EBERHARD KARLS
UNIVERSITÄT
TÜBINGEN

INTERNATIONALES ZENTRUM FÜR
ETHIK IN DEN WISSENSCHAFTEN (IZEW)

Heiner Koch, Cornelius Held, Tobias Matzner, Julia Krumm
unter Mitarbeit von Jaqueline Flack, Jens Hälterlein, Petra Markel,
Norma Möllers, Philipp Wittmann

Intelligente Videoüberwachung: eine Handreichung

herausgegeben von Regina Ammicht Quinn

IZEW Materialien Band 11

Intelligente Videoüberwachung: eine Handreichung

Materialien zur Ethik in den Wissenschaften
Band 11

herausgegeben vom
Internationalen Zentrum für Ethik in den Wissenschaften (IZEW)
Eberhard Karls Universität Tübingen

Intelligente Videoüberwachung: eine Handreichung

Heiner Koch, Cornelius Held, Tobias Matzner, Julia Krumm
unter Mitarbeit von Jaqueline Flack, Jens Hälterlein,
Petra Markel, Norma Möllers, Philipp Wittmann

herausgegeben von Regina Ammicht Quinn

Beteiligte Projektpartner_innen:

Maja Apelt (Universität Potsdam), Ralf P. Schenke (Universität Würzburg),
Fritz Strack (Universität Würzburg), Thomas Würtenberger (Universität
Freiburg)

Intelligente Videoüberwachung: eine Handreichung; Heiner Koch, Cornelius Held, Tobias Matzner, Julia Krumm unter Mitarbeit von Jaqueline Flack, Jens Hälterlein, Petra Markel, Norma Möllers, Philipp Wittmann, hg. v. Regina Ammicht Quinn. – Tübingen: IZEW 2015.
(Materialien zur Ethik in den Wissenschaften, Band 11)
ISBN 978-3-935933-12-4

 Internationales Zentrum für Ethik in den Wissenschaften (IZEW)
Eberhard Karls Universität Tübingen
Wilhelmstr. 19
72074 Tübingen
Tel.: +49 (0) 7071/29-77981
Fax: +49 (0) 7071/29-5255
E-Mail: izew@uni-tuebingen.de
Internet: www.izew.uni-tuebingen.de

Inhalt

MuViT ist ein von Mai 2010 bis September 2013 vom Bundesministerium für Bildung und Forschung im Rahmen des Programms für zivile Sicherheitsforschung für drei Jahre gefördertes Verbundprojekt. Ziel dieses Verbundes war es, mehrere technische Projekte beim Prozess der Entwicklung von Mustererkennungs- oder Video Tracking-Techniken zu begleiten. MuViT war an vier Universitäten beheimatet und integriert Perspektiven aus der Sozialpsychologie, Soziologie, Ethik und Rechtswissenschaft. Die beteiligten Projektpartner waren:

Internationales Zentrum für Ethik in den Wissenschaften, Universität Tübingen,

Prof. Dr. Regina Ammicht Quinn

Lehrstuhl für Organisations- und Verwaltungssoziologie, Universität Potsdam,

Prof. Dr. Maja Apelt

Lehrstuhl für deutsches, europäisches und internationales Steuerrecht, Universität Würzburg, Prof. Dr. Ralf P. Schenke

Lehrstuhl für Psychologie II, Universität Würzburg, Prof. Dr. Fritz Strack

Institut für Öffentliches Recht, Universität Freiburg, Prof. Dr. Thomas Würtenberger.

Diese Handreichung basiert auf den Ergebnissen des Projektes MuViT.

1 Einleitung

Diese Handreichung soll eine Unterstützung bei Entscheidungen der Forschung und Forschungsförderung, bei konkreten Technikeinsätzen und bei der politischen Entscheidung über den Technikeinsatz sein. Ethische und rechtliche Perspektiven ergänzen hierbei wirtschaftliche Erwägungen, stehen mitunter aber auch im Konflikt mit diesen. Würden diese Überlegungen unterbleiben, so könnte es zu einer wirtschaftsgetriebenen Versicherheitlichung gesellschaftlicher Lebensbereiche kommen, ohne dass die sozialen Kosten hierfür berücksichtigt werden.

Diese Handreichung ist aber keine Anleitung für die korrekte Einführung intelligenter Videoüberwachung. Der Fokus ist breiter: Es geht nicht nur um das „Wie", sondern auch um das „Ob". Dies bedeutet, dass der Sinn intelligenter Videoüberwachung generell reflektiert werden muss. Es ist wichtig zu fragen, ob es überhaupt im pragmatischen und ethischen Sinn „gut" ist, intelligente Videoüberwachung für den Sicherheitsbereich zu entwickeln und diese Technologie anschließend einzusetzen. Denn der Einsatz einer bestimmten Technologie für zivile Sicherheit ist nicht „alternativlos". Diese Handreichung beschreibt ethische und rechtliche Probleme, die sich durch die Entwicklung und den Einsatz intelligenter Videoüberwachung ergeben. Entscheidend ist dabei, dass dies vor dem Hintergrund genereller Überlegungen nach dem „Sinn" der Technologie geschieht. Es muss möglich bleiben, sich im Angesicht der im Folgenden erläuterten Aspekte gegen diese Technologie und für andere Lösungen entscheiden zu können.

Zum Gebrauch:

Diese Handreichung führt mit drei Beispielszenarien (2) in die Thematik der intelligenten Videoüberwachung ein. Anschließend werden die verwendete Technik und die Unterschiede zu herkömmlicher Videoüberwachung beschrieben (3). Nach einem Überblick über die empirischen Untersuchungen des Themas (4) werden in Abschnitt (5) die ethischen und rechtlichen Aspekte grundlegend diskutiert. Neben diesem allgemeinen, abstrakteren Teil bietet Abschnitt (6) jeweils eine fragenorientierte Entscheidungshilfe für die Forschungsförderung, die Technikentwicklung und die Anwendung der intelligenten Videoüberwachung. Abschließend wird exemplarisch eine Bewertung bezüglich einiger repräsentativer Aspekte aus den Beispielszenarien durchgeführt (7).

Grundsätzlich kann die Handreichung auf verschiedene Weise gelesen werden:

Der schnellste Einstieg gelingt über die fragenorientierte Entscheidungshilfe für die Forschungsförderung, die Technikentwicklung und die Anwendung der intelligenten Videoüberwachung (6). Am Ende jeder Frage stehen Verweise zu Abschnitt (5), in dem

die Hintergründe und die Details für die Beantwortung der jeweiligen Frage diskutiert werden.

Der Einstieg ist darüber hinaus direkt über die jeweiligen inhaltlichen Themenbereiche des Abschnitts (5) möglich. Dieser Bereich hat einen Nachschlagecharakter. Insgesamt ist es jedoch empfehlenswert, sämtliche Aspekte zur Kenntnis zu nehmen, da oft Querverweise und Zusammenhänge bestehen.

Schließlich kann die Handreichung ausgehend von drei Beispielszenarien (2) gelesen werden, die in die intelligente Videoüberwachung einführen. Am Ende der Handreichung werden die diskutierten Probleme und Bewertungen anhand dieser Beispiele exemplarisch erörtert (7). Dieses Vorgehen bietet sich vor allem für Lesende an, die mit der Thematik noch wenig vertraut sind.

Die Handreichung kann keinen demokratischen Deliberationsprozess ersetzen. Weder ist alles rechtlich Machbare anzustreben noch kann (und sollte) Ethik die Bedürfnisse aller Betroffenen in der Funktion als Stellvertreterin artikulieren. Damit geht der Umstand einher, dass die Legitimität politischer Entscheidungen nicht allein auf rechtlichen und ethischen Überlegungen gründen kann, sondern vor allem auf demokratischen Prozessen. Für diese können die ethischen (siehe 5.1.8) und rechtlichen Überlegungen besonders relevant sein. Eine spezifische Schwierigkeit für das hier behandelte Thema ist die Tatsache, dass die untersuchte Technologie in Deutschland zurzeit nicht durch staatliche Stellen eingesetzt wird. Angesichts der momentanen Rechtslage wäre das wohl auch nicht möglich. Daher basieren viele der Überlegungen auf Extrapolationen von Studien aus anderen Kontexten und Laborsituationen. Weder die psychischen noch die sozialen Auswirkungen lassen sich definitiv abschätzen. Auch die zu erwartende Rechtsentwicklung lässt sich nur begründet vermuten. Die Ausführungen in der Handreichung sind vor diesem Hintergrund zur Kenntnis zu nehmen. Nichtsdestoweniger wurden viele Punkte identifiziert und Begründungen entwickelt, die ernsthaft und verantwortungsvoll im Nachdenkprozess über intelligente Videoüberwachung berücksichtigt werden sollten.

Untersuchungsgegenstand der Handreichung ist die intelligente Videoüberwachung als Sicherheitstechnologie für den zivilen Bereich. Damit erhält der Umstand ein besonderes Gewicht, dass in verschiedenen Kontexten ein unterschiedliches Verständnis von Sicherheit existiert. Dies betrifft nicht nur unterschiedliche kulturelle Kontexte, sondern unterschiedliche gesellschaftliche Bereiche wie Wirtschaft, Recht und Ethik. Genauso gibt es in den verschiedenen Einsatzbereichen unterschiedliche Sicherheitsverständnisse, sei es beim privaten Einsatz im Geländeschutz oder in der Betriebssicherheit oder beim staatlichen Einsatz aus Gründen der Inneren Sicherheit, etwa zur Überwachung von Großveranstaltungen wie Fußballspielen oder Demonstrationen oder als Einsatz bei der Grenzsicherung.

Insofern ist bei konkreten Einsatzszenarien zu spezifizieren, von welcher Sicherheitsvorstellung die Rede ist. Insbesondere die rechtliche Perspektive geht dabei, ergänzt durch einen internationalen Rechtsvergleich, von einer europäischen bzw. spezifisch deutschen Perspektive aus. Die Debatte über intelligente Videoüberwachung ist geprägt von einem Sicherheitsverständnis als „security", also als Sicherheit vor Angriffen. Dies ist jedoch keine Selbstverständlichkeit, denn im „safety"-Bereich, also im Bereich der Betriebssicherheit, kann intelligente Videoüberwachung durchaus sinnvoll eingesetzt werden, ohne dass dieselben ethischen und rechtlichen Probleme wie im Bereich der Angriffssicherheit vorliegen müssen. Ein weiteres Problem der aktuellen Debatten über Sicherheits- und Überwachungstechnologie ist die Betonung der Terrorabwehr. Die Legitimierung einer Technik und die Strukturierung einer Debatte über Extremszenarien ist dabei nicht nur problematisch, weil Argumente auf den schlimmsten Fall reduziert werden, sondern auch, weil die Technik, wenn sie einmal rechtskonform eingeführt ist, in anderen Bereichen als der Terrorabwehr eingesetzt werden wird. Gerade im Bereich der Angriffssicherheit muss zur Bewertung der Technik eingehend und fundiert darüber diskutiert werden, inwiefern sie zur Gefahrenabwehr oder zur Aufklärung von Straftaten beitragen soll. Die höchst unterschiedlichen Sicherheitsbedürfnisse innerhalb der Bevölkerung dürfen dabei nicht übergangen werden.

2 Drei Beispiele für Standardeinsatzszenarien

2.1 Marktplatz

Der Marktplatz der Großstadt S gilt als Kriminalitätsschwerpunkt. Vor allem nachts ist er Schauplatz für Drogengeschäfte. Auch Passant(inn)en wurden schon tätlich angegriffen. Daher soll ein intelligentes Videoüberwachungssystem eingerichtet werden, das offen nahezu jeden Winkel des Marktplatzes erfassen soll. Die für den Drogenhandel typischen Bewegungsabläufe, Schlägereien sowie am Boden liegende Personen sollen erkannt werden. Bei jedem „Treffer" überprüft ein menschlicher Operator die Szene und alarmiert gegebenenfalls die nächste Polizeistreife zur Nachschau.

2.2 Einkaufszentrum

Die M-GmbH betreibt ein Einkaufszentrum („alles unter einem Dach") mit 60 Ladengeschäften sowie mehreren Cafés, Restaurants und einer Bowlingbahn. Der Betreiber nutzt ein intelligentes Videoüberwachungssystem, welches zur Wahrung der Betriebssicherheit auf gestürzte und liegende Personen ausgerichtet ist und herrenlose Gepäckstücke ausmachen soll. Außerdem wird das Bildmaterial dahingehend ausgewer-

tet, wie viele Passant(inn)en vor welchen Schaufenstern wie lange verharren. Darüber hinaus ist das Videoüberwachungssystem mit einer Gesichtserkennungssoftware ausgestattet, die Gesichter mit Fotos in einer privaten Datenbank abgleicht, in der Personen registriert sind, gegen die bereits ein Hausverbot ausgesprochen wurde. Laut aushängender Hausordnung erklären sich die Benutzer(innen) mit der detailliert geschilderten Überwachung beim Betreten des Einkaufszentrums einverstanden. Auf die Überwachung wird noch an mehreren Stellen hingewiesen.

2.3 Industriebetrieb

Die Schnell & Sicher AG ist ein renommierter Hersteller moderner Lenksysteme und exportiert als Zulieferer der Automobilbranche in zahlreiche Länder. In ihrem Werk in A beschäftigt sie ca. 500 Mitarbeiter(innen). Nachdem mit dem Betriebsrat eine Betriebsvereinbarung über die Installation von intelligenter Videoüberwachung getroffen wurde, ließ der Werksschutz ein intelligentes Videoüberwachungssystem installieren, das sowohl die Betriebssicherheit für die Mitarbeiter(innen) erhöhen als auch Betriebsspionage erkennen soll. Dazu werden in der gesamten Fertigungshalle Bewegungsmuster, die statistisch von den durchschnittlichen Bewegungsabläufen abweichen, detektiert. Sobald das System eine Abweichung ausmacht, wird der Werksschutz darauf hingewiesen. Diesem wird dann auf einem Monitor das von der alarmierenden Kamera aufgenommene Bild angezeigt.

3 Technik

Die intelligente Videoüberwachung besteht aus informationstechnischer Sicht aus einem Videoüberwachungssystem in Verbindung mit einem System zur sogenannten Mustererkennung. Darunter versteht man die automatische Erkennung von Regelmäßigkeiten in Daten und weitere darauf aufbauende Verarbeitungsschritte, wie die Klassifizierung der Daten in verschiedene Kategorien (Bishop 2006, 1). Im Fall der intelligenten Videoüberwachung sind die Daten die digitalisierten Bilder aus Überwachungskameras. Die Kategorien könnten beispielsweise verschiedene Verhaltensweisen sein oder auch zu identifizierende Personen. Neben der Klassifizierung ist die Berechnung der Position von Objekten in Videobildern über die Zeit – das Videotracking – eine weitere Möglichkeit der intelligenten Videoüberwachung (Maggio und Cavallaro 2011).

Ein Mustererkennungssystem verarbeitet die Daten für gewöhnlich in mehreren Schritten. Zuerst werden die Eingangsdaten für die weitere Verarbeitung aufbereitet. Diese Vorverarbeitung besteht bei Kamerabildern beispielsweise aus Filtern, welche den Kontrast verbessern oder verschiedene Beleuchtungssituationen der gefilmten Szene ausgleichen. In einem nächsten Schritt werden die relevanten Merkmale aus

den vorverarbeiteten Daten extrahiert. Ein Mustererkennungssystem benutzt nicht die gesamten Daten, sondern wertet nur bestimmte Eigenschaften dieser Daten aus. Für die Erkennung von Objekten könnte das etwa der Abstand zwischen ähnlich farbigen Bildpunkten oder die Anzahl ähnlich farbiger Bildpunkte in einer definierten Umgebung sein. Verbreitet ist auch die Beschränkung auf Bildbereiche, die sich zeitlich stark verändern, weil hier „etwas geschieht", während unveränderte Bereiche als „Hintergrund" betrachtet werden. Der sogenannte Merkmalsraum fasst alle Merkmale zusammen, die für eine bestimmte Mustererkennungsaufgabe berücksichtigt werden (Theodoridis und Koutroumbas 2008, 6). Um eine komplexe Aufgabe wie die Erkennung von Aktivitäten zu lösen, sind für gewöhnlich mehrere Schritte nötig, die jeweils als separates Mustererkennungsproblem verstanden werden können. Deshalb können beispielsweise die Bewegung oder die räumliche Position erkannter Objekte – also die Ergebnisse eines Mustererkennungsprozesses – als komplexe Merkmale für eine weitere Mustererkennung dienen. Vorstellbar wäre als Beispiel folgender Aufbau: In jedem einzelnen Videobild werden Objekte erkannt. Anschließend wird versucht, diese auf den folgenden Bildern wiederzufinden, woraus sich die Bewegung der Objekte im Raum (die Bewegungstrajektorie) ableiten lässt. Damit ließe sich ein System zum Videotracking realisieren. Sollen Aktivitäten erkannt werden, müssten in einem weiteren Schritt bestimmte Objekte als Menschen identifiziert und diese wiederum in verschiedene Gesten klassifiziert werden. Basierend auf den Gesten und den Bewegungstrajektorien könnte ein Mustererkennungsalgorithmus verschiedene Aktivitäten erkennen.

Für die ethische und gesellschaftliche Bewertung von Mustererkennungssystemen sind vor allem die Merkmale relevant, die in den letzten Verarbeitungsschritten eines solchen Systems zum Einsatz kommen. Beispielsweise hat ein System, das auf Gesten beruht, aus sozialer und ethischer Perspektive andere Probleme und Vorteile als eines, das auf der Bewegung von Objekten im Raum beruht.

Für die Mustererkennung selbst existiert eine Vielzahl verschiedenster Techniken (Theodoridis und Koutroumbas 2008). Generell lassen sich dabei zwei Ansätze unterscheiden: Regelbasierte Techniken und statistische Verfahren. Regelbasierte Techniken verwenden eine von Expert(inn)en formulierte Anzahl an formalen Beschreibungen dessen, was erkannt werden soll. Hier werden also die Merkmale angeführt, die vorhanden sein müssen. Dagegen generieren statistische Verfahren die Kriterien zur Erkennung aus den Daten selbst. Hier lassen sich nochmals zwei Vorgehensweisen unterscheiden (Theodoridis und Koutroumbas 2008, 7):

Überwachte Verfahren verwenden eine Anzahl sogenannter Trainingsdaten. Das sind Daten, die exemplarisch für die zu erkennenden Muster stehen – beispielsweise Videobilder, auf denen aggressives Verhalten zu sehen ist. Dazu müssen die zu erkennenden Muster vorher festgelegt und die Trainingsdaten entsprechend ausgewählt und markiert werden. Mit diesen Daten werden dann die Parameter eines ebenfalls vorher festgelegten, statistischen Modells so eingestellt, dass die Daten vom System richtig verarbeitet werden.

Unüberwachte Verfahren versuchen dagegen, ohne im Voraus bekannte Klassen oder Muster auszukommen. Sie teilen die Daten aufgrund einer statistischen Analyse in zwei oder mehrere Klassen ein. Dieses Verfahren könnte im einfachsten Fall „normale" von „außergewöhnlichen" Ereignissen unterscheiden. Es gibt aber auch Ansätze, die automatisch eine größere Anzahl von Klassen generieren. Diese basieren auf Ähnlichkeiten zwischen den Merkmalen und müssen nicht zwangsläufig mit natürlichsprachlichen Konzepten übereinstimmen. Vorannahmen hinsichtlich der Auswahl des Algorithmus, der Merkmale und die Definition von „Ähnlichkeit" spielen jedoch trotzdem eine Rolle.

In all diesen Systemen laufen Prozesse automatisiert ab. Automatisierung bezeichnet die Selbstständigkeit des ablaufenden Datenverarbeitungsprozesses (Langmann 2010). Von automatisierten Abläufen sind automatische zu unterscheiden und sprachlich klar zu trennen. Automatisch bedeutet durch Selbststeuerung oder Selbstregelung erfolgend (Wermke et. al. 2007). Für ein automatisiertes System ist die Steuerung definiert – ein automatisches System steuert sich selbst. Diese Unterscheidung ist für den Einsatz intelligenter Videoüberwachung wichtig, denn hinter den Begrifflichkeiten verbirgt sich die Frage, wer nach der Detektion gesuchter Verhaltensmuster über die Folgen entscheidet. In einer automatischen Architektur ist dies die Software des Überwachungssystems, wohingegen in automatisierten Verfahren ein(e) menschliche(r) Entscheidungsträger(in) aktiviert wird. In diesem Fall dient das System also als Assistenz für das Personal. Im letzteren Fall stellt sich allerdings die Frage, inwiefern der Entscheidungsspielraum des Personals bereits durch das technische System beeinflusst oder eingeschränkt ist. (Siehe 5.1.4 und 5.1.10.)

4 Empirische Grundlagen

Im Folgenden sollen einige praxisrelevante Ergebnisse sozialwissenschaftlicher und psychologischer Forschung zu automatisierter Videoüberwachung behandelt werden. Dabei werden nicht nur die eigenen Forschungsergebnisse des Projektes MuViT sondern auch der allgemeine Forschungsstand berücksichtigt. Die sozialpsychologischen und soziologischen Perspektiven auf die automatisierte Videoüberwachung beschäftigen sich mit deren Voraussetzungen, Prozessen und Folgen.

4.1 Psychologische und gesellschaftliche Voraussetzungen automatisierter Videoüberwachung

4.1.1 Psychologische Voraussetzungen

Akzeptanz von automatisierter Videoüberwachung

Gerade im letzten Jahrzehnt wurden immer wieder Versuche unternommen, das allgemeine Stimmungsbild in der Bevölkerung bezüglich herkömmlicher Videoüberwachung möglichst differenziert abzubilden. Neben der Frage der Effektivität von Überwachungstechnik ist die Ermittlung ihrer Akzeptanz äußerst wichtig geworden. Akzeptanz ist dabei nicht mit Legitimität oder Akzeptabilität zu verwechseln (siehe auch 5.1.9b). Die dargestellten Akzeptanzergebnisse beziehen sich auf Untersuchungen öffentlicher Videoüberwachung in den frühen 2000er Jahren. Zahlreiche Umfragen zur Videoüberwachung zu dieser Zeit ermittelten eine Zustimmung der Bevölkerung zwischen 60% und 80% (Hempel 2007) und eine Erhöhung des subjektiven Sicherheitsgefühls (Bornewasser et al. 2008). Weitere Studien bestätigen diese Ergebnisse (Gössner 2001; Reuband 2001). Im europäischen Vergleich zählt Deutschland zusammen mit Österreich dennoch eher zu den skeptisch eingestellten Ländern, während in Europa der Einsatz von Videoüberwachung mehrheitlich unterstützt wird (Hempel & Töpfer 2004).

