichnung der Aufnahmen. Gegenüber einer direkten Beobachtung durch Mitarbeiter der verantwortlichen Stelle oder Ladendetektive ist die Eingriffsintensität höher, weil der Betroffene nicht erkennen kann, wann er tatsächlich beobachtet wird. Außerdem muss der Betroffene bei einer Übertragung des Live-Bildes befürchten, dass durch mehrere Personen ein Zugriff auf die Bilder möglich ist. Dies führt letztlich dazu, dass die Anforderungen an eine Videoüberwachung ohne Aufzeichnung relativ gering sind, aber gleichwohl nicht von einer grundsätzlichen Zulässigkeit ausgegangen werden kann.

[Rz 16] Wichtig ist vor allem eine sorgfältige Auswahl der überwachten Bereiche, da auch ohne Aufzeichnungsfunktion eine lückenlose Erfassung aller Flächen nicht erforderlich ist und damit auch nicht gerechtfertigt werden kann.²⁸ Erst recht unzulässig ist regelmäßig eine Videoüberwachung, die über die eigenen Grundstücksgrenzen in den öffentlichen Raum hinausgeht.

3.3 Kameras mit Aufzeichnung

[Rz 17] Sobald die Videoüberwachung neben präventiven Zwecken auch noch für weitere Zwecke eingesetzt werden soll, ist regelmäßig eine zeitliche befristete Aufzeichnung der Aufnahmen erforderlich. Auf diese Weise ist es möglich, nachträglich die Aufnahmen zu sichten und nach bestimmten Ereignissen zu suchen. Die Aufzeichnung ermöglicht eine viel weitergehende Überwachung als bei der bloßen Übertragung von Live-Bildern. Der Betroffene muss damit rechnen, dass die Aufnahmen später unter bestimmten Gesichtspunkten betrachtet und bewertet werden, was ohne Aufzeichnung nicht möglich wäre. Durch die Aufzeichnungen werden flüchtige Beobachtungen zu dauerhaften Beweisen. Der Betroffene ist dadurch dem Risiko ausgesetzt, dass die Aufnahmen gegen ihn über einen längeren Zeitraum verwendet werden können.

[Rz 18] Vor diesem Hintergrund ist im Rahmen der Abwägung zu verlangen, dass gerade für den Zugriff auf gespeicherte Aufnahmen klare Vorgaben existieren. Es muss ausgeschlossen sein, dass die Aufzeichnungen später ohne Vorgaben und ohne Kontrolle ausgewertet werden. Ein Zugriff auf die gespeicherten Informationen soll idealerweise nur möglich sein, wenn hierfür ein konkreter Anlass besteht und dies auch einer Kontrolle unterliegt.

[Rz 19] Weiter wird verlangt, dass die Aufzeichnungen nur so lange gespeichert bleiben dürfen,

²⁶ Vor diesem Hintergrund sind derartige Systeme nach österreichischem Recht als «Echtzeitüberwachung» besonders privilegiert, vgl. etwa §§ 50a Abs. 4 Nr. 3, 51c Abs. 2 Nr. 1 DSGVO 2000.

²⁷ SCHOLZ in Simitis, § 6b Rn. 90.

²⁸ SCHOLZ in Simitis, § 6b Rn. 90.

bis ersichtlich ist, ob die Aufzeichnungen noch benötigt werden.²⁹ Dabei ist nicht ausgeschlossen, dass bestimmte Sequenzen, die später noch benötigt werden, im Rahmen der Auswertungen für einen längeren Zeitraum gespeichert bleiben. Ohne Anlass müssen die Aufzeichnungen innerhalb definierter Zeiträume gelöscht werden. Der Zeitraum ist dabei davon abhängig, wann typischerweise der Zweck der Aufzeichnungen entfällt. Soll etwa eine Videoüberwachung vor Beschädigungen und Diebstahl außerhalb der Öffnungszeiten schützen, kann regelmäßig kurz nach Fortsetzung des Geschäftsbetriebs eine Prüfung erfolgen, ob es zuvor zu besonderen Vorkommnissen gekommen ist. War dies nicht der Fall, können die Aufzeichnungen binnen weniger Tage gelöscht werden.³⁰

