Stellungnahme

der Gesellschaft für Datenschutz und Datensicherung e.V. (GDD) i. R. d. Konsultation der Datenschutzgruppe nach Artikel 29 der EG-Datenschutzrichtlinie betreffend die Verarbeitung personenbezogener Daten aus der

Videoüberwachung

1. Allgemeines

Die Artikel 29-Datenschutzgruppe weist in ihrem Arbeitsdokument WP 67 zu Recht auf wachsende Gefahren für das Persönlichkeitsrecht durch eine zunehmende Videoüberwachung im öffentlichen und privaten Sektor und den Einsatz moderner Technologien zur Erhebung, Verarbeitung und Nutzung personenbezogener Bild- und Tondaten hin. Vor diesem Hintergrund und mit Blick auf den europa- und verfassungsrechtlich gewährleisteten Schutz der Privatsphäre unterstützt die Gesellschaft für Datenschutz und Datensicherung e.V. (GDD) die Bemühungen der Artikel 29-Gruppe zur Förderung einheitlicher und EG-richtlinienkonformer Datenschutzgrundsätze im Bereich der Videoüberwachung.

Verhindert werden muss insbesondere eine flächendeckende Videoüberwachung öffentlicher Räume. Das Grundrecht auf Freizügigkeit (Artikel 11 GG) gewährt nicht nur die Möglichkeit sich frei zu bewegen, sondern auch, dass dies nicht festgehalten und später den Grundrechtsträgern entgegengehalten wird. Dabei gilt es allerdings einen am Grundsatz der Verhältnismäßigkeit ausgerichteten Ausgleich zwischen den Interessen öffentlicher und nicht öffentlicher Stellen an der Durchführung der Videoüberwachung einerseits und dem Persönlichkeitsschutz der Betroffenen andererseits zu schaffen.

Ausgehend von dem in Deutschland bestehenden Regelungsgefüge zur Videoüberwachung werden nachfolgend - auf der Basis bisheriger praktischer Erfahrungen insbesondere der Privatwirtschaft - einige Empfehlungen zum datenschutzgerechten Umgang mit der Videotechnik gegeben. Dabei wird zunächst auf die Videoüberwachung allgemein und sodann speziell auf die Videoüberwachung am Arbeitsplatz eingegangen.

2. Rechtsgrundlagen in Deutschland

Die Zulässigkeit der Erhebung, Verarbeitung und Nutzung mittels Videotechnik gewonnener personenbezogener Informationen ist in Deutschland durch allgemeine Datenschutzgesetze (Bundesdatenschutzgesetz, Landesdatenschutzgesetze) und vorrangige bereichsspezifische Vorschriften für staatliche Stellen und die Privatwirtschaft geregelt. Entsprechend dem Grundsatz der Spezialität ist der Umgang mit personenbezogenem Bildmaterial bereits dann zulässig, wenn eine bereichsspezifische Vorschrift diesen vorsieht bzw. gestattet. Eine über das nationale Datenschutzrecht hinausgehende Rechtmäßigkeitsprüfung am Maßstab von Artikel 7 der EG-Datenschutzrichtlinie, wie sie das Arbeitsdokument WP 67 unter Gliederungspunkt 7. C) vorsieht, ist den verantwortlichen Stellen regelmäßig nicht zumutbar.

Das verfassungsrechtliche allgemeine Persönlichkeitsrecht findet im Hinblick auf Bildnisse insbesondere in den §§ 23 ff. des Kunsturhebergesetzes (KUG) eine spezielle Ausprägung. Grundsätzlich bedarf es nach dem KUG der Einwilligung der betroffenen Personen. Betroffene können ihre Persönlichkeitsrechte sowohl auf strafrechtlicher (Ehrenschutz gem. §§ 185 ff. StB) als auch auf zivilrechtlicher Ebene (Unterlassungs-, Wiederrufs-, Gegendarstellungs-, Schadensersatz-, und Geldentschädigungsansprüche) geltend machen. Wesentliche Bedeutung kommt ferner dem § 6b des Bundesdatenschutzgesetzes (BDSG) zu, der die Zulässigkeit der Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen durch staatliche und nicht staatliche Stellen regelt.