Experimentelle Untersuchungen haben ergeben, dass bei der Risikowahrnehmung rationale und gefühlsbasierte Faktoren zusammenspielen und auf diese Weise das Bild neuer Technologien und deren Akzeptanz beeinflussen (z.B. Kahan et. al. 2007). Die im sozialpsychologischen MuViT-Teilprojekt durchgeführten Studien bestätigen die positive Haltung gegenüber herkömmlicher Videoüberwachung. Der Einsatz von Videokameras wird hauptsächlich aufgrund des Sicherheitsaspektes als sinnvoll erachtet. Jedoch lehnt ein Großteil der Befragten einen flächendeckenden Einsatz ab und wünscht sich mehr Transparenz bezüglich der überwachten Bereiche (z.B. eine höhere Anzahl und Sichtbarkeit von Hinweisschildern). Die Ergebnisse machen außerdem

deutlich, dass bei Studien zum Thema Akzeptanz sowohl die Meinung als auch das Verhalten von Personen in überwachten Situationen erfasst werden sollte, da in den vorliegenden Studien die abgefragte Meinung teilweise anders ausfällt als das gezeigte Verhalten. Ähnliche Befunde ergeben sich zum Teil bezüglich der neuen intelligenten Technik; so sind Menschen, die gegenüber klassischer Videoüberwachung eine positive Einstellung haben, auch aufgeschlossener gegenüber intelligenter Videoüberwachung.

4.1.2 Gesellschaftliche Voraussetzungen

Kriminologische und sozialwissenschaftliche Perspektiven auf Videoüberwachung

Soziologische und kriminologische Analysen von Videoüberwachung betonen, dass diese eine Form der situativen Kriminalitätsbekämpfung darstellt, die von „schlechten" Anreizstrukturen ausgeht, die kriminelles Handeln rational werden lassen (Garland 2008, 291ff.; Krasmann 2003, 330ff.). Videoüberwachung soll potenziellen Täter(inn)en eine hohe Wahrscheinlichkeit der Sanktionierung von Straftaten anzeigen und kriminelles Handeln somit irrational(er) machen. Allerdings lässt sich ein tatsächlicher kriminalpräventiver Nutzen von Videoüberwachung wissenschaftlich bislang nur begrenzt nachweisen, was auch von der Gewerkschaft der Polizei betont wird (GdP 2012). Wenn Kriminalitätsraten infolge des Einsatzes von Videoüberwachung sinken, was lediglich bei Diebstählen und Sachbeschädigungen eindeutig der Fall ist (Gras 2003, 124 ff.; Hempel 2007; Bornewasser et al. 2008), stabilisieren sich diese mit der Zeit wieder auf ihr Ausgangsniveau (Kammerer 2008, 76). Oft kommt es nur zu einer Verdrängung von Kriminalität an andere Orte.

Während in politischen Debatten häufig nur die datenschutzrechtliche Problematik von Videoüberwachung thematisiert wird, betont eine Reihe von sozialwissenschaftlichen Studien, dass Videoüberwachung auch zu Diskriminierung bestimmter Personengruppen führt (Armstrong & Norris 1999; Lyon 2003). Wenn sich die Auswertung von Videoaufnahmen auf äußere Merkmale einer Person konzentrieren muss, reproduzieren und verfestigen sich soziale Vorurteile, die bestimmte äußere Merkmale wie Geschlecht, Hautfarbe, Kleidung etc. als Indikator für die Gefährlichkeit einer Person bestimmen.

Automatisierte Videoüberwachung aus Sicht der Öffentlichkeit

Der öffentliche Diskurs wurde für den Zeitraum von 2006 bis 2010 am Beispiel diverser Printmedien analysiert. Im Lichte aktueller Ereignisse kann dieser sich gegenüber den hier beschriebenen Resultaten verschieben. Bezüglich des untersuchten Zeitraums lässt sich über automatisierte Videoüberwachung konstatieren, dass diese als ein Instrument betrachtet wird, mit dem sich ein breites Spektrum devianten Verhaltens (vom

Ladendiebstahl bis zum Terrorismus) kontrollieren lässt. Die sozialen oder psychischen Ursachen des devianten Verhaltens spielen im Diskurs keine Rolle. Dies gilt auch, wenn automatisierte Videoüberwachung als geeignetes Mittel zur Kontrolle von Risiken bezeichnet wird, die im Kontext von Massenveranstaltungen entstehen. Ereignisse wie eine Massenpanik werden als Risiken betrachtet, die sich auf der Basis von ausreichendem Wissen über die biologischen Grundlagen menschlichen Verhaltens und über statistisches Wissen erklären und vorhersagen lassen. Die Ergebnisse der Analyse des öffentlichen Diskurses spiegeln die kriminologische Annahme wider, dass Videoüberwachung vorrangig als Instrument der situativen Kriminalprävention eingesetzt wird, durch das versucht wird, das Ausmaß von Kriminalität zu kontrollieren, indem negative Anreizstrukturen geschaffen werden und darauf verzichtet wird, auf die sozialen oder psychischen Ursachen einzuwirken.

Der Einsatz automatisierter Videoüberwachung wird im öffentlichen Diskurs des Untersuchungszeitraums als zugleich notwendig und sinnvoll erachtet, da, so die öffentliche Argumentation, eine Auswertung der Aufnahmen durch Polizist(inn)en oder privates Sicherheitspersonal sowohl unzuverlässiger als auch kostenintensiver sei. Somit lässt der Fokus des öffentlichen Diskurses auf kriminalpräventive Potenziale automatisierter Videoüberwachung ihren Nutzen deutlich höher erscheinen als ihre Nachteile, auch wenn dies nicht explizit gesagt wird. Die Sicherheitsgewinne dieser Technik werden zumindest an keiner Stelle der untersuchten Dokumente in Frage gestellt.

Ebenso wenig problematisiert werden mögliche Diskriminierungseffekte. Im Zentrum einer kritischen Haltung gegenüber automatisierter Videoüberwachung, die durchaus vorhanden ist, stehen hingegen Datenschutzaspekte. Allerdings werden diese häufig als Ergebnis mangelnder Informiertheit der Öffentlichkeit interpretiert. Durch eine strategische Kommunikation sei die Sorge um datenschutzrechtliche Aspekte, so die Befürworter(innen) öffentlicher Videoüberwachung, letzten Endes lösbar. Grundlegender Zweifel am Sinn und Nutzen von automatisierter Videoüberwachung, der in politischen und sozialwissenschaftlichen Debatten durchaus geäußert wird, lässt sich im öffentlichen Diskurs im Untersuchungszeitraum noch nicht feststellen.

Eine ergänzende Untersuchung, die den öffentlichen Diskurs bis einschließlich des Jahres 2013 in Printmedien, dem Fernsehen und im Internet auf ethisch relevante Fragen untersucht, zeigt, dass sich spätestens seit Beginn des EU-Forschungsprojekts INDECT im Jahr 2009 die kritischen Stimmen zur Anwendung öffentlicher Videoüberwachung mehren. Im öffentlichen Diskurs werden seitdem neben datenschutzrechtlichen Aspekten zunehmend die Risiken der Etablierung eines Überwachungsstaates, Fragen zur informationellen Selbstbestimmung als auch Aspekte von Privatheit sowie der Bedrohung individueller Freiheit diskutiert.

Die öffentliche Problematisierung von Videoüberwachung findet jedoch bisher fast ausschließlich in den medialen Nischen eines kritischen Journalismus statt. So thema-

tisiert eine Sendung des rrb „Kontraste“ im Jahr 2011[1] unter dem Titel „Totale Überwachung. INDECT schafft Freiheit ab“, die freiheitsgefährdenden Aspekte durch den zunehmenden Einsatz von Videoüberwachung in öffentlichen Räumen. Auch der Fernsehsender 3 sat diskutiert 2009 in einer Sendung unter dem Titel „Mehr Sicherheit durch Videoüberwachung?“[2] den tatsächlichen Nutzen von Videoüberwachung im Kontext von Kriminalitätsbekämpfung kritisch. Zudem wird die Notwendigkeit einer differenzierten öffentlichen Berichterstattung, die sowohl über Grenzen öffentlicher Videoüberwachung zur Kriminalitätsbekämpfung als auch zu deren unterschiedlichen Anwendungskontexten kritisch informiert, reflektiert.

Vehemente und öffentlichkeitswirksame Kritik am Forschungsprogramm INDECT wird auch vonseiten der Aktivisten-Bewegung Anonymous getätigt: In zahlreichen öffentlichen Aktionen und Aufrufen versucht diese, eine größere Sensibilisierung der Öffentlichkeit für die privatheitsgefährdenden Aspekte von Videoüberwachung zu erzielen.

Im wissenschaftlichen Diskurs hingegen wird die Verwendung von Videoüberwachung bereits seit längerem kritisch diskutiert. Neben rechtlichen Fragestellungen, werden Fragen zu Privatheit und Freiheit, zu technischen Aspekten sowie gesellschaftlichen Problemstellungen analysiert. Während sich die rechtliche Auseinandersetzung den rechtsstaatlichen, bürger- und datenschutzrechtlichen sowie menschenrechtlichen Aspekten von Videoüberwachung widmet, zielen privatheitsrelevante Probleme auf Fragen nach der Gewährleistung der Anonymität erhobener Daten. Freiheitsrechtliche Fragestellungen hingegen werden in Hinblick auf Probleme von ziviler Freiheit und sozialer Kontrolle diskutiert. Weiterhin setzt sich der wissenschaftliche Diskurs kritisch mit den gesamtgesellschaftlichen Auswirkungen von Videoüberwachung in öffentlichen Räumen auseinander: In diesem Zusammenhang werden sowohl demokratietheoretische und zivilgesellschaftliche Fragstellungen, Effekte der Disziplinierung, der Diskriminierung und Exklusion von Randgruppen sowie damit einhergehende Verfremdungseffekte öffentlicher Räume reflektiert.

4.2 Prozesse

4.2.1 Psychische Prozesse der Überwachten

Auf der Grundlage der im sozialpsychologischen MuViT-Teilprojekt durchgeführten Analysen zur Wirkung von automatisierter Videoüberwachung lässt sich feststellen, dass die Effekte einer Überwachung mit intelligenter Technik durch eine Kombination aus „reinen“ Überwachungseffekten und Erwartungseffekten der Personen zustande kommen. Das bedeutet zum einen, dass Personen durch die Anwesenheit der Videokameras selbstaufmerksam werden, was wiederum zu einer Veränderung ihres Denkens,

[1] http://www.youtube.com/watch?v=TeSBwW20aTk&feature=related
[2] http://www.youtube.com/watch?v=C3vybvmMvyw.

Fühlens und Verhaltens führt; zum anderen entwickeln Personen zusätzlich Annahmen über die Wirkung von Videoüberwachung.

„Reine" Überwachungseffekte: Selbstaufmerksamkeit

Untersuchungen zur Theorie der Selbstaufmerksamkeit (Silvia & Duval 2001) zeigen, dass eine erhöhte Aufmerksamkeit auf die eigene Person zu Verhaltens- und Einstellungsänderungen führt. Die im sozialpsychologischen MuViT-Teilprojekt durchgeführten Analysen zeigen, dass sowohl bei Exposition mit herkömmlicher Videoüberwachung als auch bei Exposition in Verbindung mit Informationen zur intelligenten Videoüberwachung der Fokus der Aufmerksamkeit auf die eigene Person gelenkt wird. Dieser Zustand kann als unangenehm erlebt werden und sich auf das Verhalten von Personen auswirken (siehe 4.3.1).

Erwartungseffekte: Annahmen über die Wirkung von Überwachung

Aufgrund der im sozialpsychologischen MuViT-Teilvorhaben realisierten Studien lässt sich feststellen, dass Menschen persönliche Annahmen über die Wirkung von Videoüberwachung haben, die ihr Verhalten in einer überwachten Situation beeinflussen. Wenn Personen bspw. das Fühlen und das Verhalten in einer überwachten Situation vorhersagen sollen, wird der Einfluss der Überwachung überschätzt. So erwarten Versuchsteilnehmer(innen), dass sich mehr Personen in einer überwachten Situation von der Kamera wegsetzen oder den überwachten Raum meiden, als es tatsächlich der Fall ist. Die Information über eine neue intelligente Form der Überwachung kann dabei eine andere Erwartungshaltung erzeugen als die Information über herkömmliche Verfahren. Dies könnte Unterschiede erklären, die zwischen den beiden Überwachungsformen gefunden werden.

4.2.2 Soziale Prozesse der Entwicklung und Implementierung Entwicklungsprozesse

Aus den vom soziologischen MuViT-Teilprojekt mit den Entwicklern geführten Interviews geht hervor, dass zum Teil große Unterschiede in den Auffassungen von Kriminalität und Sicherheitsarbeit bestehen. So betrachten einige Entwickler kriminelles Verhalten als unabhängiges, konstantes, sozial invariables Phänomen und damit als ein durch einen Computer lösbares Problem. Andere wiederum sehen kriminelles Verhalten als sozial, kulturell und situativ bedingt, was ihrer Auffassung nach nur sehr begrenzt durch einen Computer erfasst werden kann.

Daraus ergeben sich auch Unterschiede, was die Einschätzung der Automatisierung betrifft. Das eine Extrem des Spektrums zwischen Voll- und Teilautomatisierung bilden einige Entwickler, die zuversichtlich sind, dass nicht nur die Erkennung und Analyse menschlichen Verhaltens technisiert werden könne, sondern von den automatisierten Videosystemen der Zukunft auch Entscheidungen übernommen werden könnten, sodass menschliches Sicherheitspersonal irgendwann entbehrlich werde. Auf dem an-

deren Ende des Spektrums bezweifeln einige Entwickler, ob die Systeme überhaupt in einem befriedigenden Maße kriminelles Verhalten erkennen können.

Implementierungsprozesse

Hinsichtlich der Frage, wie und in welchem Umfang automatisierte Videoüberwachungssysteme in die Sicherheitsarbeit integriert werden sollten, zeigten Interviews mit potenziellen Endanwendern deutliche Unterschiede zwischen polizeilichen Akteur(innen) und Akteur(innen) von Personenverkehrsunternehmen auf. Für die polizeilichen Akteur(innen) ging es in der Hauptsache um Gewaltdelikte und Terrorismus und weniger um Eigentumsdelikte wie bei den Personenverkehrsunternehmen. Gleichzeitig verband sich diese Fokussierung stets mit der Betonung des polizeilichen Erfahrungswissens und der eigenen Problemlösungskompetenz. Damit wurde automatisierter Videoüberwachung nicht der Status einer genuinen Lösung von Kriminalitätsproblemen zugewiesen, sondern lediglich eines möglicherweise sinnvollen Assistenzsystems. Dies ist sicherlich auf das professionelle Selbstverständnis der Polizei zurückzuführen, deren Legitimität auf der Herstellung von Sicherheit und Ordnung beruht.

Wohl weil Personenverkehrsunternehmen nicht in erster Linie für Sicherheit und Ordnung zuständig sind, findet sich weder die grundsätzliche Skepsis gegenüber der Realisierbarkeit automatisierter Videoüberwachung noch die damit einhergehende Verteidigung der eigenen Problemlösungskompetenz. Stattdessen stützt die Hoffnung auf die Vermeidung finanzieller Schäden den Glauben an die Realisierbarkeit automatisierter Videoüberwachung in absehbarer Zukunft.

Unterschiede traten zudem hinsichtlich der Arbeit der Operatoren in den Kontrollräumen auf. Während die polizeilichen Akteur(innen) die Auffassung vertraten, dass nichtautomatisierte Videoüberwachung ineffizient sei, weil die kognitiven Fähigkeiten menschlicher Überwachender begrenzt seien, war dies für die befragten Akteur(innen) der Personentransportunternehmen kaum ein Thema. Für letzteres dürfte entscheidend sein, dass mit Angestellten gesprochen wurde, die einen Stab von Sicherheitspersonal beschäftigen. Die Ineffizienz zu thematisieren, hätte den Wert der Arbeit in den Kontrollräumen aberkannt. Im Kontrast dazu haben die Akteur(innen) der Personenverkehrsunternehmen den mühevollen Charakter der Arbeit der Operatoren unterstrichen und damit automatisierte Videoüberwachung als Arbeitserleichterung definiert. Der Unterschied dürfte darauf zurückzuführen sein, dass die Polizei wesentlich weniger Personal zu reinen Überwachungszwecken abstellt, weil der größte Teil der Überwachungsinfrastruktur in privater Hand ist.

Schließlich traten auch Unterschiede hinsichtlich der Bedeutung datenschutzrechtlicher Vorgaben für die Sicherheitsarbeit auf. Aus der Perspektive der interviewten polizeilichen Akteur(innen) ist die Legitimität automatisierter Videoüberwachung vollständig in rechtlichen Regulierungen abgesichert. Das könnte sich daraus erklären,

dass diese in ihrer alltäglichen Arbeit nicht in demselben Maße mit Datenschutzregulierungen konfrontiert werden wie Akteur(innen) aus Personentransportunternehmen. Datenschutzrechtliche Löschfristen werden bei den Personentransportunternehmen hingegen ganz explizit zum Problem gemacht. Das lässt sich darauf zurückführen, dass sich die Personentransportunternehmen einerseits selbst in der Verantwortung sehen, die Polizei mit der Bereitstellung der Aufzeichnungen bei der Strafverfolgung zu unterstützen, andererseits jedoch als Betreiber der Videosysteme politischem und öffentlichem Druck hinsichtlich des Datenschutzes ausgesetzt sind und potenzielle Image-Verluste befürchten. Das professionelle Selbstverständnis sowie die Tatsache, dass es sich hier um staatliche Einrichtungen einerseits und um privatwirtschaftliche Unternehmen andererseits handelt, scheinen folglich entscheidend für die jeweils zugeschriebene Bedeutung automatisierter Videoüberwachung zu sein.

4.3 Sozialpsychologische und gesellschaftliche Folgen automatisierter Videoüberwachung

4.3.1 Folgen für die Überwachten

4.3.1.1 Psychologische Folgen

Im sozialpsychologischen MuViT-Teilvorhaben wurden Studien unter Laborbedingungen durchgeführt. Diese deuten darauf hin, dass automatisierte Videoüberwachung sowohl das Erleben als auch das Verhalten der beobachteten Personen beeinflusst.

Bewusstheit der Überwachung

Personen, die darüber informiert werden, dass sie mit automatisierter Technik überwacht werden, nehmen Kameras und Hinweisschilder stärker wahr, als Personen, die einer herkömmlichen Überwachung ausgesetzt sind.

Subjektives Erleben

Es zeigt sich, dass sich Personen, die intelligenter Videoüberwachung ausgesetzt werden, tendenziell beeinträchtigter fühlen als Personen, die mit herkömmlicher Technik überwacht werden. Darüber hinaus nimmt der subjektiv erlebte Stress zu Beginn der Überwachung in Verbindung mit Informationen zu intelligenter Technik stark zu, was bei herkömmlicher oder ausbleibender Überwachung nicht der Fall ist.

Verhaltensanpassung

Insgesamt zeigt sich, dass Personen überwachte Bereiche deutlich mehr meiden, wenn die Überwachung sehr auffällig ist. Dies gilt für alle Arten der Überwachung. Darüber hinaus wird ein Raum, der mit automatisierter Technik überwacht wird, stärker gemieden als ein Raum, der mit herkömmlicher Videoüberwachung ausgestattet ist. Es stellt sich die Frage, ob diese Verhaltensänderung auf eine Einschüchterung der Überwachten zurückzuführen ist, weil Einschüchterung häufig als Argument gegen den Einsatz von Videoüberwachung herangezogen wird. Jedoch gibt es keine Forschung, die speziell diesen Effekt von Videoüberwachung untersucht. Die Ergebnisse weiterer Studien im sozialpsychologischen MuViT-Teilvorhaben zur Einschüchterung durch Überwachung deuten darauf hin, dass eine reine Überwachungssituation für eine Einschüchterung nicht ausreicht. Vorläufige Resultate bestätigen die Annahme, dass andere Faktoren, bspw. das Aufzeigen möglicher Konsequenzen, eine Einschüchterung bedingen können.

Insgesamt muss beachtet werden, dass bereits nach kurzer Zeit eine Gewöhnung an die neue Technik beobachtet werden kann. Daher stellt sich die Frage, inwiefern die beschriebenen Effekte einen qualitativen Unterschied beschreiben oder mit einer anfänglichen Unsicherheit, die bei einer noch unbekannten Technik auftreten kann, zusammenhängen. Die Gewöhnung bedeutet allerdings nicht, dass die Technik damit unproblematisch würde. Die ethischen Gesichtspunkte bleiben relevant (siehe insbesondere 5.1.5 und 5.1.9). Darüber hinaus kann die Gewöhnung sogar dazu beitragen, dass negative Folgen – beispielsweise für Minderheiten – weniger Aufmerksamkeit bekommen.

4.3.1.2 Soziale Folgen

Über die sozialen Folgen automatisierter Videoüberwachung in Deutschland existieren keine umfassenden Studien, weil diese Systeme in Deutschland im öffentlichen Raum noch nicht eingesetzt werden. Die folgenden Vermutungen sind aus dem abgeleitet, was wir bereits über nicht-automatisierte Videoüberwachung im öffentlichen Raum wissen.

Diskriminierung & Exklusion

Soziale Exklusion bedeutet, dass Personen oder ganze Gruppen aufgrund bestimmter Merkmale (Alter, Ethnizität, Geschlecht, Religion etc.) aus bestimmten sozialen Prozessen, Ereignissen, Institutionen oder Räumen ausgeschlossen werden. Im Kontext der sozialwissenschaftlichen Erforschung von Überwachungspraktiken wurde soziale Exklusion als Effekt von vorurteilsbehafteten Entscheidungen des Überwachungspersonals thematisiert (Armstrong & Norris 1999; Lyon 2003). In Bezug auf die intelligente Videoüberwachung wäre es einerseits möglich, dass der Einsatz von Algorithmen die

unerwünschte Ausübung vorurteilsbehafteter Überwachung forcieren wird – etwa indem soziale Vorurteile bereits in die von Expert(inn)en formulierten formalen Beschreibungen einfließen, auf denen regelbasierte Techniken aufbauen, oder indem die Auswahl von Trainingsdaten für überwachte Techniken vorurteilsbehaftet erfolgt (siehe 3). Andererseits könnte bei der Programmierung der Algorithmen auch bewusst auf die Vermeidung von vorurteilsbehafteten Entscheidungen geachtet werden. Dies gilt es, dementsprechend zu reflektieren und (ggf. durch Antidiskriminierungsbeauftragte) zu kontrollieren (siehe 5.1.5).

4.3.2 Intendierte und nicht-intendierte psychologische und soziale Folgen für Überwachende

Auch über die psychologischen und sozialen Folgen der automatisierten Videoüberwachung für das Sicherheitspersonal existieren noch keine Studien. Wir können auch hier aus dem, was wir über die Technisierung von Arbeitsprozessen wissen, Vermutungen für die automatisierte Videoüberwachung ableiten.

Verbesserte Kontrolle vs. Kontrollmissbrauch

Die in die Technik eingebauten Möglichkeiten der Überwachung des Sicherheitspersonals durch automatische Protokolle der Überwachung („Wer schaut was wie lange an?“) bergen das Risiko der Überprüfung von Arbeitsleistung und Anwesenheit. Aus einem Instrument zum Schutz der Überwachten würde ein Instrument zur Kontrolle der Arbeitseffizienz durch Überwachende.