3.4 Kameras mit Auswertung

[Rz 20] Bei der klassischen Videoüberwachung erfolgt die Auswertung der Aufnahmen manuell. Soweit nur Live-Bilder übertragen werden, müssen die Mitarbeiter der verantwortlichen Stelle diese im Blick behalten und direkt entsprechend reagieren. Wenn eine Aufnahmefunktion verfügbar ist, können die Aufnahmen auch nachträglich ausgewertet werden. Die Auswertung erfolgt typischerweise wieder manuell, indem ein Mitarbeiter die Aufzeichnungen durchsieht und bestimmte Sequenzen sichert.

3.4.1 Videoanalyse als automatisierte Einzelfallentscheidung

[Rz 21] Durch die gestiegenen technischen Möglichkeiten ist es denkbar, dass die Auswertung weitgehend automatisiert erfolgt. Auf der einen Seite ist die Eingriffsintensität reduziert, weil Mitarbeiter der verantwortlichen Stelle keinen Einblick mehr in die Aufzeichnungen nehmen müssen. Auf der anderen Seite entscheidet dafür jetzt aber ein System über die Konsequenzen, die aus der Videoüberwachung gezogen werden. Der Betroffene muss sich damit der Entscheidung eines Systems unterwerfen, auf das er keinen Einfluss hat.³¹ Vor diesem Hintergrund ist im deutschen Datenschutzrecht geregelt, dass Entscheidungen, die für den Betroffenen eine rechtliche Folge nach sich ziehen oder ihn erheblich beeinträchtigen, nicht ausschließlich auf eine automatisierte Verarbeitung personenbezogener Daten gestützt werden dürfen, die der Bewertung einzelner Persönlichkeitsmerkmale dienen. Durch die Vorgabe gem. § 6a BDSG soll erreicht werden, dass die Letztverantwortung immer durch eine natürliche Person mit echtem Ermessensspielraum erfolgt.³² Nach der gesetzlichen Wertung sind daher Systeme, die vollautomatisiert arbeiten und entscheiden, grundsätzlich bedenklich. Gleichwohl hat der Gesetzgeber zahlreiche Ausnahmenvorschriften vorgesehen, die eine automatisierte Videoanalyse ermöglichen. So genügt als Ausnahmetatbestand etwa wieder die Berufung auf berechtigte eigene Interessen, wenn ausreichende Sicherheitsvorkehrungen getroffen wurden. Eine weitere Anforderung ist zwar die Information des Betroffenen über die automatisierte Entscheidung, für die aber keine besondere Form gilt, so dass bereits ein entsprechender Aushang ausreichen könnte.³³

²⁹ BECKER in Plath, § 6b Rn. 30.

³⁰ GOLA/SCHOMERUS, § 6b Rn. 31.

³¹ GOLA/SCHOMERUS, § 6a Rn. 3.

³² HORNING/DESOL, K&R 2011, 153, 158.

³³ KAMLAH in Plath, § 6a Rn. 21.

3.4.2 Thinking Camera als Standardbeispiel

[Rz 22] Das typische Beispiel für eine automatisierte Videoanalyse ist der Einsatz von «Thinking Cameras» (auch als «Smart Cameras» bezeichnet), die beispielsweise alle Besucherströme darauf überprüfen, ob bestimmten Personen nicht bereits zuvor ein Hausverbot erteilt wurde.³⁴ Technisch ist dies über einen Abgleich mit hinterlegten Bildern von Personen mit Hausverbot möglich.³⁵ In der fortgeschrittenen Version sollen auch auffällige Verhaltensmuster zu einer Meldung führen, etwa das Betreten des Ladenlokals mit einer Maske.³⁶ In beiden Fällen liegen sicherlich berechnete Interessen der verantwortlichen Stelle vor, allerdings werden zugleich Daten anderer Betroffener analysiert. Auch insoweit bedarf es immer einer sorgsamsten Interessenabwägung.

