



# Orientierungshilfe für die Videoüberwachung in und an staatlichen Hochschulen

Stand 05/2011

## I. Grundsätze

1. Staatliche Stellen und privatwirtschaftliche Unternehmen setzen zunehmend Videoanlagen zur Überwachung öffentlicher und nicht-öffentlicher Räume ein, um Straftaten zu verhindern oder mögliche Täter zu ermitteln. Wissenschaftliche Studien belegen allerdings, dass die Videoüberwachung kein Allheilmittel ist, mit dem man überall Sicherheit und Ordnung gewährleisten kann. Vor ihrem Einsatz ist deshalb stets eine sorgfältige Prüfung erforderlich.
2. Die Videoüberwachung lässt sich in technischer Hinsicht auf unterschiedliche Weise realisieren. Von Videobeobachtung (Monitoring) spricht man, wenn die aufgenommenen Bilder nur auf einen Monitor übertragen werden. Bei dieser Fallkonstellation stellt der Monitor sozusagen ein "verlängertes Auge" des Betrachters dar. Deshalb greift diese Form der Videoüberwachung auch weniger intensiv in die Rechte der Betroffenen ein als dies bei der Speicherung (Videoaufzeichnung) der Bilddaten der Fall ist. Sie ist die andere Variante der Videoüberwachung. Noch eingriffsintensiver ist die zusätzliche Speicherung und Übermittlung von so genannten Audiodaten, also von Tonaufnahmen. Sie ist deshalb grundsätzlich auch nicht erlaubt.
3. Jede Form der Videoüberwachung stellt einen Eingriff in das Persönlichkeitsrecht der davon betroffenen Personen dar. Sie ist deshalb nur zulässig, wenn es dafür eine gesetzliche Grundlage gibt oder die Betroffenen der Videoüberwachung zugestimmt haben. Dies gilt für jede Form der Videoüberwachung.
4. Im Hochschulgesetz selbst gibt es keine Regelungen zur Videoüberwachung. Als gesetzliche Grundlage kommen deshalb nur die Bestimmungen des Landesdatenschutzgesetzes (LDSG) in Betracht. Es enthält in § 34 eine Sonderregelung für die Videoüberwachung in öffentlich zugänglichen Räumen. Für die Videoüberwachung in sonstigen Bereichen kommen die §§ 12 bis 14 des LDSG in Betracht.
5. Bei der Prüfung der Zulässigkeit der Überwachungseinrichtung ist also danach zu unterscheiden, ob sie sich in öffentlich zugänglichen oder nicht öffentlich zugänglichen Räumen befinden. Unter öffentlich zugänglichen Räumen sind Bereiche zu verstehen, die von einem unbestimmten oder nur nach allgemeinen Merkmalen bestimmten Personenkreis betreten und genutzt werden können und ihrem Zweck nach auch dazu bestimmt sind. Die Zweckbestimmung kann sich aus einer Widmung für den öffentlichen Verkehr oder aus dem erkennbaren Willen des Berechtigten ergeben. Ein öffentlicher Raum kann innerhalb und außerhalb von Gebäuden liegen.

Bezogen auf die Hochschulen sind vor allem der Campus, Hörsäle, Seminar- und Kursräume, auch wenn sie als PC-Pools benutzt werden, Lesesäle oder Kopierräume in Bibliotheken sowie Amtsbereiche mit Publikumsverkehr während der üblichen Sprechzeiten öffentlich zugängliche Bereiche, natürlich auch die dazu gehörenden Gebäudeflure und Foyers.

Beispiele für nicht öffentliche Bereiche sind vor allem der zentrale Serverraum der EDV-Abteilung oder nur mit Schlüsselgewalt zugängliche Institutslabore, auch Büros und sonstige Verwaltungsräume, ebenso öffentlich zugängliche Gebäude außerhalb der üblichen Nutzungszeiten, wenn sie nur von Personen mit Schlüsselgewalt betreten werden können. In diesen Bereichen kann der Inhaber des Hausrechts die Nutzer konkret (namentlich) bestimmen.

6. In bestimmten Tabubereichen ist die Videoüberwachung grundsätzlich unzulässig. Das ist immer dort der Fall, wo die Überwachung mit einem Eingriff in die Intimsphäre der Betroffenen verbunden wäre, was regelmäßig bei einer Videoüberwachung vor oder in Umkleide- oder Toilettenräumen der Fall ist.

Zugänge zu Toiletten können ausnahmsweise zur Verhinderung von Gewalt videoüberwacht werden, wenn diese Zugänge nur eingeschränkt einsehbar sind.