Entlastung vs. Entqualifizierung von Arbeit

Wenn die intelligente Videoüberwachung die Rolle des Sicherheitspersonals auf ein ausführendes Organ ohne oder nur mit eingeschränkten Entscheidungskompetenzen reduziert, kann dies zu einer De-Qualifizierung dieser Formen der Arbeit führen. Von den betroffenen Arbeitskräften würde dies möglicherweise nicht oder nicht nur als Unterstützung bei und Erleichterung von Arbeitsprozessen bzw. als Entlastung von Verantwortung erlebt, sondern (auch) als Degradierung empfunden werden. Dies wiederum könnte die intrinsische Arbeitsmotivation senken.

Betriebliche Kosteneffizienz vs. Stellenabbau

Die im öffentlichen Diskurs als „Entlastung des Sicherheitspersonals“ bezeichnete mögliche Auswirkung des Einsatzes von intelligenter Videoüberwachung kann genauso gut eine Entlassung des Sicherheitspersonals bedeuten. Sollte dies nicht der Fall sein, könnten sinkende Qualifikationsanforderungen trotzdem sinkende Löhne rechtfertigen. Insbesondere in privatisierten Bereichen der zivilen Sicherheit (also Bahnhö-

fen, Flughäfen, Großveranstaltungen etc.) könnte die intelligente Videoüberwachung Effekte zeigen, die zwar ökonomisch gesehen positiv bewertet werden können, aus der Warte der betroffenen Personen aber äußerst negativ sind. In noch stärkerem Maße als bereits geschehen, könnten sich im Sicherheitsgewerbe prekäre Arbeitsformen durchsetzen.

Die ethische Analyse der intelligenten Videoüberwachung legt allerdings nahe, dass es für deren Nutzung besonders geschultes Personal bedarf (siehe 5.1.10.). Ob sich die verbreitete Hoffnung auf eine kostensparende Technik vor diesem Hintergrund bewahrheitet, bleibt abzusehen – insbesondere, weil eine neue Technologie regelmäßig mit einem erhöhten personellen Aufwand für die Installation und die Wartung verbunden ist.

5 Problemfelder

5.1 Aus ethischer Perspektive

5.1.1 Zwecksetzung

Einsatzziele der intelligenten Videoüberwachung, Transparenz, Beteiligung

Die Bewertung einer Technologie hängt von ihrem Einsatz ab, und damit von den Zielen, die mit dieser Technologie erreicht werden sollen. Bei der Untersuchung dieser Ziele aus ethischer Perspektive ist es wichtig, zu beachten, ob:

a. die Ziele nicht auf falschen Annahmen über den momentanen Status des Einsatzkontextes beruhen (das bedeutet, dass die Überprüfung der verwendeten Begriffe, Statistiken und Theorien notwendig ist) und über die Leistungsfähigkeit der Technik

b. Transparenz besteht bezüglich der verfolgten Ziele.

c. die Interessen aller möglicherweise von einem Einsatz betroffener Personen berücksichtigt worden sind (siehe auch 5.1.8.).

d. die Ziele bei der Einführung der Technologie nicht andere sind als diejenigen, die zur Rechtfertigung angegeben werden (sog. function creep).

So kann es sein, dass die intelligente Videoüberwachung zur Abwehr terroristischer Gefahren oder schwerer Kriminalität eingeführt wird. Zeigen sich in diesen Bereichen keine Erfolge, dafür aber beim Einsatz gegen „anti-soziales Verhalten“ oder gegen Ord-

nungswidrigkeiten, könnte der Einsatz mit Verweis auf diese Erfolge gerechtfertigt werden, obwohl bei der Einführung andere Ziele angegeben worden sind.

Die Ethik sollte hierbei nicht den demokratischen Prozess der Zielfindung ersetzen. Solange es jedoch nicht gelingt, Minderheiten und nicht gehörte Stimmen zu integrieren, kann die Ethik bei der Zielsetzung versuchen, diese Perspektiven einzubringen und stark zu machen.

5.1.2 Alternative Lösungsansätze/Sicherheitsversprechen

Abhängigkeit von Technik und sozialen Prozesse, sozialpolitische Kriminalprävention

Technik alleine ist keine Lösung für soziale Probleme. So setzt etwa die intelligente Videoüberwachung nicht bei den Ursachen für Kriminalität an, sondern versucht sie als Symptom zu kontrollieren. Hier stellt sich die Frage, ob es nicht andere, ethisch besser zu rechtfertigende Möglichkeiten gibt, diese Ziele zu erreichen. Könnte etwa mit vergleichbarem Aufwand durch soziale Programme und Ursachenbekämpfung statt durch die Entwicklung und den Einsatz intelligenter Videoüberwachung ein vergleichbarer Erfolg in der Kriminalitätsbekämpfung erreicht werden, so dürfte die Ursachenbekämpfung vorzuziehen sein.

Gerade der Perspektivwechsel hin zur Ursachenbekämpfung kann mit einem Zielwechsel einhergehen. So könnte etwa statt der Bekämpfung von „anti-sozialem Verhalten" die Bekämpfung von Perspektivlosigkeit oder Ausgrenzung im Mittelpunkt der Überlegungen stehen. Dabei ist zu sehen, dass menschliches Verhalten keinem einfachen Ursache-Wirkungsprinzip folgt. Die Vorstellung, dass es sich um ein Problem mit einer gezielten „Lösung" handelt, kann deshalb noch immer ähnliche Schwierigkeiten aufwerfen wie der Versuch, die Symptome zu kontrollieren – nur dass es sich dann um eine soziale statt um eine technischen „Lösung" handelt. Nachhaltige und ethisch akzeptable soziale Veränderungen erfordern dagegen die Geduld, an einem komplexen Prozess teilzunehmen, statt schnell Ergebnisse zu schaffen. Dabei muss die Frage gestellt werden, wer definiert, was als „kriminell" wahrgenommen wird, und inwiefern sich diese Definition durch den Technikeinsatz verschiebt. Es ist insbesondere zu beachten, dass diese Wahrnehmung von „Kriminalität" durch den Technikeinsatz nicht mit der juristisch definierten Kriminalität – etwa im StGB – übereinstimmen muss.

5.1.3 Nicht-intendierte Einsatzszenarien

Dual use, Proliferation und Technikgestaltung

Sollten die Ziele, die bei der Entwicklung der intelligenten Videoüberwachung angegeben werden, ethisch vertretbar sein, so genügt dies noch nicht zur Beurteilung der möglichen Einsatzszenarien. Entwickler, Politik und Erstanwender haben nicht immer die Kontrolle über den Einsatz der Technologie. Daher müssen auch nicht-intendierte

Einsatzszenarien bedacht werden. Zivile Sicherheitstechnik kann dabei sowohl im militärischen Bereich als auch repressiv im Inneren eingesetzt werden. Daher stellen sich Fragen, inwiefern die Einsatzbereiche kontrolliert werden können und die Verbreitung der Technik in andere Länder geregelt werden kann. Gerade bei so grundlegenden Entwicklungen wie der Musterkennung und Bewegungsverfolgung in Videobildern ist eine Kontrolle über den Einsatz und die Verbreitung der Technologie schwierig.

Intelligente Videoauswertung ist schon jetzt im militärischen Bereich verbreitet und es besteht eine große Nachfrage nach einer verbesserten Technologie für den Einsatz von Drohnen. Darüber hinaus wäre die intelligente Videoüberwachung ausgezeichnet zur Unterdrückung demokratischer Bewegungen einzusetzen oder generell zur Unterdrückung politisch oder religiös abweichender Personen und Gruppierungen.

Deshalb stellt sich die Frage, ob man eine Technologie, die derart fragwürdige und durchaus wahrscheinliche Einsatzszenarien hat, bedenkenlos entwickeln sollte. Hier gilt es zumindest Anstrengungen zu unternehmen, solche Einsatzszenarien durch rechtliche Regelungen, durch Entwicklung und Design sowie durch Exportkontrollen zu erschweren. Während innerhalb Deutschlands die Möglichkeit besteht, durch rechtliche Regelungen eine Kontrolle der Einsatzszenarien zu gewährleisten, ist eine wirksame Einschränkung durch Design, durch Exportkontrollen oder durch rechtliche Regelungen im internationalen Bereich nicht absehbar. Dies gilt für die intelligente Videoüberwachung im besonderen Fall, weil die relevanten Informationen Datenverarbeitungsprozesse und folglich Ergebnisse der technischen Forschung betreffen. Diese können auch ohne den Export konkreter Technologie, sondern beispielsweise nur der Mustererkennungssoftware, den Einsatz solcher Systeme in anderen Staaten ermöglichen. Die technische Entwicklung aufzuhalten, ist dabei weder möglich noch unbedingt wünschenswert. Mit ihr geht jedoch die Verantwortung einher, in jedem Einsatzszenario dafür zu sorgen, dass sie ethisch verantwortungsvoll eingesetzt wird. Dies erfordert umfassende Anstrengungen der internationalen Politik. (Siehe auch 5.2.3. zur dual-use Problematik und 5.2.4. zur rechtlichen Situation in anderen Staaten).

5.1.4 Verantwortung

Künstliche Intelligenz, Mensch-Maschine-Interaktion, Zurechnungsprobleme

Bei Systemen mit künstlicher Intelligenz zeigt sich ein besonderes Problem in der Zurechnung von Verantwortung. In Deutschland sind vollautomatische Systeme, die Sicherheitsaufgaben wahrnehmen, nicht erlaubt. Eine intelligente Kamera dürfte etwa keine Schussvorrichtung auslösen. Dennoch stellt sich die Frage, wer die Verantwortung trägt, wenn Menschen sich auf die technische Assistenz des intelligenten Systems verlassen, etwa wenn eine Personenkontrolle auf der Grundlage eines Alarms der intelligenten Videoüberwachung durchgeführt wird oder aufgrund der vermeintlichen Gesichtserkennung eines Terroristen oder einer Terroristin jemand fälschlicherweise festgenommen wird.

Die „Intelligenz" technischer Systeme ist weit davon entfernt, dass diesen moralische Verantwortung zuzuschreiben wäre. Hierfür müssten sie moralische Argumentationen verstehen, verarbeiten und ihr Verhalten danach ausrichten können. Insofern kommt für technisches Versagen nur eine Verantwortung im Sinne der Haftung in Frage. Bei dieser haftungsrechtlichen Frage handelt es sich jedoch um eine juristische Frage danach, wer genau in Haftung zu nehmen ist – der Endanwender(innen), die Entwickler(innen) oder diejenigen, die über den Einsatz der Technik entschieden haben. An der Entwicklung und dem Einsatz von Sicherheitstechnologien sind viele unterschiedliche Akteur(innen) beteiligt. Dies reicht von Akteur(innen) auf der politischen Ebene, die sich für eine Forschungsförderung einsetzen bis hin zu konkreten Endanwender(inne)n wie dem Sicherheitspersonal, das die Technik bedient und nutzt. Hier ist die Zurechnung von Verantwortung nicht immer leicht. Daher macht es Sinn, die Verantwortlichkeiten der unterschiedlichen Akteur(innen) klar und transparent zu gestalten. Verantwortungslücken sollten vermieden werden. Aber auch wenn damit Haftungsfragen geklärt werden können, ist die moralische Verantwortung, die auch eine Änderung der Situation herbeiführen könnte, damit noch nicht unbedingt gegeben.

Während Verantwortungszuschreibungen für Haftungsfragen an Gruppen oder juristische Personen sinnvoll ist, ist dies bei der moralischen Verantwortung, welche die Handlungen beeinflussen soll, nicht der Fall. Die Verantwortung muss letztlich von realen Einzelpersonen getragen werden und nicht von juristischen Personen, technischen Systemen oder von Gruppen. Hierbei ist entscheidend, welche Personen ihr Verhalten so ändern können, dass die entsprechenden Probleme nicht mehr auftreten. Kann eine Einzelperson nicht alleine Änderungen bewirken, so kann sie dennoch die Pflicht haben, dies zu versuchen, in der Hoffnung, dass andere es ihr gleich tun. Das ist etwa dann der Fall, wenn angestrebt wird, über die demokratische Teilhabe einen Einfluss auf die politischen Entscheidungen auszuüben.

5.1.5 Gerechtigkeit/Diskriminierung

Lastenverteilung, Vorurteilsverstärkung, nicht-intendierte Diskriminierung

Die intelligente Videoüberwachung führt eine Klassifikation durch und sortiert Ereignisse oder Personen in bestimmte Kategorien ein. Im Sicherheitsbereich ist das letztendlich eine Klassifikation in „gefährlich" oder „ungefährlich". Die Klassifikation als „gefährlich" soll einen Alarm auslösen, der weitere Schritte einleitet. Diese können sich jedoch unter Umständen nachteilig für die als „gefährlich" eingestufte Person auswirken.

Die Klassifikation basiert auf der Differenzierung von Merkmalen, die in den Videobildern für das technische System erkennbar sind. Zentral ist die Frage, wann eine solche Differenzierung zu einer Diskriminierung wird. Die Einstufung einer Person als „gefährlich" aufgrund ihrer Hautfarbe ist diskriminierend. Das Allgemeine Gleichbehand-

lungsgesetz (AGG) gibt uns weitere Kategorien an die Hand, welche Differenzierungen diskriminierend sein können. Doch gerade mit der technischen Differenzierung von Merkmalen zur Identifikation von Sicherheitsrisiken können nicht nur altbekannte, sondern auch neue Formen der Diskriminierung auftreten. So könnte das System Menschen mit einem besonderen Gang als ungewöhnlich und potenziell „gefährlich" einstufen. Dies könnte dazu führen, dass beispielsweise Menschen mit Gehbehinderungen vom technischen System als Sicherheitsrisiko wahrgenommen werden. Zumindest solche objektiv grundlosen Einstufungen stellen eine Diskriminierung dar. Schwieriger wird dies bei besser gerechtfertigten Einstufungen. Sollten in einem bestimmten Bereich männliche Jugendliche statistisch übermäßig häufig als Gewalttäter in Erscheinung treten, könnte man sich die Frage stellen, ob diese einer intensiveren Überwachung und Kontrolle ausgesetzt sein dürfen. Hier würden Einzelpersonen, die selbst keinen Anlass dafür geliefert haben, stärker überwacht. Wiederum anders verhält es sich, wenn das System Schlagbewegungen erkennen könnte und auf dieser Basis einen Alarm auslösen würde. Hier hätten dann nur noch Fehler in der Erkennung potentiell diskriminierende Folgen.

Da die Diskriminierungen nicht nur explizit bei der Programmierung der Algorithmen zum Tragen kommen können, sondern auch unbeabsichtigt durch die Funktionsweise der Technik (z. B. durch häufige Fehlalarme bezüglich einer bestimmen Personengruppe), ist eine sorgfältige Überprüfung der Technik auf ein mögliches Diskriminierungspotential je nach Einsatzszenario durchzuführen. In diesem Zusammenhang kann eine ausführliche Protokollierung aller aufgrund der automatisierten Überwachung durchgeführten Handlungen sinnvoll sein. Gleichzeitig ist zu beachten, dass diese ein zusätzliches Überwachungsrisiko mit sich bringen kann.

Neben der Diskriminierung gibt es weitere allgemeinere Gerechtigkeitsprobleme. Die Vorteile und auch die Kosten der Sicherheitsmaßnahmen können ungerecht verteilt sein. So kann es sein, dass nur bestimmte Gruppen die Lasten zu tragen haben, die mit den Sicherheitsmaßnahmen verbunden sind, während gleichzeitig eine andere privilegierte Gruppe von den Sicherheitsmaßnahmen profitiert. Die Sicherheit der einen könnte somit auf Kosten der Privatheit anderer erkauft werden. Ein vergleichbares Problem stellt sich bei der Finanzierung der Maßnahmen: Wer hat in welchem Ausmaß die finanziellen Kosten zu tragen? Werden Sicherheitsmaßnahmen etwa privatisiert, haben ärmere Personen nicht immer die Möglichkeit, sich diese zu leisten.

5.1.6 Normalisierung Überwachung, Anpassungsdruck und Normalitätseinschreibung in die Technik

Eine Abweichung von der „Normalität" stellt für die intelligente Videoüberwachung einen möglichen Fall dar, ein Sicherheitsrisiko zu modellieren. Dies ist insbesondere bei statistisch arbeitenden Systemen der Fall. Diese lösen einen Alarm aus, wenn etwas „Ungewöhnliches" passiert. Die Normalitätserwartung des technischen Systems muss dabei nicht deckungsgleich mit der Normalitätserwartung des menschlichen Sicherheitspersonals sein. Aus Sicherheitserwägungen werden Details aus der Entwicklung solcher Systeme geheim gehalten. Deshalb ist es schwer nachzuvollziehen, wie die im System implementierte Normalitätserwartung zustande kam (Expertenwissen, Auswahl der Trainingsbeispiele etc.).

Dies könnte dazu führen, dass ein Anpassungsdruck entsteht, sich normal zu verhalten. Denn gerade weil die Normalitätserwartung des technischen Systems nicht transparent ist, ist unklar, an welche Normalität man sich anpassen muss, um nicht aufzufallen. Dies könnte zu einer Anpassung an Normen führen, die gar nicht durch das System überwacht werden sollen. Außerdem könnte die Intransparenz eine Überanpassung zur Folge haben. Selbst wenn die im System umgesetzte Normalitätserwartung relativ flexibel oder locker ist, könnte die diesbezügliche Unklarheit eine Verhaltensanpassung an durchaus strengere Normen nach sich ziehen, weil befürchtet oder vermutet wird, dass solches Verhalten erwartet würde.

Die Anpassung an eine Normalität ist ethisch beispielsweise in Hochsicherheitsbereichen besser vertretbar als im öffentlichen Raum. In ersteren kann klarer (und transparenter) definiert werden, welche Handlungsweisen erwartetet werden. Gleichzeitig ist die Einschränkung durch den Zwang, sich normal zu verhalten, in Hochsicherheitsbereichen oft geringer, es liegt eine bessere Vertretbarkeit des Sicherheitszwecks in sensiblen Bereichen vor und die Fehlerquote bei der Erkennung von Abweichungen ist geringer. Demgegenüber ist der Zwang zur Anpassung an die Normalität an öffentlichen, Plätzen mit pluralen Verhaltensweisen (etwa Marktplätzen) nur schwer durchführbar und kaum zu rechtfertigen. Ungerechte und nicht oder kaum zu rechtfertigende Ausschlüsse bestimmter Personen oder Personengruppen von öffentlichen Orten könnten die Folge sein.

Grundsätzlich ist zu bedenken, dass selbst an hochgradig regulierten Orten wie Flughäfen einheitliche Verhaltensweisen (üblicher Abstand zwischen Personen, Interaktionen etc.) kaum zu erwarten sind. Hier kommen kulturell variierende Verhaltensweisen zum Tragen, welche die Bestimmung von Normalitätserwartungen erschweren. Die Erwartung einer bestimmten Normalität kann sich hier schnell diskriminierend auswirken oder ein intelligentes Videoüberwachungssystem unzuverlässig machen.

5.1.7 Freiheit

Sicherheit als Freiheit, freiheitsschonende Alternativen, Abwägungsprobleme

Sicherheit und Freiheit werden oft als gegeneinander abzuwägende Güter dargestellt. Die Sicherheit steht dabei aber nicht als Selbstzweck, sondern soll beispielsweise der Gewährleistung von Rechtsgüterschutz und der Sicherheit bei der Grundrechtsausübung dienen oder die demokratische Betätigung sichern. Deshalb wird letztlich nicht Sicherheit gegen Freiheit abgewogen, sondern unterschiedliche Freiheiten. Aus diesem Grund stellt sich bei der intelligenten Videoüberwachung die Frage, welche Freiheiten eingeschränkt und welche gesichert werden sollen. In Szenarienbeschreibungen, wie auch bei der Planung eines Einsatzes intelligenter Videoüberwachung, müssen demnach zunächst die konkreten Freiheiten benannt werden, die geschützt werden sollen. Erst dann ist eine qualifizierte Bewertung und Abwägung möglich. Gerade weil Videoüberwachung oft nur erfolgreich bei der Aufklärung, nicht aber bei der Verhinderung von Straftaten eingesetzt werden kann, stellt sich die Frage, inwiefern Freiheiten überhaupt geschützt werden. Empirische Nachweise über die Wirksamkeit aus Vergleichsszenarien sowie die Evaluation des konkret vorliegenden Einsatzes müssen herangezogen werden, um die Sicherheitsleistung im Einzelfall der Überwachung nachzuweisen. Die Ergebnisse sind dann jeweils in Verhältnis zu den zu erwartenden Freiheitseinschränkungen zu setzen. Hierzu gehören sowohl die Freiheitseinschränkungen im Rahmen des Privatheitverlustes (siehe 5.1.9) als auch diejenigen im Bereich der Normalisierung (siehe 5.1.6). Generell festzuhalten ist, dass immer dann, wenn die intelligente Videoüberwachung einen Abschreckungseffekt haben soll, auch die Möglichkeit einer Einschüchterung besteht: Was getan werden muss, um nicht aufzufallen, ist bei der intelligenten Videoüberwachung intransparent. Dasselbe gilt für die Verarbeitung der erhobenen Daten. Deshalb könnten Personen eingeschüchtert werden, grundlegend unproblematisches Verhalten zu zeigen, weil sie unsicher sind, wie dieses eingestuft werden wird. Aus diesem Grund könnten sie auch vermeiden, den überwachten Kontext überhaupt zu betreten.

Wenn die intelligente Videoüberwachung Teil einer umfassenderen Überwachung wird, droht eine umfassende Kontrolle aller Lebensaspekte von Personen. Während hierfür in Deutschland insbesondere die Schnittstelle zwischen privater und öffentlicher intelligenter Videoüberwachung eine Bedrohung darstellt, kann dies in Bereichen mit einem eingeschränkten Grundrechtsschutz schon allein durch einzelne staatliche Akteur(innen) oder private Sicherheitsunternehmen geschehen. Hierzu gehören Grenzkontrollen, der Umgang mit Geflüchteten, die „totalen Institutionen" wie Gefängnisse, die Terrorismusabwehr, die Überwachung politischer Gruppierungen und Einzelpersonen sowie der Einsatz in autoritären Staaten (siehe 5.1.3).

Grundsätzlich macht es Sinn, nach Alternativen zu suchen, die freiheitsschonender sind (siehe 5.1.2). Die Ursachenbekämpfung und die Prävention stellen dabei ebenso Möglichkeiten dar wie eine Erhöhung der Resilienz als Widerstandsfähigkeit gegen Schäden und Angriffe. Es ist darüber nachzudenken, inwiefern die intelligente Videoüberwachung tatsächlich Angriffe oder Schäden verhindern kann oder ob sie hauptsächlich der Strafverfolgung dient.

5.1.8 Demokratie

Partizipation statt Akzeptanz, Akzeptanz und Akzeptabilität, Transparenz

Hier lassen sich zumindest vier zentrale Aspekte anführen, die zu bedenken sind: die Berücksichtigung der Interessen Betroffener, die Rolle von Akzeptanz und Transparenz sowie die Wirkung von Überwachung auf Demokratie.