4 Case Studies

[Rz 23] Anhand von zwei weiteren Beispielen soll die Anwendung der vorstehenden Grundsätze für neue Konzepte zur Videoüberwachung verdeutlicht werden. Es ist jeweils zu prüfen, ob die neuen Konzepte zu einer stärkeren Beeinträchtigung der Betroffenen führen, inwieweit dies gerechtfertigt sein könnte und auf welche Weise der Betroffene geschützt werden kann.

4.1 Videoanalyse zur Verkaufsförderung

[Rz 24] Die Videoüberwachung kann nicht zur Kriminalitätsbekämpfung eingesetzt werden, sondern auch als Methode zur Optimierung von Verkaufsprozessen. Für den Betreiber von Ladenlokalen ist es etwa von großer Bedeutung, zu erfahren, wie lange Kunden in welchem Bereich verharren und wo bestimmte Produkte optimal platziert werden können. Hierbei kann die Videoanalyse unterstützend herangezogen werden.

4.1.1 Blickverlaufsanalyse

[Rz 25] Im Vorfeld der Eröffnung neuer Ladenlokale oder bei Veränderung der Inneneinrichtung kann anhand von ausgewählten Testpersonen exakt ermittelt werden, wohin der Blick der Testpersonen geht (Eye-Tracking). Hierfür ist es mit speziellen Videokameras unter Einsatz von unsichtbarem Infrarotlicht möglich, genau die Blickrichtung der Testpersonen festzustellen.³⁷ Auf diese Weise ist eine Überprüfung möglich, wie sich ein Kunde in dem Ladenlokal orientiert und welche Produkte dem Kunden besonders ins Auge fallen.

[Rz 26] Diese Technik greift jedoch massiv in das Persönlichkeitsrecht des Betroffenen ein. Ein Betroffener rechnet nicht damit, dass auf diese Weise genau sein Verhalten in einem Ladenlokal analysiert wird. Selbst wenn der Betroffene nicht namentlich bekannt ist, existieren derart genaue Aufnahmen von ihm, dass ein Personenbezug immer gegeben ist. Selbst ohne Personenbezug ist alleine die Beeinträchtigung des Persönlichkeitsrechts so stark, dass derartige Techniken aus-

³⁴ GOLA/SCHOMERUS, § 6b Rn. 4.

³⁵ Dieser Anwendungsfall wird aber in Österreich durch § 50a Abs. 7 DSGVO 2016 ausdrücklich ausgeschlossen.

³⁶ HORNING/DESOL, K&R 2011, 153, 155; GOLA/SCHOMERUS, § 6b Rn. 4.

³⁷ LAMIERI in Schwarz, Leitfaden Dialog-Marketing, S. 141.

schließlich mit Testpersonen durchgeführt werden dürfen, die genau über die Hintergründe der Analyse aufgeklärt wurden und zugestimmt haben.

4.1.2 Videoanalyse der Kundenströme

[Rz 27] Viele Unternehmen möchten jedoch ohne größeren technischen Aufwand auch im laufenden Betrieb das Verhalten der Kunden analysieren um die Gestaltung des Ladenlokals oder die Platzierung von Produkten zu optimieren. Hierbei kommt es gar nicht auf das Verhalten des einzelnen Kunden an, sondern auf statistische Erkenntnisse.