3. Videoüberwachung durch private und staatliche Stellen

Zu Recht weist die Artikel 29-Datenschutzgruppe darauf hin, dass ein erheblicher Teil der Informationen, die durch Videoüberwachung gesammelt werden, bestimmte oder bestimmbare Personen betrifft, die bei ihrem Aufenthalt in der Öffentlichkeit oder in öffentlich zugänglichen Gebäuden gefilmt werden. Dem trägt § 6b BDSG Rechnung, indem er speziell die Zulässigkeit der Beobachtung öffentlich zugänglicher Räume regelt. Für nicht öffentlich zugängliche Räume sind besondere Regelungen - bspw. im Rahmen des Arbeitnehmerdatenschutzes (z. B. Dienst-/Betriebsvereinbarungen) - erforderlich (WP 67, Gliederungspunkt 3.). Obwohl die Differenzierung nach öffentlich und nicht öffentlich zugänglichen Räumen insoweit sinnvoll ist, ergeben sich in der Praxis doch schwierige Abgrenzungsfragen im Hinblick auf das Merkmal „öffentlich zugänglich“. Hier wären Empfehlungen der Datenschutzgruppe bspw. in der Gestalt von Fallgruppen, wie sie das Innenministerium Baden-Württemberg veröffentlicht hat (Hinweise zum BDSG für die private Wirtschaft Nr. 40, vgl. Anlage 1), wünschenswert. Weitere Fallbeispiele finden sich bei Königshofen, RDV 2001, 220 f. (vgl. Anlage 2). Schwierige Abgrenzungsfragen können sich z. B. ergeben, wenn die Videokamera zum Zwecke der Zugangskontrolle bei Privatwohnhäusern oder nicht öffentlich zugänglichen Gewerbeobjekten (Firmengeländen) so ausgerichtet ist, dass gleichzeitig auch öffentliche Flächen (z.B. Teile von Gehwegen oder Straßen) erfasst werden. Klargestellt werden sollte ferner, dass öffentlich zugängliche Räume innerhalb oder aber auch außerhalb von Gebäuden liegen können.

Wünschenswert wäre ferner eine Klarstellung dahingehend, dass die Videoüberwachung nicht generell einer Vorabkontrolle (vgl. WP 67, Gliederungspunkte 7. A) und B)) unterliegt, sondern nur dann, wenn sie tatsächlich besondere Risiken im Sinne von Artikel 20 der EG-Datenschutzrichtlinie - z.B. auf Grund ihrer Großflächigkeit oder Intensität - beinhaltet.

Unter Gliederungspunkt 7. I) des WP 67 wird die Aussage getroffen, dass Videoüberwachungen, aus denen die rassische Herkunft, religiöse oder politische Überzeugungen, die Gewerkschaftszugehörigkeit oder sexuelle Gewohnheiten hervorgehen (sensitive Daten nach Artikel 8 der Richtlinie), zu verbieten seien. Dem kann in dieser Pauschalität nicht gefolgt werden. Zum einen kann eine derartige Videoüberwachung zur Verfolgung rechtlicher Ansprüche gem. Artikel 8 Abs. 2 e) 2. Alternative der EG-Datenschutzrichtlinie erforderlich sein. Da die Richtlinienvorschrift weit zu interpretieren ist und auch die vorgelagerte außergerichtliche Geltendmachung, Ausübung oder Verteidigung von - z. B. deliktischen - Rechtsansprüchen mit umfasst (vgl. Dammann, in: Dammann/Simitis, EG-Datenschutzrichtlinie, Artikel 8 Erl. 17; Klug, RDV 2001, 266 (273)), gilt insoweit eine Ausnahme vom grundsätzlichen Verbot der Verarbeitung sensitiver Daten. Zum anderen sind Videoüberwachungen, aus denen die rassische Herkunft, religiöse oder politisch Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, oftmals im öffentliche Interesse erforderlich, so

z. B. im Rahmen der Gefahrenabwehr bei öffentlichen Versammlungen. Zweifelsohne zu vermeiden ist aber eine diskriminierende Verwendung von Videomaterial.

Zutreffend stellt die Artikel 29-Gruppe fest, dass die Zwecke der Videoüberwachung im Vorfeld klar zu definieren (Grundsatz der Zweckbestimmung) und überdies zu dokumentieren sind. Die Videoüberwachung hat sich auf diese rechtmäßigen Zwecke zu begrenzen bzw. darf nur anderweitigen Zwecken dienen, wenn dies mit der ursprünglichen Zweckbestimmung nicht unvereinbar ist. Der Umstand der Videoüberwachung ist regelmäßig in geeigneter Weise für die Betroffenen transparent zu machen.

Hinsichtlich der den verantwortliche Stellen obliegenden Löschungsverpflichtung ist auf die Erforderlichkeit des Vorhaltens des Videomaterials im Einzelfall abzustellen. Im Übrigen sollte den Unternehmen ein angemessener Zeitraum für die Löschung zur Verfügung stehen, der u.U. eine Woche (vgl. WP 67, Gliederungspunkt 7. E)) überschreiten kann. Die Löschungspflicht sollte möglichst durch eine automatisierte Technik unterstützt werden, wobei anzumerken ist, dass dem Grundsatz der Datenvermeidung und -sparsamkeit schon bei der Gewinnung des Videomaterials eine gewichtige Bedeutung zukommt.