Berücksichtigung der Interessen Betroffener

Oft werden in der Technikentwicklung als Stakeholder nur die Politik, die Forschung und die Wirtschaft angegeben. Diejenigen, die direkt von der Technik betroffen sind, werden dann vergessen: die überwachten Personen. Diese sollten, ggf. repräsentativ, so früh wie möglich in entsprechende Entscheidungs- und Planungsprozesse eingebunden werden. Dies gilt bei der Technikentwicklung genauso wie beim Technikeinsatz.

Bezüglich konkreter Überwachungsmaßnahmen sollte eine klar bestimmte und bekannte Stelle eingerichtet werden, an die sich die Überwachten bei Problemen wenden können. Da auf die Videoüberwachung zumindest im öffentlichen Raum entsprechend hinzuweisen ist, wären diese Hinweise auch dafür geeignet, auf eben jene Ansprechpartner(innen) aufmerksam zu machen.

Akzeptanz

Akzeptanzfragen scheinen bei der Einführung einer neuen (Sicherheits-)Technologie die entscheidenden, manchmal die einzigen Fragen zu sein. Dies ist ein grundlegender Fehler. Nach Akzeptanz zu fragen genügt, wenn man sich die Frage stellt, ob ein Produkt gut verkauft werden kann und es keinen Widerstand gegen dessen Einführung geben wird. Akzeptanz genügt jedoch nicht, um ethische Probleme zu lösen. Menschen könnten etwa aus Unkenntnis intelligenter Videoüberwachung zustimmen, ohne dabei zu wissen, welche Folgen dies für ihre Privatheit hat. Deshalb hat sich bspw. in der Medizinethik das Konzept der informierten Zustimmung durchgesetzt. Akzeptanz ist aus ethischer Perspektive nur dann interessant, wenn sie informiert stattfindet. Darüber hinaus stellt sich die Frage, wie viel Akzeptanz nötig ist, damit eine Technologie entwickelt und eingesetzt werden sollte. Hier ist der Minderheitenschutz

von zentraler Bedeutung. Wenn Personengruppen besondere Bedenken bezüglich der Überwachung haben, sollten diese berücksichtigt werden, selbst wenn die Mehrheit andere Bedürfnisse hat. Die Informiertheit und der Minderheitenschutz sind zentrale Elemente, um von einer faktischen Akzeptanz zu einer ethischen Akzeptabilität zu gelangen. Doch auch hier gilt, dass ethische Reflexion dies nicht alleine lösen kann. Erst durch die Partizipation der Betroffenen an den Entscheidungen kann gewährleistet werden, dass Akzeptanz in Akzeptabilität transformiert wird.

Transparenz

Eine informierte Zustimmung setzt voraus, dass eine hinreichende Transparenz vorhanden ist. Dies gestaltet sich bei modernen Technologien als schwierig. Während bei der herkömmlichen Videoüberwachung noch ein grobes Vorverständnis vorhanden ist, wie diese Überwachung funktioniert, ist dies bei der intelligenten Videoüberwachung nicht mehr unbedingt der Fall. So kann es kompliziert sein, zu vermitteln, nach welchen Kriterien das System einen Alarm gibt. Bei adaptiven Systemen, die sich automatisch an die Situation anpassen sollen, ist unter Umständen sogar dem Sicherheitspersonal unklar, warum das System einen Alarm gegeben hat. Oft ist die Vermittlung der Funktionsweise des Systems nicht gewünscht, da mit dieser Kenntnis das System leichter umgangen werden könnte. Zudem handelt es sich dabei um wertvolle Unternehmensgeheimnisse. Die demokratischen Kontrollmöglichkeiten werden durch die Einführung intelligenter Systeme also zunächst reduziert.

Es besteht Forschungsbedarf, wie diese Systeme so entwickelt oder modifiziert werden können, dass eine grundlegende Transparenz als Basis für die demokratische Kontrolle von Entwicklung und Einsatz hergestellt werden kann. Die Offenlegung der Funktionsweise gegenüber einem Datenschutzbeauftragten oder einer anderen unabhängigen Stelle könnte zumindest ein erster Schritt in die richtige Richtung sein.

Die Wirkung von Überwachung auf Demokratie

Generell bedeutet die technische Herstellung von Sicherheit, dass die Definitionsmacht darüber, was als sicher und was als Bedrohung gilt, zumindest teilweise an die Entwickler(innen), Hersteller(innen) und Betreiber(innen) der Technik übergeht (siehe 5.1.10). Damit birgt die technische Herstellung von Sicherheit die Gefahr, demokratische Prozesse, in denen der Wert von Sicherheit ausgehandelt wird, einzuschränken. Dieser Effekt wird verstärkt, wenn der Einsatz der Technik die Geheimhaltung von Details zu deren Funktion erfordert.

Neben dem Umstand, dass – auch in Demokratien – die Überwachung zur Kontrolle politischer Tätigkeiten eingesetzt werden kann, ist es denkbar, dass eine verbreitete Überwachung auch einen Einschüchterungseffekt hat, der Menschen davon abhält, sich politisch zu betätigen. Durch die Intelligenz der Videoüberwachung, die kosten-

günstigere Gestaltung der intelligenten Videoüberwachung und die Möglichkeit der weiteren Datenverarbeitung könnten sich diese Effekte verstärken. Daher besteht hier ein besonders strenger Regelungsbedarf. Während in demokratischen Ländern solche Regelungen teilweise möglich scheinen, dürfte die Etablierung von entsprechenden Regelungen in pseudodemokratischen Ländern oder autoritären Staaten unwahrscheinlich sein.

5.1.9 Privatheit

Datenerhebung, Datenverknüpfung, Missbrauch, privacy by design

Im öffentlichen Diskurs werden im Zusammenhang mit der intelligenten Videoüberwachung vor allem Probleme des Datenschutzes und der Privatheit thematisiert. Bei der Beurteilung der Auswirkungen auf die Privatsphäre ist es deshalb wichtig, sich zu vergegenwärtigen, dass diese Probleme zwar zentrale, aber bei Weitem nicht die einzigen wichtigen Faktoren sind.

Die Erhebung neuer personenbezogener Daten stellt eine Gefährdung für die Privatheit dar. Aus der Verhaltenserkennung und der Bewegungsverfolgung von Personen lassen sich viele Informationen gewinnen. Das ist insbesondere dann der Fall, wenn diese Daten mit einer Möglichkeit der Personenerkennung oder anderen Datensätzen verbunden werden. Daher bedarf eine solche Datenerhebung aus ethischer Perspektive einer besonderen Rechtfertigung, die bei allgemeiner und unspezifischer Überwachung nicht notwendig ist. Hierbei stellt sich die Frage, wie intelligente Videoüberwachung so gestaltet werden kann, dass die erhobenen Daten sicher sind, nur für einen bestimmten Zweck verwendet werden und nicht einfach ausgelesen oder mit anderen Daten abgeglichen werden können. Die Verschlüsselung von Daten und die mit detailliert spezifizierbaren Befugnissen ausgestattete Authentifizierung vor einem Datenzugriff sind hierbei Mindestvoraussetzungen. Da es konkrete Forschungsprojekte auch auf EU-Ebene gibt (etwa INDECT), welche Erforschen, wie die intelligente Videoüberwachung bei Drohnenflügen allgemein und unspezifisch eingesetzt und auch mit Gesichtserkennung und verschiedenen Datenbanken kombiniert werden kann, besteht Handlungsbedarf. Ob die Technik so gestaltet sein kann, dass sie nur privatheitschonend eingesetzt werden kann, ist fraglich.

Dennoch wird mitunter argumentiert, dass intelligente Videoüberwachung auch privatheitschonend eingesetzt werden kann. Die intelligente Überwachung könne ohne die Möglichkeit der Identifikation aller Personen eingesetzt werden. Im Gegensatz zur herkömmlichen Videoüberwachung wären nur die vom System als gefährlich eingestuften Personen identifizierbar. Bei gleicher Häufigkeit der Videoüberwachung könnte dies zur Reduzierung der Eingriffe in die Privatsphäre führen. Sollte intelligente Videoüberwachung so gut funktionieren, dass das der Fall ist, wäre jedoch davon auszugehen, dass sie aufgrund der Kosteneffizienz auch in Bereichen eingesetzt wird, in denen bisher nicht überwacht wird oder in denen zwar Kameras existieren, die Kame-

rabilder jedoch nicht ausgewertet werden. Dies könnte trotz des im Einzelnen privatheitschonenden Einsatzes zu einer deutlich umfassenderen Überwachung führen und damit letztendlich zu weitreichenderen Eingriffen in die Privatheit.

Das Recht auf informationelle Selbstbestimmung ist das Recht der einzelnen Person, über ihre Daten, deren Preisgabe und Verwendung selbst zu verfügen. Intelligente Videoüberwachung wird hier zum Problem: Insofern nicht transparent ist, nach welchen Kriterien überwacht wird, welche Daten erhoben und wie die erhobenen Daten genutzt werden, besteht nicht mehr die Möglichkeit, die Kontrolle über die Erhebung und die Verwendung von Informationen über die eigene Person zu erlangen bzw. zu behalten. Dies kann zu einer Verunsicherung darüber führen, wer was über wen weiß und wer mit welchem Wissen welche Zwecke verfolgt – oder auch nicht. Daher gilt es, transparente intelligente Videoüberwachungssysteme zu gestalten. Zugleich ist mit der Forderung nach Transparenz aber die Befürchtung verbunden, dass mit Hilfe der verfügbaren Informationen das System umgangen werden kann. Wie Systeme gestaltet werden können, deren Funktionsweise hinreichend transparent gemacht werden kann, ohne ihre Sicherheitsleistung zu untergraben, bleibt eine offene Forschungsfrage.

5.1.10 Kontextabhängigkeit

Dateninterpretation, kulturelle und lokale Unterschiede, Wertepluralismus

Das Ziel der intelligenten Videoüberwachung ist es, Bedrohungen für die Sicherheit im weitesten Sinne zu erkennen. Sicherheit ist aber kein objektiver Wert. Gerade in öffentlichen Räumen trifft eine Vielzahl von Menschen mit stark divergierenden Sicherheitsvorstellungen aufeinander. Handeln in der Öffentlichkeit ist damit Aushandeln der an einem konkreten Ort etablierten Sicherheitsvorstellungen. Sicherheit ist dabei eingebunden in ein Geflecht von Wertvorstellungen und wird gegen andere Werte wie Freiheiten, ökonomische Interessen, Praktikabilität u. a. abgewogen. (Auch wenn diese Abwägungsprozesse aus ethischer Perspektive problematisch sein können. Siehe 5.1.7.) Um gut zu funktionieren, muss ein intelligentes System an solche variablen Kontexte angepasst sein. Insbesondere muss sichergestellt werden, dass stetig Überprüfungen der Angemessenheit an den Einsatzkontext vorgenommen werden – insbesondere von adaptiven Systemen. Ansonsten besteht die Gefahr, gesellschaftlich-demokratische Prozesse zu bremsen, indem beispielsweise veraltete oder unrealistische Sicherheitsvorstellungen durchgesetzt werden.

Allgemein besteht das Problem, dass mit der Einführung der intelligenten Überwachung die damit implementierte Sicherheitsvorstellung den Kontext „kolonialisiert". Diese Sicherheitsvorstellung kann die Vorstellung einiger weniger Experten sein oder eine, die statistisch an einem anderen Ort gewonnen wurde. Mit dem Einsatz eines Systems, das Sicherheitsvorstellungen durchsetzt, besteht zudem die Gefahr, dass andere für den betreffenden Kontext wichtige Werte gegenüber der Sicherheit ins Hintertref-

fen geraten. Hier spielt nicht nur die tatsächlich durch die Überwachung gebotene Sicherheit eine Rolle. Auch die Erwartungen, die von den Überwachten an das System gerichtet werden, können das Handeln verändern (siehe 4.2.1). Dies kann sowohl durch eine Überschätzung (die dann z. B. zu fahrlässigem Verhalten aufgrund vermeintlicher Sicherheit) als auch Unterschätzung (z. B. durch die fälschliche Wahrnehmung einer Einschränkung der Privatheit) geschehen.

Auf einer allgemeineren Ebene stellt sich das Problem, dass alle menschlichen Handlungen (nicht nur sicherheitsrelevante) lediglich mit einem entsprechenden Hintergrundwissen verstanden werden können. Dieselbe Handlung (etwa eine bestimmte Geste) kann an unterschiedlichen Orten oder gegenüber verschiedenen Menschen ganz Unterschiedliches bedeuten. Während bei menschlichem Sicherheitspersonal ein solches Wissen zumindest potenziell vorausgesetzt werden kann, orientieren sich intelligente Systeme tendenziell an Äußerlichem und Häufigem. Seltene und ungewöhnliche – aber völlig legitime – Handlungen laufen Gefahr, ungerechtfertigter Weise verdächtig zu werden. Dies gilt es ebenfalls zu beachten, wenn Daten, die durch die intelligente Überwachung gewonnen wurden, in anderen Kontexten weiterverarbeitet oder mit anderen Daten zusammengeführt werden. Solche Daten müssen vor dem Hintergrund des Kontextes, dem sie entstammen und des Systems, mit dem sie gewonnen wurden, gesehen werden, um Fehlinterpretationen zu vermeiden. Schließlich ist zu beachten, dass verschiedene intelligente Überwachungssysteme auch unterschiedliche Daten produzieren. Die Daten können also nicht ohne Weiteres mit anderen Daten in Verbindung gebracht werden, ohne dabei zu berücksichtigen, mit welcher Technik und unter welchen Umständen diese gewonnen wurden.

5.1.11 Private Überwachung vs. öffentliche Überwachung

Unterschiedliche Standards, public-private-partnerships

Ein besonderes Problem ist, dass die intelligente Videoüberwachung gerade im privaten Bereich breit eingesetzt werden kann. Schon jetzt findet nur ein sehr geringer Anteil der sicherheitsrelevanten Videoüberwachung durch öffentliche Stellen statt. Der prominentere Einsatz durch nicht öffentliche Stellen entspricht hierbei nicht den strengen Kriterien des Einsatzes durch öffentliche Stellen (und muss dies auch nicht, siehe 5.2.2). Wie unter 4.2.2. beschrieben, herrschen in beiden Bereichen unterschiedliche Sensibilitäten für die Probleme der automatisierten Überwachung vor. Die Folgen der privaten Überwachung reichen jedoch nicht unbedingt so weit wie jene der staatlichen Überwachung. Dafür kann bei der privaten Überwachung, etwa bei der Überwachung am Arbeitsplatz, ein größerer ökonomischer oder sozialer Druck entstehen, gegen den eigenen Willen dem Einsatz von Überwachung zuzustimmen. Zudem ist zu bedenken, dass die Grenze zwischen öffentlicher und privater Überwachung verschwimmt. So haben öffentliche Stellen einzelfallabhängig Zugriff auf private Videoüberwachungsaufzeichnungen, beispielsweise im Zuge polizeilicher Ermittlungen.

Ebenso denkbar ist eine teilweise Übertragung von Sicherheitsaufgaben an Private, die intelligente Videoüberwachung in ihr Repertoire aufnehmen könnten. In diesem Kontext relevant sind die Bereiche der Flughafensicherheit, der Grenzsicherung und der ÖPNV.

Gerade wenn angenommen wird, dass mit potenziell invasiveren Technologien – wie der intelligenten Videoüberwachung – ein erhöhter Regelungsbedarf einhergeht, stellt die private Nutzung eine mögliche Gefahrenquelle für die Grundrechte dar. Hier gilt es Interaktionen zwischen dem Staat und Privaten (z. B. public-private-partnerships) genau zu untersuchen und sowohl rechtliche Regelungen für den privaten Einsatz als auch für die Weitergabe der Daten an öffentliche Stellen zu schaffen.

5.1.12 Szenarienbeschreibung

Zuverlässigkeit empirischer Daten, Zweckbindung, Komplexität
Anhand der Szenarien, die den Einsatz intelligenter Videoüberwachung beschreiben, findet oft eine Rechtfertigung der intelligenten Videoüberwachung statt. Diesbezüglich ist es wichtig, die Szenarien genau zu überprüfen. Die Komplexität der Wirklichkeit ist in Szenarien schwer einzufangen. Es können nicht-intendierte Folgen, eine größere Fehlerquote oder unberücksichtigte Diskriminierungen auftreten. Diese sind bei der Szenarienbeschreibung zu benennen und zu reflektieren. Des Weiteren sind empirische Daten über das Kriminalitätsaufkommen oder die erwarteten Effekte der Überwachung oft umstritten. Die Szenarien sollten außerdem nicht so vage formuliert werden, dass beliebige Überwachungszwecke in sie integriert werden können.

5.2 Aus rechtlicher Perspektive

5.2.1 Staatliche, insb. polizeiliche intelligente Videoüberwachung

5.2.1.1 Zulässigkeit staatlicher bzw. polizeilicher intelligenter Videoüberwachung nach geltendem Recht

Das Grundgesetz versagt dem Staat ein in Grundrechte eingreifendes Handeln, außer ein Gesetz sieht dies ausdrücklich vor. Dies erfordert sowohl das rechtsstaatliche Bestimmtheitsgebot als auch der im Demokratieprinzip und den Grundrechten wurzelnde Vorbehalt des Gesetzes. Momentan existieren im Bundespolizeigesetz sowie den Polizei- und Sicherheitsgesetzen der Länder Eingriffsgrundlagen, die der Polizei und teilweise auch den Sicherheitsbehörden herkömmliche Videoüberwachungsmaßnahmen zur Abwehr von Gefahren sowie zur Strafverfolgungsvorsorge gestatten. Dane-

ben sieht die Strafprozessordnung vor, dass die Polizei Verdächtige mittels Bildaufnahmen zur Aufklärung von erheblichen Straftaten observieren darf (§100 h StPO). Ferner richtet sich das Bundesdatenschutzgesetz an öffentliche Stellen, wenn es diesen in §6b erlaubt, etwa zur Wahrnehmung des Hausrechts, Videoüberwachung einzusetzen. Es zeigt sich, dass bereits durchaus Rechtsgrundlagen existieren, welche die staatliche Videoüberwachung vorsehen.

Allerdings stellen der Vorbehalt des Gesetzes und das Bestimmtheitsgebot keine geringen Anforderungen an diese Befugnisnormen. Sie sollen klar und präzise erkennen lassen, welche Maßnahmen von ihnen gedeckt sind, damit die staatlichen Stellen die Reichweite und die Grenze ihrer Handlungskompetenz kennen. Auf der anderen Seite sollen sich die Bürger auf die Eingriffe sowie deren Voraussetzungen und Gewicht einstellen können. Schließlich soll die Einführung neuer Eingriffsinstrumente dem parlamentarischen Gesetzgeber vorbehalten bleiben. Daran wird deutlich, dass die bestehenden Rechtsgrundlagen den Einsatz intelligenter Videoüberwachung nicht ohne vorhergehende und positiv geklärte Prüfung verfassungsgemäß vorsehen können.

Die Grundrechtsrelevanz einer Überwachungsmaßnahme entscheidet darüber, ob sie noch von einem Gesetz gedeckt ist. Dieser Parameter fungiert als grundrechtlicher „Belastungsindex" und ergibt sich daraus, wie tief, einschneidend und nachhaltig ein staatlicher Akt in Grundrechte eingreift. Der Wechsel von herkömmlicher zu intelligenter Videoüberwachung beeinflusst die Grundrechtsrelevanz direkt und indirekt.

Durch den technischen Fortschritt verändert sich, technisch-modal betrachtet, die Auswertung der Bilder von der visuellen Wahrnehmung eines menschlichen Operators hin zur automatisierten Analyse durch Software anhand zuvor festgelegter Algorithmen. Diesen Modus der Automatisierung hat das Bundesverfassungsgericht mehrfach als eingriffsintensivierend gewertet. Dies folge aus den stark effektuierten Möglichkeiten der Datenverarbeitung, die dank des automatisierten Modus in der Lage sei, große Datenmengen zu erfassen, zu rastern sowie diese miteinander zu verknüpfen. In staatlicher Hand resultiere aus diesem technischen Können eine Grundrechtsgefährdung, da auch sensible oder private Daten auf diesem Weg gewonnen oder verknüpft werden könnten. Die Erstellbarkeit von Persönlichkeitsprofilen wäre dann nicht ausgeschlossen. Aber sogar Informationen aus der Sozialsphäre, etwa Daten zu politischem Engagement, könnten in staatlicher Hand – nach der Lesart des Gerichts – Bürger einschüchtern und sie davon abhalten, ihre legitimen Freiheitsrechte wahrzunehmen. Auch mittelbar beeinträchtigt die Innovation die Situation der Grundrechte potenziell. Mit der leistungsstärkeren, automatisierten Auswertung wird es für die Polizei möglich, größere Räume und mehr Menschen zu überwachen. Somit stellt der technische Fortschritt eine sicherheitspolitische Innovation mit gesamtgesellschaftlicher Relevanz dar. Es muss also insgesamt von einer gegenüber der einfachen Videoüberwachung erhöhten Grundrechtsrelevanz ausgegangen werden. Dies bedeutet für die Zulässigkeit nach geltendem Recht, dass die momentanen Rechtsgrundlagen im Polizei- und

Sicherheitsrecht nicht ausreichen. Bis zu einem Angleichen der Rechtslage an die geänderten Erfordernisse wird dem Staat der Einsatz dieser Technologie versagt bleiben.

5.2.1.2 Grundrechtliche Grenzen des Einsatzes

Die Grundrechte des Grundgesetzes setzen staatlichem Handeln inhaltlich unterschiedliche Grenzen, welche die Rechtsgrundlagen zu beachten haben.

Nach weit verbreitetem Verständnis verletzen vor allem zwei Überwachungsmodi bzw. -ziele die Würde des Menschen (Art. 1 Abs. 1 GG). Beide Fallgruppen lassen sich dahingehend abstrahieren, dass Menschen durch übermäßig intensive Überwachung nur noch als Risiko behandelt werden. Zum einen verbietet die Achtung der menschlichen Würde eine flächendeckende Überwachung. Eine solche würde die Voraussetzungen eines autonomen Freiheitsgebrauches unzumutbar beeinträchtigen. Allerdings wird sich kaum abstrakt klären lassen, wann Überwachung „flächendeckend" ist, da dies eine Frage der kulturellen Prägung und des individuellen Empfindens ist. Diese Grenze nicht zu verletzen, ist angesichts der praktischen Möglichkeiten intelligenter Videoüberwachung kein bloß theoretisches Postulat. Zum anderen wird es als entwürdigend angesehen, wenn Informationen über Menschen in einer Art und Anzahl erhoben und verknüpft werden, dass „Persönlichkeitsprofile" erstellt werden könnten. Da mit Hilfe der intelligenten Videoüberwachung wohl nur schwerlich Daten erhoben werden können, die relevante Rückschlüsse auf den Mentalbereich zulassen, trägt dieses Tabu für eben jenen Bereich eher symbolischen Charakter. Jedoch dürfen Verknüpfungsmöglichkeiten nicht außer Acht gelassen werden. Problematische Qualitäten können erreicht werden, wenn etwa eine Person identifiziert und über einen längeren Zeitraum per Tracking verfolgt wird.

