



# Video-Überwachungstechnik

## *Gerichtsverwertbarkeit digitaler Bilder aus Videoüberwachungskameras*

Der Grundsatz der freien Beweiswürdigung ist ein elementarer Bestandteil der deutschen Strafverfahrensordnung. Die Gerichte entscheiden in richterlicher Unabhängigkeit, welche Beweise sie in einem Prozess zulassen.

Das vorliegende BHE-Papier ist daher nicht als Richtlinie oder Empfehlung zur Nutzung digitaler Videobilder vor Gericht zu verstehen, sondern vielmehr als Hinweispapier, wie die Gerichtsverwertbarkeit solcher Bilder im Falle einer Nutzung vor Gericht reibungsloser und zuverlässiger erfolgen kann. Dabei wird hier vorausgesetzt, dass der Betrieb der Videoüberwachungsanlage den jeweils gültigen Datenschutzrichtlinien entspricht.

Daher soll unter Wahrung des Grundsatzes der freien Beweiswürdigung nachfolgend dargestellt werden, wie die technischen Standards digitaler Videobilder verbessert und diese so für die Gerichte einfacher handhabbar gemacht werden können.

### Die Videoüberwachung

Die Videoüberwachung in bestimmten Einsatzbereichen, z.B. in Banken, Supermärkten oder an Tankstellen, gehört heute zu unserem täglichen Leben wie der Geldautomat oder die Scannerkasse im Einzelhandel.

Das Ziel der Videosysteme ist jedoch nicht, jeden beliebigen Menschen ständig im Blick zu haben, sondern entweder Straftaten zu verhindern oder kritische, meist kriminelle Vorgänge zu dokumentieren und so den Ermittlungsbehörden Hinweise und Beweise für die Überführung der Täter zu liefern.



Bei professionell eingesetzten Videoüberwachungsanlagen werden inzwischen ausschließlich digitale Bildaufzeichnungssysteme eingesetzt. Zielsetzung dabei ist die zuverlässige und aussagekräftige Nachvollziehbarkeit von Vorgängen, die im Erfassungsbereich der Videoüberwachung passieren.

So sind nach Überfällen oder gewalttätigen Übergriffen bspw. im Selbstbedienungsfoyer von Banken die Bilddaten der vorgeschriebenen digitalen Bildaufzeichnungssysteme eine wichtige Ermittlungsbasis für die Polizei.

## Die Problematik

Im deutschen Rechtssystem müssen Beweismittel bestimmten Anforderungen genügen, um einerseits vor Gericht überhaupt zugelassen zu werden und andererseits als aussagekräftig akzeptiert zu werden. Sowohl Betreiber von Videosystemen als auch Anwälte und Polizeibehörden mussten hier schon leidvolle Erfahrungen machen: Sofern die Echtheit der Bilder vor Gericht von der Verteidigung angezweifelt wird, muss nachgewiesen werden, dass die Bildsequenzen authentisch sind und vor allem nicht manipuliert worden sind.



Daneben wird häufig die Aussagekraft der Bilder in Frage gestellt, z.B. wenn der Blickwinkel, die Perspektive, die Auflösung oder Kompressionsartefakte die Bildqualität beeinflussen.



Gerade digitale Bilder werden vor Gericht immer wieder angezweifelt. Es ist allgemein bekannt, wie einfach z.B. digitale Urlaubsfotos am PC mit billigen Bildbearbeitungsprogrammen manipuliert werden können: den Himmel ein wenig blauer machen, der Schwiegermutter eine Hakenna-se verpassen usw. Wenn Laien mit einfachen technischen Mitteln so einfach Bilder verändern können, schafft das jemand mit etwas krimineller Energie sicherlich deutlich professioneller.

## Die geschlossene Beweiskette

Nachfolgend wird dargestellt, wie die Aussagekraft digitaler Videobilder und -sequenzen vor Gericht optimiert werden kann.

Bildaufzeichnungssysteme speichern von Videokameras aufgenommene Bilder auf digitalen Speichermedien, meist Festplatten. Zunächst muss nach einem Vorfall nachvollziehbar sichergestellt sein, dass die Bilder, die sich auf der Festplatte des Systems befinden, tatsächlich die Bilder sind, die während des Vorfalls aufgenommen wurden. Das System selbst sollte z.B. durch eine manipulationssichere Struktur der Datenbank gesichert sein. Der Betreiber eines Systems sollte sich vorab vom Systemlieferanten eine entsprechende schriftliche Erklärung geben lassen, in der das Verfahren, mit dem die Manipulationssicherheit hergestellt wird, genau beschrieben ist. Diese Erklärung kann auch vor Gericht als Nachweis genutzt werden.



Ist nun ein Vorfall, z.B. ein Tankstellenüberfall, dokumentiert worden, so werden die ermittelnden Behörden die Beweisbilder und -sequenzen sicherstellen. Bei Aufzeichnungssystemen mit Wechselfestplatte kann dazu die Festplatte gegen eine Neue getauscht werden, mit dem Vorteil, dass die Originalbilder auf der Originalfestplatte verbleiben können. Bei Aufzeichnungssystemen mit fest integrierter Festplatte muss das System die Auslagerung von Einzelbildern bzw. Bildsequenzen ermöglichen (Bildexport), um zu vermeiden, dass durch Abbau des Aufzeichnungssystems das gesamte Objekt ungeschützt ist.