Auch Mensen und Cafeterien, die zur Kommunikation mit anderen Personen besucht werden, sollten prinzipiell von Videoüberwachung verschont bleiben.

7. Gegenstand dieser Orientierungshilfe sind nicht die sog. "virtuelle Hörsäle", bei denen Vorlesungen z.B. in einen anderen Hörsaal übertragen werden. Gleichwohl sollte hier nur die/der Dozent/in von der Kamera erfasst werden. Falls auch Studierende ins Blickfeld geraten, sollte darauf hingewiesen und dies auf die vorderen Sitzreihen beschränkt werden. Werden von einzelnen Veranstaltungen Aufzeichnungen beispielsweise zur wissenschaftlichen Dokumentation angefertigt, ist dies nur möglich mit (konkludenter) Einwilligung der Teilnehmer/Innen nach vorheriger Information.

Soweit die Videoüberwachung an Hochschulen nicht von vornherein ausgeschlossen ist (vgl. I. 6.) sind an ihre Zulässigkeit - je nach Fallkonstellation - also unterschiedliche Anforderungen zu stellen.

## II. Videoüberwachung öffentlich zugänglicher Räume

1. Soweit es um die Videoüberwachung öffentlich zugänglicher Räume geht, kommt als gesetzliche Grundlage § 34 LDSG in Betracht. Danach ist eine Videoüberwachung in Form der Videobeobachtung (Monitoring) zulässig, wenn dies
  - a. Zur Aufgabenerfüllung oder der Wahrung des Hausrechtes
  - b. erforderlich ist und
  - c. keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Die Videoaufzeichnung ist nur dann zulässig, soweit dies

- d. zur Abwehr einer konkreten Gefahr für die öffentliche Sicherheit oder zum Schutz der Funktionsfähigkeit gefährdeter öffentlicher Anlagen
- e. erforderlich ist und
- f. keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Für die Videoaufzeichnung ist eine Vorabkontrolle nach § 9 Abs. 5 LDSG durchzuführen.

2. Eine konkrete Gefahr für eine zulässige Videoaufzeichnung liegt grundsätzlich nur dann vor, wenn Vorkommnisse in der Vergangenheit die Annahme rechtfertigen, dass auch künftig schwerwiegende Beeinträchtigungen der Interessen und Schutzgüter der Studierenden und der Hochschule drohen. Dabei kann es um die Sicherheit der Studierenden, der Lehrenden sowie der Beschäftigten gehen, aber auch um die Unversehrtheit von Hochschuleigentum. Sachbeschädigungen, Diebstähle und Einbrüche können daher eine Videoaufzeichnung - jedenfalls prinzipiell - ebenso rechtfertigen, wie Körperverletzungen oder sonstige Delikte gegen die körperliche Integrität der genannten Personen.
3. Die Videoüberwachung muss außerdem auch verhältnismäßig sein. Dies ist nicht der Fall, wenn der Hochschule Mittel zur Verfügung stehen, die weniger eingriffsintensiv sind als die Videoüberwachung. Eine solche Alternative besteht in der Regel während laufender Kurs-, Seminar- oder Fortbildungsveranstaltungen, weil die soziale Kontrolle durch die Referenten, Studierenden oder Beschäftigten so hoch ist, dass es nicht zu Straftaten kommen dürfte. Mit anderen Worten: Videoüberwachung ist dann grundsätzlich unzulässig.

Als weitere mildere Mittel zum Schutz des Eigentums kommt die Sicherung von DV-Geräten gegen Gelegenheitsdiebstähle mittels Stahlseilen, Kensington-Schlössern oder Brandsiegeln in Betracht. Gegebenenfalls kann auch die Beobachtung der Eingangstür zu einem PC-Pool genügen, um Diebstähle zu vermeiden bzw. aufzuklären. Bildschirmhalte der Arbeitsplätze in PC-Pools dürfen auf keinen Fall von der Überwachungsanlage erfasst werden. In Außenbereichen kann die Sicherheit gegebenenfalls durch den Einsatz von Scheinwerfern mit Bewegungsmeldern erhöht werden.

4. Eine bloße Bildübermittlung zur unmittelbaren Betrachtung auf Monitoren ("verlängertes Auge") greift weniger intensiv in die Rechte Betroffener ein als die Speicherung solcher Bilddaten. Monitoring ist aber nur dann zweckmäßig und somit verhältnismäßig, wenn auch tatsächlich eine simultane Beobachtung der übertragenen Daten erfolgt. Zudem muss sichergestellt sein, dass bei einer für ein Rechtsgut auftretenden Gefahr von der beobachtenden Stelle ohne Verzögerung Schutzmaßnahmen eingeleitet werden können. Wurde die Videoüberwachung z.B. anlässlich eines tätlichen Übergriffes

auf eine Studentin bzw. einen Studenten auf dem Campus eingerichtet, um solche Vorfälle zu vermeiden bzw. direkt eingreifen zu können, wäre die Maßnahme zur Erfüllung des Zwecks nicht geeignet und deshalb unzulässig, wenn eine Beobachtung nur zeitweise sichergestellt wäre. Ansonsten kann die Videoüberwachung den unerwünschten Effekt haben, dass auf anonyme Hilfe vertraut wird und in Gefahrensituationen Anwesende nicht selbstständig helfend intervenieren.