Das Grundrecht mit der größten theoretischen und praktischen Relevanz für das hier behandelte Thema ist das vom Bundesverfassungsgericht 1983 erkannte Recht auf informationelle Selbstbestimmung. Stark vereinfacht bedeutet dieses Konzept, dass die staatliche Erhebung persönlicher Informationen nie außer Verhältnis zu einem legitimen Ziel stehen darf. Die damit notwendige Verhältnismäßigkeitsprüfung lässt sich mit einem relationalen Dreieck strukturieren.

Die Beziehungen lassen sich schematisch wie folgt beschreiben:

Je größer das Produkt aus A) und B) ist, desto größer darf auch C) sein.

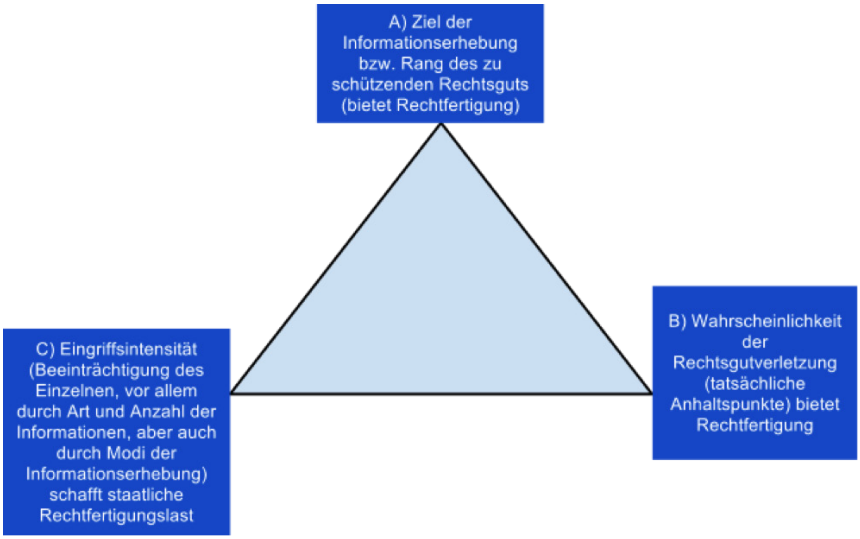
Je geringer das Produkt aus A) und B) ist, desto kleiner muss C) gehalten werden.

Je geringer B) ist, desto größer muss A) oder kleiner muss C) sein.

Je größer B) ist, desto geringer darf A) und desto größer darf C) sein.

Je geringer C) ist, desto geringer darf das Produkt aus A) und B) sein.

Je größer C) ist, desto größer muss das Produkt aus A) und B) sein.



Das Bundesverfassungsgericht hat in seiner Rechtsprechung zu Informationseingriffen eine ganze Reihe an Kriterien zur Bestimmung der Eingriffstiefe ausgemacht, die im Folgenden exemplarisch und vereinfacht aufgezählt werden: ein vom Grundrechtsträger zur Datenerhebung gegebener Anlass, die Streubreite der Erhebungsmaßnahme, die Quantität (Massenhaftigkeit) und Qualität der Daten, insbesondere die Sensibilität und Privatheit der Daten, die Heimlichkeit oder Offenheit der Datenerhebung, die Speicherung der Informationen und die Verknüpfung(-smöglichkeiten) der Daten.

Eine weitere grundrechtliche Grenze für die Sicherheitstechnik erwächst aus Art. 3 GG, welcher ungerechtfertigte Ungleichbehandlungen verbietet. Dies wird beispielsweise virulent, wenn es die neue Technik ermöglicht, gezielt Menschen anhand der Hautfarbe oder des Geschlechts zu erkennen. Diese Eigenschaften gehören zum Katalog verpönter Merkmale in Art. 3 Abs. 3 GG. Eine Detektion eben jener Merkmale in der Praxis unterläge erheblich gesteigerten Rechtfertigungsanforderungen, wäre also nur in sehr begründeten (Ausnahmefällen) zulässig.

Ein anderes Problem stellt die unbeabsichtigte Detektion von Menschen mit Behinderung dar. Mit manchen Krankheitsbildern mag es einhergehen, sich gar nicht „unauffällig“ bewegen zu können. Hier ist an die Diskussion über mittelbare Diskriminierung zu denken. Ob diese in einer solchen Situation angenommen werden kann, ist bereits fraglich. Um diese Konstellation zu bejahen, wird jedoch eine Benachteiligung von einem gewissen Gewicht gefordert. Als „Benachteiligung“ kommt hier der kurze, abklärende und noch folgenlose Operatorenblick in Betracht. Dieser Grundrechtseingriff wiegt nach den genannten Kriterien (siehe 5.2.1.1) nicht schwer, da er auf objektiv auffälliges Verhalten folgt, keine Informationen zutage fördert, die nicht bereits offen-

sichtlich wären, und keine Anschlussmaßnahmen nach sich zieht. Deutlich problematischer ist hingegen die gezielte Kontrolle und Beobachtung von Randgruppen, welche die neue Technik ermöglichen könnte.

5.2.1.3 Chancen für den Grundrechtsschutz durch die neue Technik

Die neue Technik kann nicht per se als Überwachungstechnik größerer Grundrechtsrelevanz angesehen werden. Intelligente Videoüberwachung kann gezielt auf eine auffällige Szene reagieren und muss nur für die Betroffenen dieser Szene durch die anschließende Überprüfung der Situation einen Grundrechtseingriff zur Folge haben. Herkömmliche Videoüberwachung ist dagegen ein vergleichsweise unpräzises Instrument, weil sie nur alle oder niemanden einem menschlichen Blick aussetzen kann, was zu einem Grundrechtseingriff führt. Voraussetzung für den schonenderen Einsatz ist aber, dass intelligente Videoüberwachung in „Reinform" eingesetzt wird – also nicht zusätzlich alle Bilder gespeichert werden oder ein Mensch zusätzlich das gesamte Bildmaterial auswertet. Bei dieser grundrechtsschonenden Einsatzmöglichkeit verringern sich in der Terminologie des Bundesverfassungsgerichts „Verdachtslosigkeit", „Massenhaftigkeit" und „Streubreite" der Maßnahme und so deren Eingriffsintensität. Die bundesverfassungsrichterliche Bewertung der beiden letztgenannten Kriterien wird jedoch in der Literatur bestritten.

5.2.1.4 Möglichkeiten des grundrechtskonformen Einsatzes

Um die intelligente Videoüberwachung als polizeiliches Instrument grundrechtsachtend und damit verfassungsgemäß einsetzen zu können, bedarf es eines Gesetzes. Dieses muss zweifelsfrei benennen, dass es die neue Technik erlaubt. Weiter müssen die Voraussetzungen und die Grenzen des Einsatzes für Anwender(innen) und Bürger(innen) klar erkennbar sein. Um ein hohes Maß an demokratischer Legitimation zu erreichen, empfiehlt es sich, die Anordnungskompetenz hierarchisch hoch anzusiedeln. Da die Rechtsgrundlage abstraktgenerell formuliert werden muss, bleibt für die einzelne Maßnahme noch ein Spielraum hinsichtlich ihres Ziels und der anzuwendenden Taktik. Dieser Spielraum ist in verhältnismäßiger Weise zu gebrauchen. Das bedeutet, dass die Modalitäten des Einsatzes in ihrer Grundrechtsrelevanz wie unter 5.2.1.2 skizziert, in ein Verhältnis zu den Beeinträchtigungen der Bürger gebracht werden müssen. Außerdem sind die weiteren grundrechtlichen Vorgaben an Organisation und Verfahren, wie Datensparsamkeit, Datensicherheit und Evaluationen der Maßnahmen sowie Hinweispflichten zu berücksichtigen.

5.2.2 Private intelligente Videoüberwachung

Die staatliche Videoüberwachung dient der Prävention und der Abwehr von Gefahren sowie der Strafverfolgung. Private setzen die Möglichkeiten der Videoüberwachungstechnologie jedoch seit jeher zum Schutz ihrer körperlichen Unversehrtheit, ihres Eigentums und der Kontrolle über ihren Machtbereich ein. Der Betrieb privater intelligenter Videoüberwachung ist also unter anderen als den im staatlichen Bereich vorherrschenden Aspekten zu bewerten.

5.2.2.1 Raumkategorien

Zunächst müssen die Räume, in denen private bzw. nicht öffentliche Stellen intelligente Videoüberwachungssysteme einsetzen, rechtlich erfasst werden. Die bietet sich bspw. auf privaten Grundstücken, in Einkaufszentren, Stadien, Museen, Tankstellen und vielen weiteren Bereichen an. Dabei nutzen Private die intelligente Videoüberwachung vor allem in Räumen, die dem Rechtsregime des öffentlichen Rechts entzogen sind, die jedoch zugleich als „öffentlicher Raum" oder „öffentlich zugänglicher Raum" bezeichnet werden. Denn mit „öffentlicher Raum" ist der öffentlich zugängliche Raum i. S. d. § 6b BDSG gemeint. Dieser kann sowohl in einem Gebäude als auch außerhalb liegen und steht einem unbestimmten oder lediglich bestimmbaren Kreis von Personen offen. Über die öffentliche Zugänglichkeit entscheiden dabei nicht die Eigentumsverhältnisse. Vielmehr ist die Entscheidung des Berechtigten, den Raum der Nutzung durch die Allgemeinheit zu öffnen, maßgeblich. Dies kann durch eine Zweckwidmung geschehen oder durch bestimmte Arten der Zugangsberechtigung, wie z. B. den Erwerb von Eintrittskarten oder das Erreichen bestimmter Altersgrenzen. Rechtlich teilweise ungeklärt ist die Einordnung von Räumen, die nur zu bestimmten Tageszeiten oder unter bestimmten Gegebenheiten von jedermann betreten werden können, ansonsten aber nur bestimmten Personen zugänglich sind. Beispiele hierfür sind Selbstbedienungsbereiche von Banken, die nach Ende der Öffnungszeiten nur mit Kunden- oder EC-Karte betreten werden können. Der Zutritt wird hier vorab durch Vertragsbestimmungen geregelt bzw. durch Kriterien bestimmt, die prinzipiell durch eine unbestimmte Vielzahl an Personen erfüllbar sind.

Gesondert zu erörtern ist der öffentlich-rechtlich überlagerte halb-öffentliche Raum. Dieser ist der Allgemeinheit zugänglich und der private Eigentümer hat die grundsätzliche Befugnis, über die Nutzung zu entscheiden. Aufgrund der besonderen öffentlichen Funktion dieses Raumes, müssen jedoch bestimmte Nutzungen zugelassen werden. Dies betrifft Räume, die zwar privatwirtschaftlich betrieben, aber in der öffentlichen Hand stehen, wie bspw. die meisten Bahnhöfe oder Flughäfen.

5.2.2.2 Besonderheiten des Privatrechts

Die Bewertung der intelligenten Videoüberwachung durch nicht öffentliche Stellen muss sich des Weiteren an den Besonderheiten des Privatrechts ausrichten. Dieses öffnet sich den Grundrechten als objektiver Wertordnung durch Generalklauseln, in denen die Wertentscheidungen des Grundgesetzes durch Auslegung zu berücksichtigen sind, während die Grundrechte unter Privaten nur mittelbar gelten. Ein wesentlicher Aspekt der Untersuchung der Zulässigkeit intelligenter Videoüberwachung durch nicht öffentliche Stellen ist aus diesem Grund die Abwägung der konfligierenden Interessen der Grundrechtsberechtigten in Dreieckskonstellationen.

Im Zentrum der privatrechtlichen Untersuchung stand § 6b BDSG, der im Zuge der Umsetzung der EG-Datenschutzrichtlinie 95/46/EG in das Bundesdatenschutzgesetz eingefügt wurde. Das Bundesdatenschutzgesetz verlangt für die Zulässigkeit der automatisierten Datenverarbeitung gem. des Verbots mit Erlaubnisvorbehalt aus § 4 BDSG entweder eine Einwilligung des Betroffenen oder eine gesetzliche Grundlage. § 6b BDSG normiert die Zulässigkeit der Videoüberwachung im öffentlich zugänglichen Raum, ohne zwischen der intelligenten und der herkömmlichen Form zu unterscheiden. Das Bundesdatenschutzgesetz und § 6b BDSG im Speziellen sind jedoch auf die intelligente Videoüberwachung als automatisierte Verarbeitung personenbezogener Daten anwendbar, da bereits das sekundärrechtliche Vorbild, die Datenschutzrichtlinie 95/46/EG, diese Form der Datenverarbeitung erfasst und der Wortlaut absichtlich weit gefasst ist, um technologischen Entwicklungen Rechnung zu tragen.

5.2.2.3 Rechtliche Zulässigkeit privater intelligenter Videoüberwachung

Da im Privatrecht die Grundrechte zumindest mittelbar Geltung erlangen müssen und der Gesetzgeber seinen grundrechtlichen Schutzpflichten entsprechen muss, ist für die Bewertung der intelligenten Videoüberwachung auf die zur herkömmlichen Videoüberwachung entwickelten Rechtsgrundlagen und deren Dogmatik abzustellen. Insofern relevant sind §§ 6a, 6b, 28, 32 BDSG, 823 Abs. 1, 1004 Abs. 1, 858 Abs. 1 BGB. Besonders in den Blick zu nehmen sind die im Privatrecht mittelbar geltenden Grundrechte aus Art. 2 Abs. 1 GG i. V. m. Art. 1 Abs. 1 GG und Art. 3 GG auf Seiten des Überwachten und Art. 12 Abs. 1 GG und Art. 14 Abs. 1 GG auf Seiten des Verwenders. Ebenso muss die Möglichkeit der ungerechtfertigten Ungleichbehandlung durch eine intendierte oder nicht-intendierte Anknüpfung an die Merkmale des Art. 3 Abs. 2, 3 GG und eine generelle Ungleichbehandlung nach Art. 3 Abs. 1 GG beachtet werden (siehe auch 5.2.1.2).

Die Verarbeitung personenbezogener Daten durch die intelligente Videoüberwachung ist zulässig, wenn der/die Betroffene einwilligt oder eine gesetzliche Grundlage die Überwachung zulässt. Die Einwilligung erscheint angesichts der technischen Komplexität der intelligenten Videoüberwachung, ihren mannigfaltigen Variationen, Einsatzmöglichkeiten und Zwecke sowie hinsichtlich der Praxistauglichkeit jedoch nicht tauglich. Im Zentrum der Untersuchungen durch MuViT-ReGI zur privaten intelligenten Videoüberwachung stand deshalb § 6 b BDSG, der die datenschutzrechtliche Garantie des Rechts auf informationelle Selbstbestimmung statuiert. Auf Private als nicht öffentliche Stellen sind § 6b Abs. 1 Nr. 2 BDSG, der die Videoüberwachung zur Wahrnehmung des Hausrechts normiert und § 6b Abs. 1 Nr. 3 BDSG, der die Videoüberwachung zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erfasst, anwendbar. Jeder Schritt der Verarbeitung personenbezogener Daten muss getrennt betrachtet werden, womit § 6b Abs. 1 BDSG für die Beobachtung und § 6b Abs. 3 BDSG für die Verarbeitung sowie Nutzung dieser Daten zu prüfen ist. Insbesondere hinsichtlich der die Überwachungsqualität auf eine andere Stufe hebenden Automatisierung ist § 6a BDSG einzubeziehen, der die automatisierte Datenverarbeitung regelt. § 6a BDSG verbietet Entscheidungen aufgrund automatisierter Verfahren, denen sich der Einzelne ausgeliefert und hilflos gegenüber fühlt, indem er die Verantwortung für die Rechtsfolge einer natürlichen Person auferlegt. Im Fokus des § 6a BDSG steht nicht die Verarbeitung der Daten, sondern deren Nutzung bzw. die Rechtsfolgen, die eine Verarbeitung und Nutzung der personenbezogenen Daten auslösen können. Die von MuViT-ReGI begleiteten Forschungsprojekte entwickelten System, die dem menschlichen Operator eine Vorauswahl an Bilddaten zur Verfügung stellt. Die algorithmische Datenanalyse assistiert somit bei der Vorbereitung der Entscheidung, die letztgültig jedoch im freien Ermessen des Menschen liegt, womit die wesentliche Voraussetzungen für eine Anwendung des § 6a BDSG auf die intelligente Videoüberwachung im Rahmen des Projektes MuViT nicht vorliegt. Allerdings sind die von § 6a BDSG präsentierten Wertungsgesichtspunkte hinsichtlich der veränderten Intensität und Gefahr einer automatisierten Datenverarbeitung bei der Beurteilung nach § 6b BDSG einzubeziehen.

Die Generalklauseln des § 6b Abs. 1 Nr. 2, 3 BDSG und §6b Abs. 3 BDSG eröffnen durch die unbestimmten Rechtsbegriffen wie „die Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke", „erforderlich" oder „schutzwürdige Interessen" erheblichen Auslegungsspielraum. Zum einen wird damit die benötigte Flexibilität gewährleistet, zum anderen geht mit der Offenheit zugleich Rechtsunsicherheit einher. Um diese Begriffe zu konkretisieren und Wertungsspielräume einzelfallbezogen auszufüllen, bieten sich die europarechtskonforme und verfassungskonforme Auslegung sowie die Topik an. Als Orientierungshilfen dienen die Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte, des Europäischen Gerichtshofs und der nationalen Gerichte zum Einsatz herkömmlicher Videoüberwachung durch Private. Die in diesen Entscheidungen zugrunde gelegten Normen und Topoi erlauben die Strukturierung der Zulässigkeitsprüfung. Die im Wege einer induktivdeduktiven Methode gewon-

nenen Kriterien sind im Bereich der Eingriffsprüfung der Personenbezug und die Einwilligung und auf Ebene der verhältnismäßigen Interessenabwägung die Automatisierung der Videoüberwachung, die Heimlichkeit der Maßnahme und notwendige Hinweispflichten, der konkrete Verdacht oder Anlass, die Art der verarbeiteten Daten, die technische Gestaltung des Systems und die zeitliche und räumliche Beschränkung sowie die Zahl der Betroffenen. Diese Topoi lassen sich im Rahmen der verhältnismäßigen Interessenabwägung auf die Besonderheit der privaten intelligenten Videoüberwachung übertragen und auf den konkreten Einzelfall anwenden. Mitberücksichtigt werden müssen zudem die datenschutzrechtlichen Grundsätze der Hinweispflicht, der Speicher- und Löschfristen sowie der Datenvermeidung und Datensparsamkeit. Zwingend ist darüber hinaus eine Vorabkontrolle nach § 4d BDSG.

Im Bereich des Datenschutzes ist im Zuge der zunehmenden Harmonisierung auf EU-Ebene das EU-Datenschutzrecht zu beachten, insbesondere die geplante EU-Datenschutzgrundverordnung. Diese würde bei Inkrafttreten unmittelbar in den Mitgliedstaaten gelten und das bislang geltende nationale Datenschutzrecht verdrängen. Auf nationaler Ebene wurden in jüngster Zeit Gesetzesänderungen zur Videoüberwachung im Bundesdatenschutzgesetz speziell zum Arbeitnehmerdatenschutz gekippt, nachdem die vorgeschlagene Regelung auf Kritik gestoßen ist. Inwiefern sich ein neues nationales Datenschutzgesetz im Hinblick auf die Verhandlungen auf europäischer Ebene noch sinnvoll realisieren lässt oder zu realisieren wäre, ist derzeit nicht absehbar.

5.2.3 Dual-Use

Die intelligente Videoüberwachung ist ebenso wie die meisten anderen, im Sicherheitsforschungsprogramm des BMBF entwickelten Techniken nicht allein im zivilen, sondern auch im militärischen Bereich einsetzbar. Dies gilt umso mehr, als die Grenzen zwischen innerer und äußerer Sicherheit, zwischen polizeilicher und militärischer Sicherheitsgewährleistung in vielerlei Hinsicht diffundieren. Dementsprechend findet auf diese Techniken die Dual-Use-Verordnung der Europäischen Union Anwendung (Ausnahme für „Software", die frei erhältlich oder allgemein zugänglich ist nach Dual Use-VO i. d. F. v. 5. Mai 2009, in der Anm. Allgemeine Software). Diese Verordnung fordert für Güter mit doppeltem Verwendungszweck eine Ausfuhrgenehmigung, die von den zuständigen nationalen Behörden zu erteilen ist. Nicht näher wird definiert, unter welchen Voraussetzungen von einem Gut mit doppeltem Verwendungszweck zu sprechen ist, sondern es werden in einer umfangreichen Anlage jene Güter gelistet, die dem Regelungsbereich der Verordnung unterfallen. Grundsätzlich ist davon auszugehen, dass Techniken der intelligenten Videoüberwachung dem Regelungsbereich der Verordnung unterfallen.

Werden die Güter mit doppeltem Verwendungszweck äußerst großzügig definiert, so bleiben die Kriterien für die Erteilung bzw. für die Verweigerung der Ausfuhrgenehmigung relativ vage. So regelt Art. 12 Abs. 1 Dual-Use-VO u. a., dass bei der Genehmigungsentscheidung „Überlegungen der nationalen Außen- und Sicherheitspolitik einschließlich solcher Aspekte, die vom Gemeinsamen Standpunkt 2008 / 944 / GASP betreffs der Ausfuhr von Militärgütern erfasst werden". Art. 2 Abs. 2 dieses Standpunktes nennt als Kriterium für die Ausfuhrgenehmigung u. a. „die Achtung der Menschenrechte und des humanitären Völkerrechts durch das Endbestimmungsland". Demgemäß kann die Ausfuhr verweigert werden, wenn die jeweilige Sicherungstechnik zur internen Repression benutzt werden würde. Nach dem Gemeinsamen Standpunkt umfasst der Begriff der internen Repression „unter anderem Folter sowie andere grausame, unmenschliche und erniedrigender Behandlung oder Bestrafung (...) und andere schwere Verletzungen der Menschenrechte und Grundfreiheiten, wie sie in den einschlägigen Menschenrechtsübereinkünften, einschließlich der Allgemeinen Erklärung der Menschenrechte und des Internationalen Pakts über bürgerliche und politische Rechte niedergelegt sind". Damit findet sich im Gemeinsamen Standpunkt ein recht robuster Maßstab für den Begriff der internen Repression.