[Rz 28] Mit Hilfe einer Videoüberwachung des Ladenlokals und einer automatisierten Auswertung der Kundenfrequenz ist es etwa möglich, die Kundendichteverteilung in einem Ladenlokal zu analysieren. Zu diesem Zweck wird nur ausgewertet, wie häufig sich Kunden in bestimmten Bereichen des Ladenlokals aufhalten. Es entsteht eine Darstellung, die durch eine farbige Darstellung der Grundfläche die unterschiedliche Kundendichte darstellt. Es können so besondere «Hot Spots» und «Cold Spots» entdeckt werden. Ein Rückschluss auf einzelne Kunden ist bei der Auswertung ausgeschlossen, so dass die Eingriffsintensität bei dieser Art der Analyse gering ist. Tatsächlich ist der Eingriff sogar geringer als wenn die Videoaufzeichnungen zu dem gleichen Zweck manuell ausgewertet werden würden. Es ist allerdings darauf zu achten, dass die Nutzung der Videokameras zu dieser Art der Analyse noch von dem definierten Zweck erfasst sein muss.

[Rz 29] Ohne Einwilligung der Kunden ist es dagegen nicht zulässig, diese bei ihrem Besuch des Ladenlokals durchgängig zu beobachten. Auf diese Weise würden komplette Kundenprofile entstehen, die nicht ohne Einwilligung des Betroffenen angelegt werden dürfen. Selbst wenn der Name des jeweiligen Kunden nicht bekannt sein sollte, ist dieser aufgrund der genauen Erfassung zumindest identifizierbar. Wäre die Aufnahmequalität so niedrig, dass eine Identifizierung ausscheidet, könnte die Person regelmäßig auch nicht automatisiert von anderen Kunden unterschieden werden.

4.2 Videoanalyse zu Abrechnungszwecken

[Rz 30] Auch zu Abrechnungszwecken kann auf Videomaterial abgestellt werden. In einem Parkhaus ist es etwa denkbar, dass bei der Einfahrt der Wagen erfasst wird. Jedenfalls bei Dauerparkern oder Stammkunden können auch Abrechnungsdaten hinterlegt sein, die es überflüssig machen, bei der Ausfahrt zunächst an der Kasse zu zahlen.³⁸ Anhand der Daten könnte ein Computersystem bei der Ausfahrt automatisch die Verweildauer im Parkhaus ermitteln und hierauf basierend die Abrechnung vornehmen.

[Rz 31] Aus Sicht der Kunden geht hiermit ein Komfortgewinn einher, weil der Weg zum Kassensautomaten überflüssig wird. Auf der anderen Weise werden bei diesem Angebot personenbezogene Daten der Kunden erfasst, die auch längerfristig vorgehalten werden. Jedenfalls für den Nachweis der abgerechneten Gebühren dürften in einem solchen Fall Fotos von der Ein- und Ausfahrt gespeichert werden. Damit lässt sich auch nachträglich lückenlos festhalten, wer zu welchem Zeitpunkt das Parkhaus genutzt hat. Bei der klassischen Abrechnung über eine Parkkarte

³⁸ Vgl. Der Standard vom 30. März 2010 über die Videoerfassung in Salzburg; online unter <http://derstandard.at/1269448456390/Salzburg-Videoerfassung-am-Garagenschranken>.

werden dagegen keinerlei Daten mit Personenbezug gespeichert, da anhand der Parkkarte kein Nutzer identifiziert werden kann.

4.2.1 Optionales Angebot statt zwingende Nutzung

[Rz 32] Um datenschutzrechtlichen Bedenken aus dem Weg zu gehen, empfiehlt es sich, die Erfassung mittels Videoanalyse nur optional anzubieten. Auf diese Weise haben alle Nutzer des Parkhauses weiterhin die Möglichkeit, dort anonym zu parken. Wenn das Angebot aktiv gewählt werden muss, dann können im Rahmen der Wahl des Abrechnungsmodus auch datenschutzrechtliche Einwilligungserklärungen eingeholt werden, mit denen der Kunde der Erfassung zu Abrechnungszwecken zustimmt. Gegenüber diesen Kunden wäre die Datenverarbeitung außerdem zur Vertragserfüllung erforderlich, da der Kunde ausdrücklich die Abrechnung auf diese Art gewählt hat.³⁹