5. Weiterhin dürfen auch keine Hinweise dafür vorliegen, dass schutzwürdige Interessen der von einer Überwachungsmaßnahme betroffenen Personen die Interessen beispielsweise des Inhabers des Hausrechts überwiegen. Die Überwachung sensibler Bereiche im Sinne der Ziffer 1.6 ist daher grundsätzlich ausgeschlossen.
6. Das reine Monitoring von Schrankenanlagen an Zutritts-/Zufahrtsbereichen kann dann weitgehend unproblematisch gehandhabt werden, wenn die Beobachtung eng auf den jeweiligen Bereich beschränkt wird und keine sonstigen, insbesondere keine dem öffentlichen Verkehr gewidmeten Flächen außerhalb des Campus erfasst werden. Die dabei zum Einsatz kommenden Kameras sollten über keine Zoom- oder Schwenkfunktionen verfügen.

### **III. Videoüberwachung in nicht-öffentlich zugänglichen Hochschulbereichen**

Geht es um die Videoüberwachung in Hochschulbereichen, die nicht öffentlich zugänglich sind (vgl. I. 5.), kommen die allgemeinen Vorschriften zur Datenverarbeitung in Betracht, also vor allem die §§ 12 bis 14 LDSG. Das bedeutet, dass ein Monitoring gem. § 12 Abs. 3 Ziff. 2 LDSG dann zulässig ist, wenn "die zu erfüllende Aufgabe ihrer Art nach eine solche Erhebung erforderlich macht und keine Anhaltspunkte vorliegen, dass ihr überwiegende schutzwürdige Interessen der Betroffenen entgegenstehen". Die Speicherung und Nutzung dieser Daten, d.h. das Aufzeichnen der Videoüberwachung, richtet sich dann nach § 13 LDSG.

Eine Videoüberwachung ist außerdem zulässig, wenn die von ihr Betroffenen eingewilligt haben. Diese Einwilligung muss freiwillig sein. Ob das der Fall ist, ist sorgfältig zu prüfen.

### **IV. Hinweispflicht**

1. § 34 Abs. 2 LDSG verlangt, dass auf die Form (Monitoring o. Aufzeichnung) der Videoüberwachung sowie die verantwortliche Stelle (z.B. Hochschule, Studierendenwerk, Gebäudeeigentümer, selbständiges Forschungsinstitut) hingewiesen wird. Dies geschieht in der Regel durch entsprechende Piktogramme (vgl. DIN 33450) oder Hinweisschilder. Sie sind so anzubringen, dass sie vor dem Betreten des überwachten Bereichs mühelos (z.B. an der Eingangstür zum PC-Pool) wahrgenommen werden können. Ist die Überwachungsanlage nur während einer bestimmten Tageszeit in Betrieb, so ist auch darauf hinzuweisen.
2. Im Hinblick auf das Transparenzgebot empfiehlt es sich, auch auf die Überwachungsmaßnahmen in nicht öffentlich zugänglichen Räumen mit geeigneten Mitteln hinzuweisen.