Die Mitgliedstaaten sind darüber hinaus nach der genannten Vorschrift berechtigt, bei der Ausfuhrgenehmigung „alle sachdienlichen Erwägungen" anzustellen, was den nationalen Ermessens und Entscheidungsspielraum deutlich erweitert. Dies führt zu der Frage, ob und inwieweit die Wertungen des Grundgesetzes zu einer Anhebung des Menschenrechtsstandards bei der Genehmigungserteilung führen können. Zudem lässt sich überlegen, ob der Rückgriff auf Europäische Grundrechte zu einer derartigen Anhebung des Menschenrechtsstandards führen kann (vgl. insofern Anhang IIc, Teil 3,1.(1d) der Dual Use-VO i.d.F.v. 16. 11. 2011). Dabei geht es um die rechtliche (und ethische) Frage, ob die dem Grundgesetz zu Grunde liegende und vom Bundesverfassungsgericht ausdifferenzierte Balance zwischen Freiheit und Sicherheit oder ob die entsprechende Balance, wie sie vom Europäischen Gerichtshof für Menschenrechte entwickelt wird, Maßstab für die Anforderungen an die Freiheitlichkeit in den politischen Systemen anderer Staaten sein darf. Der völkerrechtliche Menschenrechtsschutz ist auf die Gewährleistung von Mindeststandards begrenzt. Der Export von Sicherheitstechnik kann in dieser Perspektive nur in notorische Überwachungsstaaten, die wiederholt wegen erheblicher Menschenrechtsverletzungen verurteilt worden sind, oder in Staaten ohne Mindestgarantien im Bereich des Grundrechtsschutzes verboten werden, wenn die fragliche Technik mit überwiegender Wahrscheinlichkeit unter Verstoß gegen einen Mindeststandard von Freiheitsschutz eingesetzt wird.

5.2.4 Internationaler Rechtsvergleich

Es bestehen signifikante Unterschiede zwischen den deutschen und den ausländischen Rahmensetzungen sowohl für die herkömmliche als auch für die intelligente Videoüberwachung.

a) Diese resultieren aus unterschiedlichen rechtlichen Konzepten des Schutzes der Privatheit im öffentlichen Raum und der Privatsphäre insgesamt. Während in Deutschland die Rechtsprechung des Bundesverfassungsgerichts seit mittlerweile 30 Jahren ein verfassungsrechtliches Konzept des Schutzes der Privatheit ausdifferenziert und dabei der sicherheitsrechtlichen Überwachung teils enge Grenzen gezogen hat, fehlt es fast vollständig an einer vergleichbaren Rechtsprechung ausländischer Verfassungsgerichte, soweit es sie denn überhaupt gibt. So schützt etwa die Rechtsprechung des Supreme Court der Vereinigten Staaten von Amerika die „reasonable expectations of privacy", geht aber davon aus, dass man im öffentlichen Raum nicht erwarten könne, vor Überwachungsmaßnahmen geschützt zu werden. Der Supreme Court war bislang nicht bereit, den von der amerikanischen Verfassungsrechtswissenschaft und von Teilen der öffentlichen Meinung eingeforderten stärkeren Schutz der Privatsphäre zur Rechtsprechungsleitlinie zu machen. Grund mag sein, dass der Verfassungstext wenig Anhaltspunkte für eine Intensivierung des Schutzes von Privatheit bietet. Auch war die Rechtsprechung der letzten Jahrzehnte, wohl wegen der personellen Zusammensetzung des Supreme Court, wenig geneigt, den Grundrechtsschutz durch Fortbildung des Verfassungsrechts zu stärken. Vergleichbares gilt für die Rechtsprechung des Obersten Gerichtshofes in Japan, des Verfassungsgerichts von Korea oder des Supreme Court von Kanada. Hier ist die Verfassungsmäßigkeit der Videoüberwachung ebenfalls noch nicht thematisiert worden und es gibt keinen umfassenderen Schutz der Privatheit. Nur der Conseil Constitutionel Frankreichs hat in zwei Entscheidungen die Verfassungsmäßigkeit der Videoüberwachung erörtert, ohne freilich engere Grenzen zu ziehen.

b) Soweit es keinen verfassungsrechtlichen Schutz von Privatheit gibt, bedarf es keiner gesetzlichen Grundlage für Überwachungsmaßnahmen. So kann in einer Vielzahl von Staaten eine Videoüberwachung sowohl in konventioneller als auch in intelligenter Form eingerichtet werden, ohne dass dafür eine demokratisch beschlossene gesetzliche Grundlage erforderlich wäre. Dies gilt etwa für die Vereinigten Staaten von Amerika, England und natürlich für all jene Staaten, die, wie etwa China, erst auf dem Weg zu einer demokratischen und rechtsstaatlichen Ordnung sind.

c) In einigen Staaten wird die Videoüberwachung zwar nicht explizit gesetzlich geregelt, muss aber – wie bspw. in Großbritannien – allgemeinen datenschutzrechtlichen Vorgaben entsprechen. Da es an einer bereichsspezifischen Rechtsgrundlage fehlt, findet in diesen Staaten ein eher schwacher rechtlicher Schutz gegen eine Ausdehnung von Videoüberwachung statt.

d) In den Mitgliedstaaten des Europarates – und damit praktisch in ganz Europa – regelt Art. 8 Abs. 1 der Europäischen Menschenrechtskonvention den rechtlichen Schutz vor Videoüberwachung. Das hier garantierte Recht auf Achtung des Privatlebens schützt die Privatsphäre auch im öffentlichen Bereich. Auf der Linie der Rechtsprechung des Europäischen Gerichtshofes für Menschenrechte liegt, dass eine Videoüberwachung nur auf gesetzlicher Grundlage statthaft ist. Obwohl es noch keine Entscheidungen zu den rechtlichen Voraussetzungen der Videoüberwachung gibt, hat die Venice-Kommission des Europarates in einem ausführlichen Gutachten die Anforderungen des Verhältnismäßigkeitsprinzips für die Einrichtung und den Betrieb von Videoüberwachungsanlagen trotzdem näher entwickelt. Es steht zu erwarten, dass der Europäische Gerichtshof für Menschenrechte diesen Anforderungen zumindest im Grundsatz folgen wird. Künftige Entscheidungen des Europäischen Gerichtshofs für Menschenrechte werden aller Voraussicht nach einen gemeineuropäischen Standard an rechtlichen Vorgaben schaffen, welche die Videoüberwachung, auch in ihrer intelligenten Form, betreffen. Darauf müssten alle europäischen Staaten reagieren, die bislang Videoüberwachung ohne gesetzliche Vorgaben praktizieren.

e) In einigen Staaten des angelsächsischen Rechtskreises ist Videoüberwachung zwar nicht gesetzlich geregelt, die Errichtung und der Betrieb von Videoüberwachungsanlagen müssen sich aber bisweilen nach ausführlichen verwaltungsinternen Richtlinien rechtfertigen lassen. Dies gilt etwa für den District of Columbia der Vereinigten Staaten von Nordamerika sowie für Australien. So verfügen die meisten australischen Städte über „Codes of Practice". Diese als Richtlinien erlassenen Regelwerke haben folgenden Inhalt: Angaben zum Grund der Videoüberwachung, Darstellung technischer Einzelheiten, Angaben zum Betreiber und zur Verwaltung der Videoüberwachungsanlage, Regelungen der Verantwortlichkeit und des Beschwerdeverfahrens. Eine Bestimmung der legitimen Gründe für eine intensivere Beobachtung einzelner Personen fehlt allerdings. In einigen Städten sind „Audit Committees" zur Kontrolle der Videoüberwachung eingerichtet. In Großbritannien hat der Datenschutzbeauftragte einen Kodex erarbeitet, der sowohl Behörden als auch Privaten als Leitlinie für die Videoüberwachung dienen soll.

In anderen Staaten, wie etwa in Frankreich oder in Spanien, werden die rechtlichen Rahmensetzungen der Videoüberwachung durch detaillierte Verfahrenssicherungen flankiert. Zu den Eckpunkten effektiver Verfahrenskontrolle gehören u. a. unabhängige, nicht unter staatlicher Aufsicht stehende Institutionen, die private und öffentliche Videoüberwachungsanlagen kontrollieren.

Dieser rechtsvergleichende Befund führt zu der Frage: Besteht ein vergleichbares Schutzniveau gegenüber der Videoüberwachung, wenn diese zum einen gesetzlich mit Rechtsschutzmöglichkeiten geregelt ist oder zum anderen, wenn diese sorgfältigen Verfahrenskontrollen unterliegt? Sicher hängt die Antwort auf diese Frage von der jeweiligen Rechtspraxis bzw. vom jeweiligen rechtskulturellen Kontext ab. Davon abgesehen, können umfassende verfahrensrechtliche Sicherungen zur Transparenz der

Entscheidungsprozesse, zur detaillierten Abarbeitung des Verhältnismäßigkeitsprinzips und damit zur Akzeptanz von Videoüberwachung führen.

f) In allen verglichenen Staaten stößt die Videoüberwachung auf eine breite Zustimmung der Bevölkerung. Zugleich gibt es einen relativ kleinen Bevölkerungsanteil, der die Videoüberwachung vehement ablehnt. Rahmenbedingungen für die Akzeptanz der Videoüberwachung waren Erfolge bei der Aufklärung schwerwiegender Straftaten, auch im Bereich des Terrorismus, eine Erhöhung des individuellen Sicherheitsgefühls sowie eine hinreichende Kontrolle der (rechtlichen) Rahmenbedingungen.

Im Gegensatz dazu wird die Videoüberwachung in der internationalen veröffentlichten politischen und rechtlichen Diskussion zum Teil heftig kritisiert. Die wesentlichen Kritikpunkte sind: Die Videoüberwachung verhindere keine Straftaten, könne Minderheiten diskriminieren, führe zu angepasstem Verhalten, münde bei Vernetzung mit anderen Überwachungssystemen in neue Formen staatlicher Repression und könne zu persönlichen oder ökonomischen Zwecken missbraucht werden. Der positiven Einschätzung im kollektiven Bewusstsein steht damit eine weitgehende Ablehnung der Videoüberwachung in der veröffentlichten politischen Meinung entgegen.

g) Wirft die intelligente Videoüberwachung in der deutschen verfassungsrechtlichen Diskussion eine Reihe von Zweifelsfragen auf, so lassen sich in rechtsvergleichender Perspektive entsprechende Bedenken kaum erkennen, ist doch in Deutschland ein besonders hohes Niveau des Privatsphärenschutzes erreicht und verfassungsrechtlich bzw. verfassungsgerichtlich gesichert. So bedürfen denn die neuen Formen einer intelligenten Videoüberwachung im Ausland vielfach keiner rechtlichen Grundlage, um sie einzuführen. Davon abgesehen können die im Ausland praktizierten Verfahrenssicherungen ohne Schwierigkeiten auch auf die intelligente Videoüberwachung angewendet werden.

6 Checkliste

Die Fragen der Checkliste sollen die wichtigsten Aspekte abdecken, die im Zusammenhang mit der Technikentwicklung, dem Technikeinsatz, der Forschungsförderung und der politischen Entscheidung über den Technikeinsatz beleuchtet und bedacht werden sollten. Die übrigen Teile der Handreichung bieten Hintergründe und theoretische Grundlagen für die Beantwortung der Fragen. Bei jeder Frage wird auf die Abschnitte der Handreichung verwiesen, welche die erwähnten Aspekte genauer erläutern. Weder die Fragen noch die theoretischen Grundlagen sind erschöpfend. Sie können nur Hilfen für die anstehenden Entscheidungen sein. Bei der Entscheidung über Entwicklung und Anwendung müssen der Sache nach auch die Fragen der Technikentwicklung und Anwendung selbst berücksichtigt werden. Auf jeden Fall kann es für alle Bereiche sinnvoll sein, die jeweils anderen Frageblöcke zur Kenntnis zu nehmen.

6.1 Technikentwicklung

1.) Bei lernenden Systemen: Wer kontrolliert, was gelernt wird? Wie häufig erfolgt eine Kontrolle? Kann manuell korrigiert werden? (5.1.4, 5.1.6, 5.1.10)

2.) Werden Rechtswissenschaften, Ethik und Stakeholder(innen) am Entwicklungsprozess beteiligt? (5.1.8)

3.) Wird die Technik so gestaltet, dass ihre Funktionsprinzipien leicht transparent zu machen sind? Ist die Technik mit geringem Vorwissen verständlich? (5.1.4, 5.1.8)

4.) Wird die Technik so gestaltet, dass die Privatheit der Überwachten so gut wie möglich geschützt werden kann (privacy by design)? Hierzu gehören etwa die Verschlüsselung der Daten, Datensparsamkeit und datenspezifische Zugriffsrechte für unterschiedliche Personen. (5.1.9, 5.2.1.4)

5.) Wurde versucht, schon auf der Technikebene einen Missbrauch der Technik für inakzeptable Zwecke zu verhindern? Wird nur mit Projektpartner(inne)n zusammen gearbeitet, bei denen zu erwarten ist, dass der Gebrauch zu unmoralischen Zwecken ausbleibt und kein Verkauf an Personen stattfindet, welche die Technik unmoralisch einsetzen könnten? (5.1.1, 5.1.3)

6.) Wurde überprüft, ob die Technik nicht-intendierte Diskriminierungen verursachen könnte oder absichtliche Diskriminierungen zulässt? (5.1.5, 5.2.1.2)

7.) Sind die Verantwortlichkeiten klar definiert? Wer haftet? (5.1.4) Inwiefern übernimmt die Technikentwicklung Verantwortung für technische Fehler und den Missbrauch der Technik? (5.1.3)

8.) Ist die Technik klar für ein Einsatzszenario entworfen worden oder soll sie auch in anderen Kontexten verwendet werden? Wurden die Probleme der Anwendung in verschiedenen Kontexten analysiert? (5.1.1, 5.1.10)

9.) Welche Abweichungen werden vom System gemeldet, ohne dass diese ein Sicherheitsrisiko darstellen (false positives)? Kann es hierdurch zu Diskriminierungen (5.1.5, 5.2.1.2), unbeabsichtigten Normalisierungen (5.1.6) oder Privatheitsverletzungen (5.1.9) kommen?

10.) Welche Möglichkeiten gibt es für die Anwender(innen), Probleme zu melden und Fehler zu korrigieren? (5.1.5, 5.1.10)

6.2 Technikanwendung

1.) Ist der Zweck der Videoüberwachung hinreichend klar festgelegt und gerechtfertigt? Ist zu erwarten, dass sich die Begründung oder das primäre Ziel für die Überwachung später ändert (function creep)? Wurden alle Stakeholder (insbesondere die von der Überwachung Betroffenen) bei der Ausgestaltung der Technikanwendung berücksichtigt? Geht es „nur" um die Verbesserung des subjektiven Sicherheitsgefühls

oder auch um die Verbesserung der objektiven Sicherheit? Wird Akzeptanz angestrebt oder Akzeptabilität? Hat eine Risikokommunikation stattgefunden? (5.1.1, 5.1.3, 5.1.8, 5.1.12)

2.) Wurden alternative Lösungsansätze (auch im Hinblick auf die Kosten des Technikeinsatzes) berücksichtigt? (5.1.2)

3.) Ist das geplante Einsatzszenario empirisch ausreichend untersucht (Kriminalitätsbrennpunkt, Risikoabschätzung, Effizienzabschätzung der Sicherheitsmaßnahme)? (5.1.12, 5.2.1.2)

4.) Ist das Sicherheitspersonal in Bezug auf Diskriminierungen und die Interpretation der Ausgaben des Systems geschult worden? (5.1.4, 5.1.5)

5.) Sind die Folgen von Fehlalarmen (false positives) bedacht worden? (5.1.6, 5.1.10)

6.) An welchen Stellen kann es zu Diskriminierungen durch die Technik kommen (5.2.1, 5.2.1.2)? Durch welche Eingriffe können Diskriminierungen behoben werden? Wer kann diese durchführen und wie aufwändig sind sie? (5.1.5)

7.) Inwiefern weichen private Technikeinsätze von öffentlichen Standards ab und ist dies rechtfertigbar? (5.1.11, 5.2.2)

8.) Werden Betroffene oder Betroffenengruppen transparent über das Stattfinden der intelligenten Videoüberwachung und ihre Funktionsweise informiert? (5.1.8c, 5.2.1.4, 5.2.2.3)

9.) Sind die Verantwortlichkeiten für Entscheidungen und Fehler auf Grundlage der intelligenten Videoüberwachung klar definiert? (5.1.4)

10.) Werden durch die Videoüberwachung unauffällige, „normale" Verhaltensweisen nahe gelegt oder erzwungen, die nicht unbedingt intendiert waren? Welche Verhaltensweisen werden unterbunden? (5.1.6)

11.) Gibt es im vorliegenden Anwendungsort besondere Merkmale zu berücksichtigen? Handelt es sich etwa um einen öffentlich zugänglichen Ort, an dem das öffentliche Leben oder sogar die politische Betätigung eingeschränkt werden könnte? (5.1.8d, 5.1.10, 5.1.11, 5.2.2.1)

12.) Wird der Eingriff in die Privatsphäre minimiert (Datensparsamkeit)? Wird auf die Möglichkeit der Personenerkennung so weit wie möglich verzichtet? Gibt es unterschiedliche „Gefahrenstufen" mit unterschiedlich starken Privatheitseingriffen? Wird der Zugriff auf die Daten beschränkt und nur an jeweils autorisierte Personen gestattet? Werden die Daten verschlüsselt? Wird eine Nutzung nur für den vorgesehenen Zweck sichergestellt? (5.1.9, 5.2.1.2, 5.2.2)

13.) Durch wen wird die Funktion des Systems kontrolliert? Wie häufig geschieht dies? (5.1.5)

6.3 Entscheidungen über Entwicklung und Anwendung

6.3.1 Entscheidung über Entwicklung und Forschung (auch Forschungsförderung)

1.) Besteht die Möglichkeit, die Technik anders einzusetzen als vom geförderten Forschungsvorhaben geplant? Ist die Technik nur zivil oder auch militärisch nutzbar? Ist eine solche Nutzung zu erwarten? Ist der Export der Technologie in Länder wahrscheinlich, die diese Technik in moralisch und rechtlich problematischer Weise einsetzen könnten (5.3.)? Sind Projektpartner an der Forschung beteiligt, die die Technik in militärischen Zusammenhängen oder in moralisch und rechtlich problematischer Weise verwenden könnten? Gibt es Möglichkeiten, die Proliferation zu kontrollieren? (5.1.3)

2.) Ist die Technik dazu geeignet, die im Forschungsvorhaben beschriebenen Problemszenarien zu lösen? Handelt es sich um realistische Problemszenarien? Gibt es alternative Ansätze der Problemlösung? (5.1.12, 5.1.2)

3.) Besteht bei den Beteiligten am Forschungsvorhaben ein Problembewusstsein für ethische und rechtliche Konflikte?

4.) Kann die Technik so entwickelt werden, dass mögliche ethische und rechtliche Probleme abgeschwächt oder gelöst werden?

5.) Welche Normalitätsstandards sind technisch implementiert? Können diese Standards Lebensbereiche normalisieren, die pluralistisch bleiben sollten? (5.1.6)

6.) Welchem Zweck soll die Technik dienen? Ist der Zweck gut gerechtfertigt? Ist zu erwarten, dass Zwecke verfolgt werden könnten, die nicht explizit genannt werden? (5.1.1, 5.1.3, 5.2.2.3)

7.) Gibt es alternative Lösungsansätze zur Erfüllung des Zwecks, die sozial verträglicher sind? (5.1.2)

8.) Werden bei der Entscheidung über die Forschungsförderung Stakeholder (insbesondere Betroffene oder Betroffenenverbände) beteiligt? (5.1.8)

9.) Werden bei der Technikentwicklung Ethik und Recht beteiligt? (5.1.8, 5.2)

10.) Wird die Technik so entwickelt, dass Privatheitsschutz schon in das Design mit integriert wird (privacy by design)? Gibt es bereits Standardtechniken für privacy by design auf diesem Gebiet und werden diese berücksichtigt? Soll die Technik in Kombination mit anderer Technologie eingesetzt werden (etwa Gesichtserkennung oder Drohnen) wodurch es zu stärkeren Eingriffen in die Privatsphäre kommen kann? (5.1.9, 5.2, 5.3)

11.) Soll die Technik so entwickelt werden, dass sie auch für Laien verstehbar ist (transparency by design)? (5.1.8c, 5.2.2.3)

12.) Besteht die Sensibilität für einen nicht-intendierten oder intendierten diskriminierenden Gebrauch? (5.1.5, 5.2.1.2, 5.2.2)

13.) Wird bei der Entwicklung berücksichtigt, dass ein Technikdesign ungeeignet für unterschiedliche Kontexte sein kann? Woher stammen die Informationen über den geplanten Einsatzkontext? (5.1.10)

14.) Werden Fragen der Verantwortung der Technikentwicklung für Fehler und Missbrauch der Technik gestellt und beantwortet? (5.1.4)

6.3.2 Entscheidung über Anwendung/Einsatz der Technik

1.) Ist der Zweck der Videoüberwachung hinreichend gerechtfertigt (5.2.1.2, 5.2.2)? Ist zu erwarten, dass die Überwachung später anders verwendet wird als während der Einführung gedacht (function creep)? (5.1.1)

2.) Wurden alle Stakeholder (insbesondere die von der Überwachung Betroffenen) bei der Ausgestaltung der Technikanwendung berücksichtigt? Geht es „nur" um die Verbesserung des subjektiven Sicherheitsgefühls oder auch um die Verbesserung der objektiven Sicherheit? Wird Akzeptanz angestrebt oder Akzeptabilität? Hat eine Risikokommunikation stattgefunden? (5.1.1, 5.1.8, 5.1.12)

3.) Wurden alternative Lösungsansätze (auch im Hinblick auf die Kosten des Technikeinsatzes) ernsthaft berücksichtigt? (5.1.2.3.) Ist das geplante Einsatzszenario empirisch ausreichend untersucht (Kriminalitätsbrennpunkt, Risikoabschätzung, Effizienzabschätzung der Sicherheitsmaßnahme)? (5.1.12, 5.1.1.2)

4.) Wird das Sicherheitspersonal in Bezug auf Diskriminierungen und die Interpretation der Ausgaben des Überwachungssystems geschult? (5.1.4, 5.1.5, 5.2.1.2)

5.) An welchen Stellen kann es zu Diskriminierungen durch die Technik kommen (5.2.1.2)? Wie und von wem können diese Probleme behoben werden? (5.1.5)

6.) Inwiefern weichen private Technikeinsätze von öffentlichen Standards ab und ist dies rechtfertigbar? (5.1.11, 5.2.2)

7.) Werden Betroffene oder Betroffenengruppen transparent über das Stattfinden der automatisierten Videoüberwachung und ihre Funktionsweise informiert? (5.1.8c)

8.) Sind die Verantwortlichkeiten für Entscheidungen und Fehler auf Grundlage der automatisierten Videoüberwachung klar definiert? (5.1.4)

9.) Werden durch die Videoüberwachung unauffällige, „normale" Verhaltensweisen nahe gelegt, die nicht-intendiert waren? (5.1.6)

10.) Gibt es im vorliegenden Anwendungsort besondere Merkmale zu berücksichtigen? Handelt es sich etwa um einen öffentlich zugänglichen Ort, an dem das öffentliche Leben oder sogar die politische Betätigung eingeschränkt werden könnte? (5.1.8d, 5.1.10, 5.1.11, 5.2.2, 7.1.2)

11.) Wird der Eingriff in die Privatsphäre minimiert (Datensparsamkeit)? Wird auf die Möglichkeit der Personenerkennung soweit wie möglich verzichtet? Gibt es unterschiedliche „Gefahrenstufen" mit unterschiedlich starken Privatheitseingriffen? Wird der Zugriff auf die Daten beschränkt und nur jeweils autorisierten Personen gestattet? Werden die Daten verschlüsselt? Wird eine Nutzung nur für den vorgesehenen Zweck sichergestellt? (5.1.9, 5.2.1, 5.2.2)

12.) Wer trägt die Kosten der Überwachung (finanziell und sozial)? Wem nutzt sie? (5.1.5)

7 Aspekte zur Bewertung der Szenarien

7.1 Marktplatz

Der Marktplatz der Großstadt S gilt als Kriminalitätsschwerpunkt. Vor allem nachts ist er Schauplatz für Drogengeschäfte. Auch Passant(inn)en wurden schon tätlich angegriffen. Daher soll ein intelligentes Videoüberwachungssystem eingerichtet werden, das offen installiert nahezu jeden Winkel des Marktplatzes erfassen soll. Die für den Drogenhandel typischen Bewegungsabläufe, Schlägereien sowie am Boden liegende Personen sollen erkannt werden. Bei jedem „Treffer" überprüft ein menschlicher Operator die Szene und alarmiert die nächste Polizeistreife zur Nachschau.