[Rz 33] Die Schaffung einer Auswahlmöglichkeit ändert aber nichts daran, dass zunächst kurzfristig alle Fahrzeuge bzw. Kennzeichen erfasst werden müssen, damit diese mit der Liste der Kunden abgeglichen werden können, die eine automatisierte Abrechnung gewählt haben. Dies ist dann datenschutzrechtlich akzeptabel, wenn die Daten der übrigen Kunden sofort nach der entsprechenden Überprüfung gelöscht werden und insoweit keine weitergehende Speicherung erfolgt. Die Eingriffsintensität ist dann nicht viel höher, als wenn alle ein- und ausfahrenden Fahrzeuge von einem Mitarbeiter kontrolliert würden.

4.2.2 Speicherung der Daten und Zugriff auf die Daten

[Rz 34] Wenn die Videoanalyse tatsächlich ausschließlich zu Abrechnungszwecken erfolgt, dann genügt es, nur die Kennzeichen zu erfassen. Aus Gründen der Missbrauchskontrolle kann es zusätzlich allenfalls noch angemessen sein, Teile der Frontpartie des Wagens aufzunehmen. Auf diese Weise kann etwa verhindert werden, dass gestohlene Kennzeichen verwendet werden. Für die Abrechnung ist dagegen die Kenntnis des Fahrers oder gar etwaiger weiterer Insassen nicht erforderlich, so dass ein entsprechender Bildausschnitt zu wählen ist. Dem Kunden muss jedoch klar sein, dass in Verbindung mit der oftmals vorhandenen allgemeinen Videoüberwachung des Parkhauses auch auf diese Weise später seine Identifizierung möglich ist.

[Rz 35] Außerdem dürfte es für spätere Nachweispflichten genügen, wenn jeweils ein Standbild bei Ein- und Ausfahrt mit Zeitstempel archiviert wird. Videosequenzen, die etwa das Fahrverhalten zeigen, werden nicht benötigt und dürfen auch nicht abgespeichert werden. Bezüglich der Aufbewahrungszeit scheint es notwendig zu sein, die Nachweise so lange aufzubewahren, wie die Abrechnung angezweifelt werden kann. Ist die Rechnung gezahlt und gibt es keine Beanstandungen, dürfte zumindest kurz danach der Grund für eine weitere Speicherung der Daten entfallen.

[Rz 36] Während der Aufbewahrungszeit muss üblicherweise niemand Zugriff auf die Daten nehmen. Es ist daher ausreichend, wenn der Zugriff auf die Daten davon abhängig gemacht wird, dass eine Beschwerde des Kunden vorliegt oder ein anderer Umstand eintritt, bei dem eine Auskunftspflicht eingreift, etwa gegenüber den Strafverfolgungsbehörden. In allen anderen Fällen

³⁹ Hierzu kann auf die Ermächtigungsgrundlage gem. § 28 Abs. 1 S. 1 Nr. 1 BDSG zurückgegriffen werden, vgl. GoLA/SCHOMERUS, § 28 Rn. 8.

muss bzw. darf kein Zugriff gewährt werden.

5 Literatur

GOLA, PETER / SCHOMERUS, RUDOLF, Bundesdatenschutzgesetz, 10. Auflage, München (2010).

HORNUNG, GERRIT / DESOI, MONIKA, Smart Cameras und automatische Verhaltensanalyse, in: Kommunikation & Recht 2011, S. 153 ff.

PLATH, KAI-UWE, Kommentar zum BDSG sowie den Datenschutzbestimmungen des TMG und TKG, Köln 2013.

SCHREMS, MAXIMILIAN, Private Videoüberwachung, 1. Auflage, Wien (2011).

SIMITIS, SPIROS, Bundesdatenschutzgesetz, 8. Auflage, Baden-Baden (2014).

SEBASTIAN MEYER, Rechtsanwalt und Notar / Datenschutzauditor (TÜV), BRANDI Rechtsanwälte, Adenauerplatz 1, 33602 Bielefeld, DE, sebastian.meyer@brandi.net; <http://www.brandi.net>