### **V. Die Behandlung aufgezeichneter Daten**

1. Ist die Videoüberwachung mit einer Aufzeichnung und Speicherung der aufgenommenen Daten verbunden, müssen diese Daten gelöscht werden, wenn sie zur Erreichung des ursprünglichen Zwecks nicht mehr erforderlich sind (vgl. § 34 Abs. 5 LDSG). Dies ist regelmäßig 2 bis 3 Arbeitstage nach dem Beginn der Aufzeichnung der Fall, es sei denn, durch Feiertage werden längere Speicherzeiten notwendig. Über diesen Zeitraum hinaus können natürlich die Sequenzen gespeichert werden, die für polizeiliche Ermittlungen bei entsprechenden Vorfällen benötigt werden.
2. Es empfiehlt sich, die Aufzeichnungen zu verschlüsseln. Dies hat zur Folge, dass die aufgezeichneten Videodaten nur von einer bestimmten Person entschlüsselt und ausgewertet werden können. Nach Möglichkeit sollte das Schlüsselpaßwort auf mehrere Personen aufgeteilt werden, so dass der Zugriff auf die Aufzeichnungen immer nach dem "Vier-Augen-Prinzip" erfolgen muss.
3. Solange die Videoaufnahmen zulässigerweise gespeichert sind, dürfen nur besonders legitimierte Personen Zugriff auf diese Daten nehmen. Dieser Personenkreis ist ausdrücklich festzulegen. Er kann variieren, je nachdem, wer für die Videoüberwachung verantwortlich ist. In jedem Falle müssen die zugriffsberechtigten Personen dem Anlass entsprechend Verantwortungsträger sein. Es sollte nur ein möglichst kleiner Personenkreis zugriffsberechtigt sein.
4. Die Weitergabe von Videoaufzeichnungen darf nur im Rahmen der mit der Videoüberwachung unmittelbar verfolgten Zwecke an Polizei, Staatsanwaltschaft oder Gerichte erfolgen. Ein polizeilicher Zugriff aus anderen Gründen ist nur auf der Grundlage gesetzlicher Befugnisse erlaubt.
5. Jeder Zugriff und jede Auswertung ist zu dokumentieren. Auf diese Weise kann auch geprüft und nachvollzogen werden, ob die Überwachungsanlage nach Ablauf einer bestimmten Frist noch erforderlich ist.

## **VI. Dienstanweisung**

Alle mit einer Videoüberwachung zusammenhängenden Fragen und Probleme sind in einer allgemeinen Dienstanweisung der Hochschule unter Beteiligung der/des behördlichen Datenschutzbeauftragten zu regeln. Das gilt u.a. für den Zweck der Videoüberwachung und die zulässige Dauer der Videospeicherung, für den Kreis der zugriffsberechtigten Personen und die für eine Weitergabe in Betracht kommenden Anlässe. Auch die Notwendigkeit einer Dokumentation der Zugriffe ist festzulegen. Ggf. ist eine technisch mögliche Nutzung von Schwenk- oder Zoomfunktion zu untersagen.

## **VII. Institutionelle Beteiligungen**

1. Die von einer geplanten Überwachungsmaßnahme betroffenen Studierenden sind durch ihre Vertreter frühzeitig zu hören.
2. Die behördlichen Datenschutzbeauftragten sind gemäß § 11 Abs. 3 Nr. 1 LDSG ebenfalls rechtzeitig über geplante Videoüberwachungen zu unterrichten, damit sie auf die Einhaltung der vorstehenden Grundsätze hinwirken, im Falle einer Videoaufzeichnung die Vorabkontrolle durchzuführen, das der Videoüberwachung zu Grunde liegende Verfahren nach Maßgabe des § 10 Abs. 2 LDSG beschreiben und diese Beschreibung in das Verzeichnisseinstellen können.
3. Die zuständigen Personalräte sind entsprechend den Bestimmungen des Landespersonalvertretungsgesetzes zu beteiligen. In der Dienstanweisung oder einer entsprechenden Dienstvereinbarung (vgl. VI.) sollte eine ausdrückliche Erklärung enthalten sein, dass die mit der Überwachungsmaßnahme aufgezeichneten Daten nicht zu Verhaltens- und Leistungskontrollen der Beschäftigten genutzt werden dürfen.

## **VIII. Evaluation**

Nach Ablauf eines Jahres ist zu überprüfen, ob der Grund für eine zulässige Videoüberwachung noch fortbesteht. Zu diesem Zweck ist eine Evaluation durchzuführen. Liegen keine Anhaltspunkte für eine Gefährdung der Interessen und Schutzgüter mehr vor, ist die Maßnahme zu beenden. Die Anlagen müssen in diesem Fall nicht zwangsläufig entfernt werden. Es genügt, wenn sie gut erkennbar verhüllt sind. Liegt der Grund für eine Videoüberwachung allerdings noch vor, ist die Überprüfung regelmäßig einmal jährlich zu wiederholen.

## **IX. Kamera-Attrappen**

Der Einsatz von Kamera-Attrappen ist unter den Voraussetzungen der Videobeobachtung zulässig (§ 34 Abs. 6 LDSG). Für die Kenntlichmachung gelten dieselben Anforderungen wie dies beim Einsatz funktionstüchtiger Kameras der Fall ist.

## **X. Schlussbemerkung**

Die Entscheidung für eine Videoüberwachung im Hochschulbereich kann also nicht mit leichter Hand erfolgen. Sie bedarf umfassender und sorgfältiger Abwägungen. Das dabei zu beachtende Verfahren ist komplex und zeitaufwändig. Studierende, Lehrende, Datenschutzbeauftragte und Personalräte sind einzubinden.