7.1.1 Aspekte zur ethischen Bewertung des Szenarios

Bei der Lösungsskizze zum Marktplatzbeispiel wird ein Schwerpunkt auf die politische Entscheidung über den Einsatz gelegt. Für die politische Entscheidung ist insbesondere die Rechtfertigung des Technikeinsatzes maßgeblich. Grundlage hierfür ist die Beschreibung des Einsatzszenarios (siehe 5.1.12). Es ist zu prüfen, ob es sich wirklich um einen Kriminalitätsschwerpunkt handelt, um welche Delikte es sich handelt und was die Ursachen für die Kriminalitätsentwicklungen sind. Anschließend ist die Zielsetzung (siehe 5.1.1) zu überprüfen. Während die Verhinderung von Angriffen oder Diebstählen anzustreben ist, ist die Unterbindung von Drogenhandel schwieriger zu bewerten. Durch Videoüberwachung kann Drogenhandel verdrängt, aber nicht verhindert werden. Bei der Zielsetzung stellt sich somit die Frage, ob nicht versteckte andere Ziele, wie die Aufwertung des Marktplatzes für die Wirtschaft, eine tragende Rolle spielen.

Zentral für die ethische Bewertung ist zudem das Nachdenken über alternative Lösungsansätze (siehe 5.1.2). Auch wenn Drogenhandel gesetzlich verboten ist, existiert eine lang anhaltende ethisch-politische Diskussion darüber, dass erst die Kriminalisierung jene Probleme hervorbringe, die mit Drogenhandel und Drogenkonsum in Verbindung gebracht werden. Während die technische Lösung durch die intelligente

Videoüberwachung eher bei den Symptomen ansetzt und die Situation als Sicherheitsproblem einordnet, könnte die Betrachtung als gesellschaftliches Problem dazu führen, dass die Duldung oder die Legalisierung des Drogenhandels vorgenommen wird und damit die Ursachen für gesellschaftliche Konflikte behandelt würden. Weniger drastische alternative Lösungsansätze beinhalten präventive, soziale Maßnahmen und eine bessere Betreuung von Drogenabhängigen (etwa Fixpunkte oder Sozialarbeiter). Für ein erhöhtes subjektives Sicherheitsgefühl der Marktplatznutzer(innen) können Aufklärungskampagnen und Bürger(innen)beteiligungen erwogen werden. Dies ist auch entscheidend für den Übergang von Akzeptanz zu Akzeptabilität (siehe 5.1.8b). Während Videoüberwachung und Kriminalitätsbekämpfung hohe Zustimmungsraten haben, kann diese Zustimmung auf falschen Annahmen aufgebaut sein. Bei der demokratischen Reflexion auf den Technikeinsatz sind insbesondere Betroffene der Maßnahmen einzubinden (siehe 5.1.8a). Zu den Stakeholdern gehören allgemein die überwachte Öffentlichkeit und insbesondere jene Personen, die im Zusammenhang mit dem Drogenhandel stehen. Eine weitere Schwierigkeit stellt die Transparenz der Technik und der Überwachungsmaßnahme dar (siehe 5.1.8c). Hier sollte eine intelligente Videoüberwachungstechnik gewählt werden, die in ihrer Funktionsweise nachvollziehbar gestaltet ist. Informationsbroschüren und ein öffentlich-medial geführter Diskurs sind hilfreich, um Grundlagen für die Diskussion über den Einsatz zu schaffen.

Neben den allgemeineren politischen Überlegungen über die Zielsetzung, die Alternativen und das demokratische Verfahren, spielen auch konkretere Probleme im Zusammenhang mit der Gestaltung von Technik und Technikeinsatz eine große Rolle.

Ein Grundproblem beim Einsatz intelligenter Videoüberwachung an einem öffentlichen Ort wie dem Marktplatz ist die große Streubreite der Betroffenen. Nur eine kleine Personengruppe soll identifiziert werden, dafür aber ist die Überwachung einer besonders großen Gruppe an einem öffentlich zugänglichen Platz notwendig, wodurch die Freiheit vieler Menschen betroffen ist (siehe 5.1.7). Es wird in die Privatheit vieler Menschen eingegriffen, selbst wenn versucht wird, diesen Eingriff durch die intelligente Technik zu minimieren (siehe 5.1.9). Ein besonderes Problem bei von vielen unterschiedlichen Menschen genutzten Orten ist die „Normalisierung" (siehe 5.1.6). Unter dem Überwachungsdruck kann eine Neigung der Menschen nicht ausgeschlossen werden, sich verstärkt an eine vorgestellte Normalität anzupassen, um nicht aufzufallen. Dies kann an öffentlichen Orten wie dem Marktplatz die Freiheit stark einschränken. Darüber hinaus kann die Bereitschaft für politische Betätigungen eingeschränkt werden (siehe 5.1.8d). Der Einsatz intelligenter Videoüberwachung an solchen öffentlichen Orten ist daher hochproblematisch und alternative Lösungsansätze sind zu bevorzugen.

Neben dem Problem, dass eine große Menschengruppe überwacht wird, kann die Überwachung an einem Marktplatz für Minderheiten problematisch werden. „Problematische" Normalitätsabweichungen können von „unproblematischen" Abweichungen an inhomogenen Orten nicht trennscharf unterschieden werden. Es kann

zu Diskriminierungen von Menschen mit Gehbehinderungen, herumhängenden Jugendgruppen, Obdachlosen usw. kommen (siehe 5.1.5). Allgemein muss festgehalten, werden, dass ein zuverlässiges technisches System im Vorfeld besonders schwer herzustellen ist, da auf einem Marktplatz viele unterschiedliche Kontexte und Kulturen zusammentreffen (siehe 5.1.10).

7.1.2 Aspekte zur rechtlichen Bewertung des Szenarios

Die heutigen Polizeirechtsgesetze sehen fast durchweg Rechtsgrundlagen für die Videoüberwachung von Kriminalitätsschwerpunkten vor. Nach hier vertretener Ansicht erlauben diese der Polizei nur die herkömmliche Videoüberwachung, also Überwachung ohne eine automatisierte Analyse des Bildmaterials. Gesetze, die Grundrechtseingriffe erlauben sollen, müssen normenklar und bereichsspezifisch formuliert sein. Daraus folgt das Gebot einer präzisen Beschreibung dessen, was das Gesetz erlauben soll. Es sprechen gute Gründe dafür (siehe 5.2.1.1), von einer anderen Grundrechtsrelevanz intelligenter Videoüberwachung gegenüber der herkömmlichen Form auszugehen. Da die Grundrechtsrelevanz das wichtigste Kriterium ist, um die Gebote der Normenklarheit und der Bereichsspezifik (siehe 5.2.2.1) handhabbar zu machen, ist davon auszugehen, dass intelligente Videoüberwachung im Lichte dieses Kriteriums ein anderes Instrument ist als die herkömmliche Form. Die geltende Gesetzeslage lässt das Szenario somit nicht zu.

Eine entsprechende Rechtsgrundlage für das polizeiliche Handeln in diesem Szenario ist also erst noch zu schaffen (siehe 5.2.1.4). Diese muss klar benennen, dass der Polizei auch gestattet wird, durch Videoüberwachung gewonnenes Bildmaterial automatisiert auszuwerten. Gut vorstellbar ist, dass schon das Gesetz Abstufungen vornimmt, um die unterschiedliche Grundrechtsrelevanz der verschiedenen intelligenten Anwendungen zu berücksichtigen und damit korrespondierend die Voraussetzungen zu staffeln (siehe 5.2.1.2). So wird es beispielsweise guter Gründe bedürfen, biometrische Daten zu Identifizierungszwecken abzugleichen. Abstrakt formuliert, dürfte dafür die bezweckte Abwehr einer konkreten Gefahr für ein bedeutendes Rechtsgut zu fordern sein. Weiter sind die tatsächlichen Voraussetzungen und die Grenzen für die einzelne Maßnahme präzise zu fassen. Dazu gehört neben den erforderlichen Erkenntnissen über eine Gefahrenlage auch, wie mit den erhobenen Bilddaten zu verfahren ist und wer die Maßnahme anordnen darf. Im Beispielsszenario liegen aufgrund der Erfahrungen mit Drogenhandel und Gewaltdelikten tatsächliche Anhaltspunkte vor, die auf einen kriminogenen Ort schließen lassen.

Liegen die Voraussetzungen der Rechtsgrundlage vor, so stellt diese es in das Ermessen der Polizei, ob und wie im Einzelfall ein intelligentes Videoüberwachungssystem eingesetzt werden soll. Dieses Ermessen ist jedoch keineswegs frei, sondern muss ins-

besondere dem Grundsatz der Verhältnismäßigkeit Rechnung tragen (siehe 5.2.1.2). Vereinfacht läuft dies darauf hinaus, dass die mit der Maßnahme einhergehende Belastung der Bürger(innen) nicht außer Verhältnis zu den mit der Maßnahme verfolgten Zielen stehen darf. Im vorliegenden Szenario soll das System Bewegungsmuster erkennen, die auf Drogenhandel oder Handgreiflichkeiten schließen lassen. Außerdem sind die Algorithmen so konfiguriert, dass am Boden liegende Menschen einen Alarm auslösen sollen. Da das Szenario keine grundsätzliche Aufzeichnung der Bilddaten vorsieht, ist die Belastung für die zwar analysierten, aber nicht als relevant detektierten Personen minimal. Über sie bleiben keine Daten erhoben. Eine Belastung in Form eines Grundrechtseingriffs ergibt sich für die Personen, die der Nachschau des Operators unterzogen werden, weil sie selbst oder als Passant(in) einer Szene als relevant eingestuft wurden.

Um die Intensität des Grundrechtseingriffs zu bemessen, weist die Rechtsprechung des Bundesverfassungsgerichts etliche Faktoren auf, die den Eingriff schärfen oder mildern (siehe 5.2.1.1). Von diesen sind hier mildernd zu berücksichtigen, die Offenheit der Maßnahme sowie die Beschränkung der Nachschau auf einen reaktiven Modus, d. h. es werden nur die Personen betroffen, die selbst einen Anlass gaben oder sich räumlich und zeitlich in der Nähe des Anlasses befanden. Weniger gravierend sind die Daten hinsichtlich ihrer Persönlichkeitsrelevanz einzuschätzen, weil regelmäßig mit Aufenthaltsort und -zeit sowie dem aktuellen Verhalten nur Informationen gewonnen werden, die im öffentlichen Raum offenkundig sind. Außerdem lassen sie wenig bis kaum Rückschlüsse auf die psychische und physische Konstitution sowie innere Überzeugungen oder wirtschaftlich relevanten Kriterien zu. Die zu gewinnenden Beiträge zu Persönlichkeitsprofilen halten sich in engen Grenzen.

Schärfend ist allerdings der automatisierte Modus zu gewichten. Die automatisierte Analyse bringt gegenüber der visuellen Auswertung neue Risiken mit sich. Die Digitalisierung der Daten lässt diese abgleichbar und verknüpfbar werden. Auch ist negativ zu bemerken, dass keine Vorkehrungen ersichtlich sind, die eine Identifizierbarkeit der Betroffenen auf das tatsächlich notwendige Minimum reduzieren. Schließlich wäre negativ einzuordnen, wenn das System häufig Fehlalarme produzieren würde. Dies führte zu einem erhöhten Risiko, in den Operatorenfokus zu geraten, ohne dazu selbst Anlass gegeben zu haben. Zwei weitere Aspekte sind darüber hinaus problematisch: Flächendeckende Überwachung wird nach zutreffender herrschender Meinung als unzulässig angesehen, wobei sich dieses Tabu einer klaren räumlichen Definition entzieht. Hier wird zwar der Marktplatz lückenlos erfasst, dieser dürfte jedoch gemessen am Stadtgebiet bzw. der Innenstadt einen noch überschaubaren Anteil ausmachen. Allerdings ist die kommunikative Dimension eines zentralen öffentlichen Platzes nicht zu unterschätzen. Diese Problematik sei hier aber nur angedeutet. Daneben ist zu erörtern, dass ein Zielraster aus liegenden Personen besteht. Dies stellt kein strafrechtlich relevantes Verhalten dar. Dieses Muster kann gleichermaßen auf eine gestürzte wie auf eine „herumlungernde“ Person hindeuten. Im ersteren Fall dient das Zielmuster

der Gefahrenabwehr, weil verunglückte Personen schnell ausgemacht werden sollen. Bei der zweiten Variante stünde eher die Verwirklichung einer bestimmten Vorstellung von Stadtbild und Ordnung im Vordergrund.

Mit der Maßnahme werden verschiedene Ziele verfolgt. Den Drogenhandel zu bekämpfen, dient dem Rechtsgut Volksgesundheit. Die hohen Strafandrohungen für Delikte nach dem Betäubungsmittelgesetz legen die Wertung nahe, dass dieser Aspekt als hohes Rechtsgut anzusehen ist. Da es auch schon zu tätlichen Zwischenfällen kam, soll die Überwachung auch helfen, diese durch Abschreckung zu unterbinden, oder zumindest schnell interagieren zu können. Diesbezüglich sind Leib und Leben unzweifelhaft hohe Rechtsgüter. Diese Überlegungen greifen ganz ähnlich für das Erkennen von liegenden Personen, sofern dieses nicht dazu genutzt wird, auch in Fällen ohne Gesundheitsgefährdung zu interagieren. Insofern sollen hier durchaus hochrangige Rechtsgüter geschützt werden. Dies geschieht auch nicht aufgrund bloßer Vermutungen, sondern weil die Vergangenheit gezeigt hat, dass der Marktplatz als abstrakt gefährlicher Ort für diese Rechtsgüter anzusehen ist. Danach darf insgesamt davon ausgegangen werden, dass das skizzierte Szenario keinen unverhältnismäßigen Einsatz intelligenter Videoüberwachung durch die Polizei zeigt (siehe 5.2.1.2).

7.2 Einkaufszentrum

Die M-GmbH betreibt ein Einkaufszentrum („alles unter einem Dach“) mit 60 Ladengeschäften, sowie mehreren Cafés, Restaurants und einer Bowlingbahn. Der Betreiber nutzt ein intelligentes Videoüberwachungssystem, welches zur Wahrung der Betriebssicherheit auf gestürzte und liegende Personen ausgerichtet ist und herrenlose Gepäckstücke ausmachen soll. Außerdem wird das Bildmaterial dahingehend ausgewertet, wie viele Passant(inn)en vor welchen Schaufenstern wie lange verharren. Darüber hinaus ist das Videoüberwachungssystem mit einer Gesichtserkennungssoftware ausgestattet, die Gesichter mit Fotos in einer privaten Datenbank abgleicht, in welcher Personen registriert sind, gegen die bereits durch die M-GmbH ein Hausverbot ausgesprochen wurde. Laut aushängender Hausordnung erklären sich die Benutzer mit der detailliert geschilderten Überwachung durch Betreten des Einkaufszentrums einverstanden. Auf die Überwachung wird noch an mehreren Stellen hingewiesen.

7.2.1 Aspekte zur ethischen Bewertung des Szenarios

Anhand des Szenarios „Einkaufszentrum“ werden Fragestellungen der Anwendung intelligenter Videoüberwachung im öffentlich zugänglichen Raum durch nicht öffentliche Stellen aufgeworfen. Gerade weil es sich hier um einen Ort handelt, der Aspekte von öffentlichem und privatem Raum vermischt, ist das Szenario komplex. Es werden also nur einige prägnante Probleme herausgegriffen.

Das von der M-GmbH betriebene System vereint einen Sicherheitsaspekt – gestürzte und liegende Personen zu erkennen – mit Mitteln der Marktforschung. Hier wird deutlich, dass bereits mit recht einfachen Daten, wie dem Aufenthalt und der Geschwindigkeit der Personen im Raum ganz unterschiedliche Zwecke verfolgt werden können (siehe 5.1.3). Dabei ist insbesondere im Hinblick auf die Begründung des Einsatzes (siehe 5.1.1 und 5.1.12) zu untersuchen, ob all diese Interessen des Betreibers auch als solche dargestellt werden oder ob die Sicherheitsargumente nicht dazu dienen, ein System zur Markforschung – das alleine ggf. Akzeptanzprobleme hätte – zu verkaufen. Probleme der Anwendung betreffen also nicht nur die konkrete technische Anpassung der Detektionskriterien an den Kontext, sondern auch die Auswahl bzw. die Beschränkung der Daten.

Doch bereits die Überwachung von gestürzten und liegenden Personen alleine ist in ihrer Anwendung nicht unproblematisch. So ist es schwer, technisch eine gestürzte oder verletzte Person von Menschen zu unterscheiden, die auf dem Boden sitzen, schlafen oder sich aus anderen Gründen länger als gewöhnlich am selben Ort aufhalten. Das System kann also unter Umständen die gesuchten Hilfsbedürftigen nicht von Obdachlosen oder Jugendlichen, die auf dem Boden sitzen, unterscheiden. Wenn solche Gruppen aufgrund der Erkennung durch das System häufig mit Sicherheitsmaßnahmen konfrontiert werden, kann es zu ihrer Verdrängung aus dem Kontext kommen (siehe 5.1.5). Dies kann ebenfalls Menschen betreffen, die schlicht länger am selben Ort zusammenstehen, ohne ein Geschäft zu betreten. Ein solches „social sorting" (Lyon 2003) muss also keinesfalls intendiert sein. Vielmehr kann die Ursache eine mangelhafte Anpassung an den Kontext sein (siehe 5.1.10). So ist es denkbar, dass das System Menschen, die an Krücken gehen oder im Rollstuhl sitzen und sich somit langsamer bewegen als der durchschnittliche Fußgänger, als verletzt identifiziert. Selbst eine gut gemeinte, wiederholte Konfrontation mit Sicherheitspersonal kann für solche Menschen den Aufenthalt im Einkaufszentrum unangenehm machen. Die Aufteilung der Verantwortung zwischen Technikentwickler(in), Auftraggeber(in) und Sicherheitspersonal muss klar und transparent sein (siehe 5.1.4), damit keine Verantwortungslücken bei Fehlern und Missbrauch bestehen.

Ein weiteres Problem der Kontextabhängigkeit ergibt sich aus der Verschränkung mit der Datenbank. Ein intelligentes Videoüberwachungssystem kann nur erkennen, ob eine Person, die in der Datenbank gespeichert ist, den überwachten Raum betritt. Was das genau bedeutet und warum diese Person in der Datenbank ist, muss sich aus anderen Quellen ergeben. Ist dies nicht hinreichend dokumentiert, können Personen ungerechtfertigterweise mit Sicherheitskontrollen konfrontiert oder vom Betreten des Einkaufszentrums ausgeschlossen werden. Dies ist insbesondere dann problematisch, wenn sich die Datenbank aus mehreren Quellen speist, die eventuell unterschiedliche Kriterien anwenden. Hier ist zu beachten, dass Daten immer mit möglichst viel Information über den Kontext in dem sie entstanden sind, kombiniert werden und diese in der neuen Anwendung auch hinreichend „übersetzt" werden müssen (siehe 5.1.10).

Dies kann allerdings die Datensparsamkeit verletzen und weitere Eingriffe in die Privatsphäre bedeuten.

Auch die Eingriffe in die Privatsphäre (siehe 5.1.7) hängen hier stark von der konkreten Ausgestaltung der Anwendung ab. Eine Auswertung in Echtzeit, um Verletzte zu erkennen, ohne dass Daten gespeichert werden, ist noch ein relativ geringer Eingriff in die Privatsphäre. Diese Anwendung ist eher aus den zuvor genannten Gründen des „social sorting" und der unbeabsichtigten Diskriminierung problematisch. Die Tatsache, dass aus den Daten für die Marktforschung relevante Schlüsse gezogen werden können, zeigt, dass hier durchaus das Potenzial besteht, Profile von Personen zu erstellen. Selbst wenn diese Anwendung nicht implementiert wäre, müsste also sichergestellt werden, dass die Daten nicht später für solche Zwecke ausgewertet werden können. Ist die Anwendung implementiert, hängt der Eingriff in die Privatsphäre stark davon ab, wie die Kund(inn)en des Einkaufszentrums informiert werden. Liegt der Fokus der Information auf den Sicherheitsaspekten, die damit die Marktforschung rechtfertigen, wie oben angedeutet? Oder ist diese klar Teil der Informationen? Selbst dann ist zu sehen, dass ein Einkaufszentrum quasi einen öffentlichen Raum ähnlich dem Marktplatz simuliert, die Menschen diesen also mit bestimmten Erwartungen betreten. Der Betrieb eines Überwachungssystems kann diesen Erwartungen durchaus widersprechen. Bei mangelnder Transparenz kann die Auswertung der Verweildauer vor den Geschäften also durchaus als Bruch der legitimen Erwartungen der Menschen im Einkaufszentrum gelten (auch wenn dieser juristisch gedeckt sein sollte). Herrscht Transparenz, entsteht durch den Widerspruch ein zusätzlicher Druck, sich zwischen Privatheitsbedürfnis und der Nutzung des Einkaufszentrums entscheiden zu müssen.

Im Rahmen von Ermittlungsverfahren können privat erhobene Daten, wie die in diesem Szenario besprochenen, gegebenenfalls den Behörden zur Verfügung stehen. Der private durch die Ankündigung zumindest formal abgedeckte Eingriff in die Privatsphäre ist somit potenziell auch ein staatlicher. Hier zeigt sich das Problem, dass private Überwachung dazu beitragen kann, die hohen legalen und gesellschaftlichen Anforderungen an staatliche Überwachung abzuschwächen. Dies ist ein Punkt, der bei der Gestaltung von privater intelligenter Videoüberwachung, insbesondere der Speicherung und der Weiterverarbeitung der Daten, mit berücksichtigt werden muss.