4. Videoüberwachung am Arbeitsplatz

Zu Recht stellt die Artikel 29-Gruppe fest, dass der Einsatz von Videotechnik zur Kontrolle der Qualität und des Umfangs von Arbeitstätigkeiten, die auch eine Verarbeitung personenbezogener Daten beinhalten, nicht als Regel erlaubt sein sollte. Handelt es sich bei öffentlich zugänglichen Bereichen gleichzeitig um Arbeitsplätze von Mitarbeitern (z.B. Wächter des Museums, Kassierer der Bank) so kann sich auch der Mitarbeiter auf den Schutz des § 6b BDSG berufen. Bei der Bewertung ihrer schutzwürdigen Interessen ist von Relevanz, ob die Mitarbeiter auch „Objekt“ der Beobachtung sein sollen. Dient die Videoüberwachung z.B. dem Schutz vor Überfällen, so muss sichergestellt sein, dass eine zweckfremde Auswertung zur Kontrolle des Mitarbeiterverhaltens grundsätzlich ausgeschlossen ist. Soll auch der Mitarbeiter Objekt der Kontrolle sein, so ist mit dem Bundesarbeitsgericht (BAG, NZA 1992, 43) davon auszugehen, dass schon die Möglichkeit der jederzeitigen Überwachung einen mit dem Anspruch des Arbeitnehmers auf Wahrung seiner Persönlichkeitsrechte regelmäßig nicht zu vereinbarenden Überwachungsdruck erzeugt. Zulässig ist die Beobachtung am Arbeitsplatz nur, wenn bei gleichzeitiger Berücksichtigung des Verhältnismäßigkeitsprinzips überwiegende Sicherheitsinteressen diese erforderlich machen. Mit dem Landesbeauftragten für den Datenschutz Niedersachsen (15. Tätigkeitsbericht 1999/2000, S. 184 f.) sollte von folgenden Grundsätzen ausgegangen werden:

- Das einen Eingriff in das Persönlichkeitsrecht rechtfertigende schutzwürdige Interesse des Arbeitgebers, etwa zum Schutz vor Verlust von Firmeneigentum durch Diebstahl, Unterschlagung oder den Verrat von Betriebsgeheimnissen, muss vor Beginn der Videoüberwachung durch konkrete Anhaltspunkte und Verdachtsmomente belegt sein. Eine vage Vermutung oder ein pauschaler Verdacht gegen die gesamte Belegschaft reicht nicht aus.
- Eine unter diesen Voraussetzungen statthafte Videoüberwachung ist grundsätzlich offen mittels einer sichtbaren Anlage nach vorheriger Information der Belegschaft durchzuführen.
- Eine Überwachung durch verdeckte Kameras ist als „ultima ratio“ zulässig, wenn dieses Mittel die einzige zumutbare Möglichkeit darstellt, berechtigte, schutzwürdige Interessen des Arbeitgebers zu wahren.

- Die Videoüberwachung unterliegt der Mitbestimmung des Betriebsrats oder der Personalvertretung. Ein unzulässige Videoüberwachung wird durch die Zustimmung des Betriebs- oder Personalrats nicht legitimiert (BAG, Urteil v. 15. Mai 1991 - 5 AZR 115/90-).
- Die durch eine rechtswidrige Überwachung gewonnenen Erkenntnisse unterliegen einem Verwertungsverbot und können somit im arbeitsgerichtlichen Verfahren nicht verwertet werden.

Zu beachten ist aber auch die aktuelle Entscheidung des Bundesarbeitsgerichts vom 27. März 2003 (2 AZR 51/02), wonach bei Vorliegen eines hinreichend konkreten Verdachts einer Straftat in Ermangelung anderer zumutbarer Aufklärungsalternativen auch eine verdeckte Videoüberwachung zulässig ist. Diese sinnvolle Rechtsprechung sollte von der Datenschutzgruppe aufgegriffen werden. Eine ggf. fehlende Zustimmung der Mitarbeitervertretung zu der verdeckten Überwachung führt nach Auffassung des BAG auch nicht zu einem gerichtlichen Verwertungsverbot, wenn der Betriebsrat in Kenntnis der Sachlage der Kündigung zugestimmt hat.

Schließlich sollte dem Umstand Rechnung getragen werden, dass nicht nur schwerwiegende sondern auch sonstige Straftaten das Vertauensverhältnis zwischen Arbeitgeber und Arbeitnehmer erheblich beeinträchtigen können.

Bonn, den 20. Mai 2003