Das Videosystem sollte es ermöglichen, alle zum Vorgang gehörenden Bilder auch von verschiedenen Kameras manipulationssicher auf einem Datenträger abzulegen, am besten auf einer nicht wieder beschreibbaren CD oder DVD. Auch der Dateiname sollte aussagekräftig vom System selbst bestimmt werden. Außerdem sollten die Bilddaten zusätzliche Daten zu ihrer Identifikation enthalten wie Datum/Uhrzeit, Kameraname und Schutzobjekt. Weiterhin sollte das System die Möglichkeit



bieten, in einer Textdatei, die mit den Bilddaten abgelegt wird, die Namen der bei der Datensicherung als Zeugen anwesenden Personen sowie Datum und Uhrzeit der Bildauslagerung abzuspeichern. Werden die Bilddaten in einem proprietären (herstellereigenen) Bildformat abgelegt, so sollte das System zusätzlich noch ein Viewer-Programm, mit dem die Bilder später wieder angezeigt werden können, auf dem Datenträger speichern. Abschließend wird der Datenträger von dem verantwortlichen Ermittler auf der Außenseite unveränderbar gekennzeichnet. Es empfiehlt sich, zwei Duplikate der Originalaufnahme anzufertigen. Das zweite Duplikat sollte beim Betreiber verbleiben.

Der Datenträger mit den ausgelagerten Bildern und Sequenzen wird wie jedes andere Beweismittel durch die zuständigen Behörden gesichert.

Die geschlossene Beweiskette kann durch entsprechende Softwareprogramme der Hersteller für digitale Aufzeichnungssysteme zusätzlich unterstützt werden. Diese Programme ermöglichen das nachträgliche Laden von exportierten Einzelbildern oder Bildsequenzen zur Prüfung der eindeutigen Authentizität.

### Die Bildqualität und ihr Einfluss auf die Aussagekraft der Beweisbilder

Neben der geschlossenen Beweiskette ist die Aussagekraft der Bilder selbst von hoher Relevanz.

Dies wird in einem BGH-Urteil aus dem Jahre 2005 detailliert beschrieben.  
([www.hrr-strafrecht.de/hrr/1/04/1-91-04.php?view=print](http://www.hrr-strafrecht.de/hrr/1/04/1-91-04.php?view=print))

- Sowohl eine vollständige Dokumentation des Tathergangs anhand von Übersichtskameras als auch die Personenidentifikation mit Hilfe von Detailaufnahmen sind für eine lückenlose Beweisführung wichtig. Dies ist jedoch nur mit einer optimalen Projektion der Kamerastandorte, einer entsprechend hohen Bildauflösung sowie einer niedrigen Kompressionsrate realisierbar.
- Für die Identifikation von Personen sind Kamerastandorte ideal, die den oder die Täter „auf Augenhöhe“ aufnehmen. In der Regel sind allerdings Aufnahmen von einer erhöhten Position notwendig. Daher ist bei der Planung von einem größeren Abstand zum Objekt auszugehen, der durch Nutzung von Teleobjektiven ausgeglichen werden kann. So verbessert sich die Wahrscheinlichkeit einer zuverlässigen Identifikation.
- Ebenso wichtig für die Identifikation ist die Detailauflösung auf den Bildern. Markante körperliche Merkmale, besonders im Gesicht (wie etwa die Nasenform, Nasenkrümmung usw.) sind bei anthropologischen Identitätsgutachten von entscheidender Bedeutung. Diese Merkmale können natürlich nur dann für ein Gutachten herangezogen werden, wenn sie auf den Bildern aufgrund der Pixelauflösung erkennbar sind. Um dies sicherzustellen, sind Testaufnahmen während der



Installation notwendig. Auch die von der Verwaltungs-Berufsgenossenschaft vorgeschriebenen Prüftafeln (s. BGV-Kassen) können hierbei helfen.

- Ebenso hilfreich ist eine hohe Bildrate (z.B. 5 oder mehr Bilder pro Sekunde und Kamera), damit möglichst viele Bilder den oder die Täter in unterschiedlichen Positionen zur jeweiligen Kamera zeigen. Die Wahrscheinlichkeit, dass sich aufgrund der Vielzahl der Bilder und der lückenlos dokumentierten Bewegungsabläufe anhand der Bildsequenzen die Identität des Täters nachweisen lässt, steigt deutlich im Vergleich zu Sequenzen mit z.B. nur einem Bild pro Sekunde.



### Nachweise, die die Gerichtsverwertbarkeit digitaler Bilder fördern:

- Dokumentation der Bildentstehung
- Gewährleistung der Authentizität der Bilddaten bei einem Kompressionsverfahren
- Die unveränderte Verfügbarkeit der Originaldaten
- Nachvollziehbarkeit von Bildbearbeitungsmaßnahmen zur Verbesserung der Detailerkennbarkeit
- Vorlage einer lückenlosen Dokumentationskette für das Beweismaterial
- Softwareprogramme zur nachträglichen Prüfung der Bildauthentizität



Der Inhalt wurde mit größter Sorgfalt zusammengestellt und beruht auf Informationen, die als verlässlich gelten. Eine Haftung für die Richtigkeit kann jedoch nicht übernommen werden.