7.2.2 Aspekte zur rechtlichen Bewertung des Szenarios

Wie bereits erörtert (siehe 5.2.2), können die Rechtsgrundlagen zur herkömmlichen Videoüberwachung auf die intelligente Videoüberwachung angewendet werden. Es gilt, die besondere Qualität der Überwachung durch ein automatisiertes System in der verhältnismäßigen Interessenabwägung zu berücksichtigen. Aufgrund des gegebenen Formates ist eine ausführliche juristische Subsumtion hier nicht leistbar, weshalb der Fokus lediglich auf einige relevante Aspekte gerichtet wird.

Im Einkaufszentrum, als innerhalb der Geschäftszeiten öffentlich zugänglichem Raum (siehe 5.2.2.1), wird durch die M-GmbH, als nicht öffentlicher Stelle, ein intelligentes Videoüberwachungssystem offen für verschiedene Zwecke eingesetzt. Angesichts einer hochkomplexen Technologie und deren mannigfaltigen Einsatz- und Ausgestaltungsmöglichkeiten sowie der Problematik für einen technischen Laien im Alltag schnell und unkompliziert aufgeklärt einzuwilligen, ist die Einwilligungslösung keine für die automatisierte Videoüberwachung denkbare. Darum soll geprüft werden, ob die intelligente Videoüberwachung durch die M-GmbH nach § 6 b BDSG zulässig ist. Die Beobachtung und automatisierte Analyse der Passant(inn)en mittels des intelligenten Videoüberwachungssystems im Einkaufszentrum ist eine Datenverarbeitung i. S. d. § 6b Abs. 1, 3 BDSG. Inwiefern diese personenbezogen ist, muss hier nach den verschiedenen Zwecksetzungen unterschieden werden. Zentral ist, neben der Subsumtion unter den Tatbestand, die im Privatrecht maßgebliche Abwägung der widerstreitenden Interessen der Beobachtenden und des Beobachteten im Rahmen der Verhältnismäßigkeitsprüfung auf der Rechtfertigungsebene, wobei die Ausstrahlungswirkung der Grundrechte in das Privatrecht berücksichtigt werden muss. Diese prägt die Auslegung unbestimmter Rechtsbegriffe, wie etwa das „berechtigte Interesse" i. S. d. § 6b Abs. 1 Nr. 3 BDSG. Außerdem zu beachten sind im Bereich der Verhältnismäßigkeit, die als eingriffsrelevant eruierten Rechtsprechungskriterien, die sog. Topoi (siehe 5.2.2.3).

Die M-GmbH nimmt „berechtigte Interessen" zu festgelegten Zwecken, wie etwa der Detektion gestürzter oder liegender Personen, herrenloser Gepäckstücke und der Personenzählung sowie dem Abgleich mit einer privaten Datenbank wahr. Außerdem dient das System der Wahrnehmung ihres Hausrechts als Eigentümerin des Einkaufszentrums, die für die Sicherheit der Kund(inn)en in einem von der M-GmbH eröffneten Gefahrenbereich zuständig ist und ihr Eigentum schützen will. Jedenfalls bei der einem legitimen Zweck dienenden sowie geeigneten und erforderlichen Detektion herrenloser Gepäckstücke sind im Rahmen der Angemessenheitsprüfung keine überwiegenden Interessen der zufällig mit beobachteten Passant(inn)en gegenüber der Pflicht der M-GmbH ihre Kund(inn)en durch eine frühzeitige Aufmerksamkeitslenkung des Sicherheitspersonals vor sicherheitsrelevanten Zwischenfällen zu schützen, gegeben. Allerdings muss auch hier auf die Ausgestaltung des Systems, dessen Transparenz und Missbrauchsmöglichkeiten sowie die Erhebung personenbezogener Daten geachtet werden.

Ebenso ist die M-GmbH als Eigentümerin des Einkaufszentrums in der Ausübung ihres Hausrechts für die Sicherheit ihrer Kund(inn)en und Passant(inn)en verantwortlich. Ihr Ziel ist es, gestürzte oder verletzte Kund(inn)en zeitnahe mit der nötigen Hilfe zu versorgen. Dieses legitime Ziel ist mit der Programmierung der Algorithmen auf gestürzte bzw. liegende Personen erreichbar. Die intelligente Videoüberwachung ist zudem erforderlich. Die alternative Beobachtung durch einen menschlichen Operator hinter dem Videomonitor kann nicht als gleich geeignetes, aber milderes Mittel angesehen werden, da die Aufmerksamkeit menschlicher Beobachtender bereits nach kurzer Zeit

an Stärke verliert. Außerdem werden nur die Daten derjenigen Kund(inn)en, die aufgrund des Algorithmus „auffällig" werden, weiterverarbeitet, womit menschliche Beobachtende hinter den Videomonitoren lediglich gestürzte oder liegende Kund(inn)en angezeigt bekommt. Hierin kann eine weniger grundrechtsintensive Maßnahme als in der ständigen Beobachtung oder Aufnahme aller Kund(inn)en bei der herkömmlichen Videoüberwachung gesehen werden. Allerdings muss die gesteigerte Qualität der Überwachung mit einem automatisierten System berücksichtigt werden. Grundsätzlich ist in diesem Teilszenario die installierte intelligente Videoüberwachungsanlage jedoch angemessen und verhältnismäßig, weshalb die Interessenabwägung kein Überwiegen der schutzwürdigen Interessen der Betroffenen ergibt.

Durch die Ausrichtung des Videoüberwachungssystems auf die Detektion von Passant(inn)en, die vor den Schaufenstern verharren und der Möglichkeit der Feststellung, wie viele Personen sich jeweils wie lange vor welchem Schaufenster aufhalten, könnte jedoch eine andere Qualität der Überwachung bestehen. Wieder ist die Abwägung der widerstreitenden Interessen in der Verhältnismäßigkeitsprüfung erforderlich. Das Interesse der M-GmbH liegt in dieser Fallkonstellation darauf, statistische Daten darüber zu erhalten, welches Geschäft besonderes Interesse erregt und wie viele Personen bestimmte Geschäfte frequentieren. Dadurch können Rückschlüsse darauf gezogen werden, welche Ladengeschäfte im Einkaufszentrum attraktiv sind und welche ggf. ersetzt werden müssten. Außerdem lassen sich aus der Sorte Geschäft, die stärker frequentiert wird, Schlussfolgerungen ableiten, zu welcher sozialen Schicht die beobachteten Passant(inn)en gehören. Durch die daraufhin gezielt angepasste Auswertung, kann u. U. die Aussortierung unerwünschter sozialer Gruppen erfolgen. Darüber hinaus können sicherheitsrelevante Probleme, wie die Anzahl von Personen an bestimmten Durchgängen oder Menschenansammlungen kontrolliert werden. Wieder ist die Ausstrahlungswirkung der Grundrechte zu beachten. Betroffene Grundrechte der beobachteten Passant(inn)en sind hier das Recht am eigenen Bild gem. Art. 2 Abs. 1 GG und das Recht auf informationelle Selbstbestimmung aus Art. 2 Abs. 1 S. 1 GG i. V. m. Art. 1 Abs. 1 GG. Zwar ist im Hinblick auf die unternehmerische Freiheit der M-GmbH wohl noch von einem legitimen Zweck und der Erforderlichkeit der Videoüberwachung, um dieses zu erreichen, auszugehen. Jedoch könnte die M-GmbH die Erhebungen zur Attraktivität der Geschäfte auch durch Umfragen im Einkaufszentrum oder die Verpflichtung zur Freigabe von Geschäftszahlen erreichen. Jedenfalls ist ein Überwiegen der schutzwürdigen Interessen der Betroffenen sorgfältig zu prüfen. Abgeschwächt werden könnte die Datenverarbeitung durch eine bloß pseudonymisierte Datenerhebung, womit je nach verbleibendem Personenbezug u. U. schon die Eingriffsrelevanz fehlt.

Das Videoüberwachungssystem der M-GmbH erfasst bei der Ausrichtung auf die Gesichtserkennung und den Abgleich mit einer privaten Datenbank für Personen, die mit einem Hausverbot belegt wurden, die Passant(inn)en und misst deren biometrische Merkmale. Dabei werden Persönlichkeitsmerkmale erfasst und personenbezogene

Daten erhoben und verarbeitet. Die Verarbeitung der Daten bis zum Alarm im Falle einer Übereinstimmung mit einem Eintrag in der Datenbank läuft dabei automatisiert ab i. S. d. § 3 Abs. 2 S. 1 BDSG. Fraglich ist, ob die Verarbeitung „ausschließlich" auf die automatisierte Verarbeitung gestützt wird oder ob gem. § 6a Abs. 1 S. 2 BDSG eine inhaltliche Bewertung und darauf gestützte Entscheidung durch eine verantwortliche natürliche Person stattfindet, die den Entscheidungsvorschlag ggf. abändern kann. Eine rein formale Bearbeitung durch einen Menschen genügt dabei jedoch nicht. Bei der intelligenten Videoüberwachung, wie sie die M-GmbH zur Gesichtserkennung und dem Abgleich mit einer privaten Datenbank einsetzt, nimmt das System zwar eine Entscheidungsvorbereitung vor – es schlägt „Alarm", wenn ein Treffer erfolgt – aber der/die menschliche Beobachter(in) hat die Letztverantwortung. Er/sie prüft, ob tatsächlich eine Übereinstimmung vorliegt und wie weiter vorgegangen werden soll. Damit ist § 6a Abs. 1 BDSG im vorgelegten Szenario nicht erfüllt. Aufgrund der Verwirklichung der Tatbestandsmerkmale und der zugunsten des Verwenders der intelligenten Videoüberwachung ausgefallenen Interessenabwägung ist das von der M-GmbH eingesetzte System zulässig gem. § 6b BDSG.

7.3 Industriebetrieb

Die Schnell & Sicher AG ist ein renommierter Hersteller moderner Lenksysteme und exportiert als Zulieferer der Automobilbranche in zahlreiche Länder. In ihrem Werk in A beschäftigt sie ca. 500 Mitarbeiter. Nachdem mit dem Betriebsrat eine Betriebsvereinbarung über die Installation von intelligenter Videoüberwachung getroffen wurde, ließ der Werksschutz ein intelligentes Videoüberwachungssystem installieren, das sowohl die Betriebssicherheit für die Mitarbeiter(innen) erhöhen als auch Betriebsspionage erkennen soll. Dazu werden in der gesamten Fertigungshalle Bewegungsmuster, die statistisch von den durchschnittlichen Bewegungsabläufen abweichen, detektiert. Sobald das System eine Abweichung ausmacht, wird der Werksschutz darauf hingewiesen. Diesem wird dann auf einem Monitor das von der alarmierenden Kamera aufgenommene Bild angezeigt.

7.3.1 Aspekte zur ethischen Bewertung des Szenarios

Während die Betriebssicherheit und der Schutz vor Spionage legitime Ziele sind (siehe 5.1.1), besteht bei der Verwendung intelligenter Videoüberwachung wie im hier geschilderten Szenario erhebliches Fehler- und Missbrauchspotenzial (siehe 5.1.3). Abweichungen vom „normalen" Bewegungsablauf können schließlich nicht nur Spionage und Betriebsgefahren sein, sondern auch ungewöhnliche aber private Handlungen, die dann dem Werkschutz angezeigt werden. Außerdem kann die Technik etwa gezielt zur Überprüfung der Arbeitsleistung, Pausengestaltung oder Toilettengängen genutzt werden. Daher gilt es, die Überwachung technisch so zu modifizieren, dass

Fehler des Systems nicht zu einer Privatsphärenverletzung führen. In diesem Anwendungsfall können die verdächtigen Bewegungen sofort am Monitor überprüft werden. Deshalb kann hier beispielsweise zur Verfolgung der angestrebten Zwecke auf eine Speicherung der Daten verzichtet werden, was das Risiko von Verletzungen der Privatsphäre verringert. Außerdem ist eine ständige Kontrolle (etwa durch den Betriebsrat) einzurichten, so dass ein Missbrauch ausgeschlossen werden kann. Es besteht zudem die Möglichkeit, dass der Betriebsrat bestimmten möglichen Privatsphärenverletzungen zustimmt. Die Zustimmung (siehe 5.1.8a und 5.1.8b) muss jedoch auf einem hinreichenden Verständnis der Technik und der Anwendungsart basieren. Hierfür ist die Technik und die Anwendung möglichst transparent zu gestalten (siehe 5.1.8c). So ist der Betriebsrat etwa auch darüber zu informieren, nach welchen Prinzipien die Algorithmen „verdächtige" Abweichungen feststellen. Des Weiteren ist zu überprüfen, ob die Überwachung einige Mitarbeiter(innen) diskriminieren könnte (siehe 5.1.5). So könnte es sein, dass Arbeiter(innen) aufgrund einer Behinderung besonders oft als auffällig detektiert und überwacht werden. Schließlich muss auch beachtet werden, dass bereits die Erwartung eventuell in den Fokus der Überwachung gelangen zu können, das Handeln und die Atmosphäre am Arbeitsplatz verändern kann (siehe 5.1.10).

7.3.2 Aspekte zur rechtlichen Bewertung des Szenarios

Maßgeblich für die private intelligente Videoüberwachung am Arbeitsplatz in einem nicht öffentlich zugänglichen Raum, wie der Schnell & Sicher AG ist die mit dem Betriebsrat getroffene Betriebsvereinbarung i. S. d. §§ 75 Abs. 2, 87 Abs. 1 Nr. 6 BetrVG. Um das Persönlichkeitsrecht am Arbeitsplatz schützen und fördern zu können, wurde mit § 75 Abs. 2 BetrVG eine Norm geschaffen, die dieses explizit gewährleistet. Danach sind mitbestimmungsrechtliche Verfahren der Mitwirkung von Arbeitnehmer(inne)n nach §§ 87 Abs. 1 Nr. 6 BetrVG, 75 Abs. 3 Nr. 17 BPersVG für alle Bereiche der Videoüberwachung zulässig und einzuhalten. Diese Verfahren bedeuten allerdings nur eine prozedurale, keine materielle Legitimation. Hinsichtlich der Ausgestaltung der Betriebsvereinbarung kann auf die Ausführungen unter 5.2.2 und die ethischen Aspekte unter 7.3.1 verwiesen werden.

Gäbe es keine Betriebsvereinbarung, müsste auf das einschlägige Gesetzesrecht zurückgegriffen werden. Bislang gilt die sog. „kleine Lösung", wonach für Videoüberwachungsmaßnahmen in nicht öffentlich zugänglichen Räumen § 32 BDSG gilt. Bei Inkrafttreten der geplanten Neufassung des BDSG-E wären am Arbeitsplatz auch § 32 e Abs. 2, 4 BDSG-E, der ein Verbot heimlicher Videoüberwachung am Arbeitsplatz normiert und § 32 f Abs. 1 BDSG-E, der die Beobachtung nicht öffentlich zugänglicher Betriebsstätten mit optisch-elektronischen Einrichtungen regelt, in den Blick zu nehmen. Allerdings wurden diese Pläne zumindest in der letzten Legislaturperiode wieder verworfen. Zudem müssen die Entwicklungen auf europäischer Ebene beachtet werden. Art. 82 DS-GVO-E erwähnt bspw. die Möglichkeit der Kollektivvereinbarung nach § 75

Abs. 2 BetrVG nicht mehr, womit insofern fraglich ist, ob eine solche auch bei Inkrafttreten der Verordnung noch zulässig sein wird. In der Praxis bedeutet dies für Fragen der Zulässigkeit des Einsatzes von Videoüberwachung am Arbeitsplatz, eine weitere Orientierung an Einzelfallentscheidungen, und insbesondere für Fragen des Einsatzes intelligenter Videoüberwachung, eine Rechtsunsicherheit. Der Arbeitnehmer muss sich derzeit je nach Sachlage auf den Schutz aus dem Vertrags- und Deliktsrecht, dem BDSG, dem BetrVG oder dem Recht auf informationelle Selbstbestimmung berufen.

Wie bereits bei den vorherigen Szenarien erörtert und in der ethischen Bewertung dieses Szenarios angelegt (siehe 7.3.1), müssen auch am Arbeitsplatz die schutzwürdigen Interessen der Betroffenen in die Abwägung eingestellt werden. Die Schnell & Sicher AG stellt bspw. im vorgelegten Szenario sicher, dass Teile der Betriebsstätte, die überwiegend der privaten Lebensgestaltung des/der Beschäftigten dienen, wie etwa Sanitär- und Umkleidebereich, nicht überwacht werden. Außerdem sind die aus der Rechtsprechung herausgearbeiteten Kriterien: Konkreter Verdacht, Heimlichkeit der Maßnahme, Einwilligung des/der Betroffenen, Anonymisierung des/der Betroffenen, zeitliche und räumliche Beschränkung in die Abwägung einzustellen. Besonders eingriffsintensiv zu bewerten ist darüber hinaus grundsätzlich, dass der/die Arbeitnehmer(in) der Videoüberwachung nicht ausweichen kann und sich dadurch der Überwachungs- und Anpassungsdruck steigert.

8 Literatur

M. Apelt/ N. Möllers, „Wie „intelligente" Videoüberwachung erforschen? Ein Resümee aus zehn Jahren Forschung zu Videoüberwachung", in Zeitschrift für Außen- und Sicherheitspolitik (ZAP) 2011, S. 585-593.

G. Armstrong/ C. Norris, The maximum surveillance society. The rise of CCTV. Oxford & New York: Berg Publishers (1999).

Ch. M. Bishop. 2006. Pattern Recognition and Machine Learning. New York: Springer.

S. R. Langmann, in: ders. (Hrsg.), Automatisierung, (2010), S. 19.

M. Bornewasser/ C. Classen/ I. Stolpe, Videoüberwachung öffentlicher Straßen und Plätze: Ergebnisse eines Pilotprojekts im Land Brandenburg. Frankfurt: Verlag für Polizeiwissenschaft (2008).

D. Garland, Kultur der Kontrolle. Verbrechensbekämpfung und soziale Ordnung in der Gegenwart. Frankfurt am Main & New York: Campus (2008).

Gewerkschaft der Polizei, Pressemeldung vom 22.10.2012. Verfügbar unter: http:// www.gdp.de/gdp/gdpber.nsf/ID/F70FEEADB05B95CDC1257A9F003FEB09?Open [05.03.2013]

R. Gössner, »Big Brother« & Co.: Der moderne Überwachungsstaat in der Informationsgesellschaft. Hamburg: Konkret Literatur Verlag (2001)

M. Gras, Kriminalitätsprävention durch Videoüberwachung. Baden-Baden: Mainzer Schriften zur Situation von Kriminalitätsopfern, Bd. 33 (2003)

C. Held, Intelligente Videoüberwachung unter dem Grundgesetz – Vorgaben für den präventiv-polizeilichen Einsatz, zugl. Diss., Würzburg, vorauss. 2014

C. Held/ J. Krumm/ P. Markel/ R. P. Schenke, „Intelligent Video Surveillance", in IEEE Computer Society (March 2012), S. 83 ff.

L. Hempel, Zur Evaluation von Videoüberwachung: Methoden, Standards und Beispiele aus der Bewertungspraxis. In Zurawski, N. (Hg.), Surveillance Studies: Perspektiven eines Forschungsfeldes (S. 117-145). Opladen & Farmington Hills: Verlag Barbara Budrich (2007)

L. Hempel/ E. Töpfer, CCTV in Europe: Final report. Verfügbar unter http:// www.urbaneye.net/results/results.htm [05.10.2010]

G. Hornung, Eine Datenschutz-Grundverordnung für Europa? Licht und Schatten im Kommissionsentwurf vom 25.01.2012, in: Zeitschrift für Datenschutz (ZD) (3/2012), S. 99 ff.

G. Hornung/ M. Desoi, "Smart Cameras" und automatische Verhaltensanalyse, Kommunikation und Recht (K & R) (3/2011), S. 153 ff.

D. M. Kahan/ P. Slovic/ D. Braman/ J. Gastil/ G. L. Cohen, Affect, Values, and Nanotechnology Risk Perceptions: An Experimental Investigation. Cultural Cognition Working Paper No. 22 (2007)

D. Kammerer, Bilder der Überwachung. Frankfurt am Main: Suhrkamp (2008)

F. R. Klauser, Videoüberwachung öffentlicher Räume: Zur Ambivalenz eines Instruments sozialer Kontrolle (1.Aufl.). Frankfurt am Main: Campus Verlag GmbH (2006)

S. Krasmann, Die Kriminalität der Gesellschaft. Zur Gouvernementalität der Gegenwart. Konstanz: UVK (2003)

D. Lyon, Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination. Routledge: London (2003)

E. Maggio/ A. Cavallaro, Video Tracking: Theory and Practice. Chichester: John Wiley and Sons (2011).

T. Matzner, The model gap, AI & Society, Online first: DOI (2013).

N. Möllers/ J. Hälterlein, "Privacy issues in public discourse: the case of "smart" CCTV in Germany", Innovation: The European Journal of Social Science Research (2012), DOI: 10.1080/13511610.2013.723396

R. H. Reuband, Was die Bürger von der Überwachung halten. Verfügbar unter http://www.philfak.uniduesseldorf.de/fileadmin/Redaktion/Institute/Sozialwissenschaften/Soziologie/Dokumente/Reuband/CCTV.pdf [16.01.2011]

A. Roßnagel, Handbuch Datenschutzrecht, Die neuen Grundlagen für Wirtschaft und Verwaltung, München (2003)

A. Roßnagel/ M. Desoi/ G. Hornung, Gestufte Kontrolle bei Videoüberwachungsanlagen, Datenschutz und Datensicherheit (DuD) (10/2011), S. 694 ff.

G. Schaub, Arbeitsrechts-Handbuch, 14. Aufl. (2011)

R. P. Schenke, Videoüberwachung 2.0 auf dem Prüfstein des Grundgesetzes, in: Zöller, Mark A./Hilger, Hans/ Küper, Wilfried/ Roxin, Claus (Hg.), Gesamte Strafrechtswissenschaft in internationaler Dimension - Festschrift für Jürgen Wolter zum 70. Geburtstag, Berlin (2013), S. 1077 ff.

P.J. Silvia/ T. S. Duval, Objective self-awareness theory: Recent progress and enduring problems. Personality and Social Psychology Review (2001), 5, S. 230–241

S. Simitis, Bundesdatenschutzgesetz, 7. Aufl. (2011)

S. Theodoridis/ K. Koutrumbas, Pattern Recognition. Burlington: Academic Press (2008).

T. Wybitul/ A. Fladung, EU-Datenschutz-Grundverordnung – Überblick und arbeitsrechtliche Betrachtung des Entwurfs, Betriebsberater (BB) (2012), S. 509 ff.

T. Wybitul/ N. Rauer, EU-Datenschutz-Grundverordnung und Beschäftigtendatenschutz, Zeit-schrift für Datenschutz (ZD) (4/2012), S. 160 ff.

Internationales Zentrum für Ethik in den Wissenschaften (IZEW)
Eberhard Karls Universität Tübingen
Wilhelmstr. 19, 72074 Tübingen

Telefon: +49 / 7071 / 29 77981
Telefax: +49 / 7071 / 29 5255

izew@uni-tuebingen.de
www.izew.uni-tuebingen.de

ISBN 978-3-935933-12-4