Heinrich C. Mayr, Martin Pinzger (Hrsg.): INFORMATIK 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 413

Digitale Tarnkappe: Anonymisierung in Videoaufnahmen

Sebastian Volkmann[1], Linus Feiten[1], Christian Zimmermann[1], Sebastian Sester[1], Laura Wehle[1] und Bernd Becker[1]

Abstract: Videoüberwachung ist heute allgegenwärtig. Sie dient dazu, Delikte im Nachhinein aufzuklären, zur Echtzeit-Überwachung oder zur Abschreckung. Darüber hinaus gibt es aber auch wirtschaftliche Interessen für eine Videoüberwachung und automatische Erfassung von Personen – z.B. zur Erstellung von Kundenprofilen und somit zur Analyse von Kaufverhalten. Dem gegenüber stehen Rechtsansprüche sowie ethische und gesellschaftliche Grundnormen, etwa dass Menschen nicht unter Generalverdacht gestellt oder ohne Zustimmung aufgezeichnet werden dürfen. In dieser Arbeit wird ein technischer Lösungsansatz behandelt, der eine flexible Handhabung der Videoüberwachung erlaubt. Es werden in diesem Zusammenhang neben der technischen Umsetzung auch ökonomische, ethische und juristische Fragen betrachtet. Der Lösungsansatz besteht darin, Personen auf Videoaufnahmen durch ein kryptographisches Verfahren unkenntlich zu machen, noch bevor die Aufnahmen die Kamera-Elektronik verlassen. Nur mittels eines geheimen kryptographischen Schlüssels können einzelne Zeit- und Bildbereiche einer Aufnahme wieder deanonymisiert werden, wodurch rechtlichen wie ethischen Bedenken Rechnung getragen werden kann. In kommerziellen Szenarien erlaubt es diese *digitale Tarnkappe*, dass Kunden z.B. im Rahmen eines Prämien-Programms freiwillig auf Anonymisierung verzichten. Während in der Literatur der Informatik bereits seit längerem Technologien für solche System beschrieben werden, werden in dieser Arbeit Wege gezeigt, wie dessen Einbettung in die Gesellschaft wirklich realisiert werden könnte.

Keywords: Videoüberwachung, Datenschutz, Transparenz, Privatsphäre

1 Einleitung

Videoüberwachung ist heute aus dem Lebensalltag größerer Städte nicht mehr wegzudenken. Staatliche Einrichtungen, Unternehmen und Privatpersonen versprechen sich in erster Linie einen Zuwachs an Sicherheit, indem die Aufnahmen in Echtzeit ausgewertet oder aufgezeichnet werden können, um bei Delikten im Nachhinein die Täter zu identifizieren. Da die Echtzeit-Auswertung ab einer gewissen Anzahl von Kameras nicht mehr effektiv von menschlichem Personal durchführbar ist, gibt es Bestrebungen, die Analyse automatisiert durch Bilderkennungsalgorithmen durchführen zu lassen, wie es sich z.B. das kontrovers diskutierte EU-Forschungsprojekt INDECT zum Ziel gesetzt hat.

Aber nicht nur zur Herstellung von mehr Sicherheit kann Videoüberwachung eingesetzt werden. Durch automatische Bildanalyse rückt die Technik auch in das Interesse privater Wirtschaftsunternehmen. Wie heute bereits das Such- und Click-Verhalten von Internetnutzern gesammelt und analysiert wird, um daraus Nutzerprofile für unter anderem personalisierte Werbung oder Angebotsoptimierung zu generieren, kann dies auch mit Videoaufnahmen geschehen. Durch das *Tracken* von Kunden eines Kaufhauses könnte der

[1] Universität Freiburg, Centre for Security and Society, Bertoldstraße 17, 79085 Freiburg, {feiten, sesters, wehle, becker}@informatik.uni-freiburg.de, sebastian.volkmann@philosophie.uni-freiburg.de, zimmermann@iig.uni-freiburg.de

Betreiber z.B. die Anordnung der Produktregale optimieren – ganz im Sinne der heute schon im Internet geläufigen Empfehlungen: „Personen die ... gekauft haben, interessieren sich auch für ...". Per Smartphone-App, Bildschirmen im Kaufhaus oder sogar eingebautem Display im Einkaufswagen der Zukunft können dem Kunden dann personalisierte Werbung oder Rabattangebote angezeigt werden.

Trotz gesetzlicher Normen dazu, unter welchen Bedingungen Videoüberwachung stattfinden darf, gibt es eine andauernde gesellschaftliche Debatte darüber, inwieweit diese mit einer freiheitlichen Gesellschaft vereinbar ist. Man betrachte z.B. die ‚Big Brother Awards', welche mit Anspielung auf George Orwells Roman ‚1984' seit 1999 weltweit von Bürgerrechtlern an Akteure verliehen werden, die als besonders schädlich für die persönliche Privatsphäre empfunden wurden. Einen direkten Bezug zu Videoüberwachung gab es z.B. bei den deutschen ‚Preisträgern' der Jahre 2000 (Deutsche Bahn, Überwachung von Bahnsteigen), 2004 (Lidl, Überwachung von Mitarbeitern) und 2013 (Uni Paderborn, Überwachung von Hörsälen und Rechnerpools). Am 20.4.2016 entschied zudem das Bundesverfassungsgericht, dass die Ermächtigung zur verdeckten Erhebung personenbezogener Daten im BKA-Gesetz – etwa durch heimliche Videoüberwachung von Privaträumen – in dieser weitreichenden Form nicht Verfassungsgemäß ist und forderte die Sichtung des erhobenen Materials durch eine unabhängige Datenschutzinstanz.

In dieser Arbeit wird ein technischer Ansatz behandelt, der die divergierenden Interessen von Videoüberwachungsbetreibern und um ihre Privatsphäre besorgten Bürgern bzw. Kunden miteinander vereinbart: die *digitale Tarnkappe* (DTK). Dieses eigentlich generelle Konzept [BMP12] wird hier auf Videoaufnahmen angewandt, indem Personen auf Videoaufnahmen automatisch unkenntlich gemacht werden, was jedoch im Nachhinein auch wieder aufgehoben werden kann, wenn eine unabhängige *Schlüsselinstanz* den dafür nötigen kryptographischen Schlüssel freigibt. Für ein kommerzielles Szenario ist es dabei möglich, dass Kunden freiwillig auf ihre Anonymisierung verzichten. Abschnitt 2 beschreibt die Funktionsweise dieser DTK aus technischer Sicht, während Abschnitt 3 ihre ökonomischen Anwendungsmöglichkeiten aufzeigt. Abschnitt 4 unternimmt eine ethische Folgenabschätzung, während Abschnitt 5 die DTK in den Kontext der heutigen deutschen Gesetzeslage setzt. Jede dieser Betrachtungen kann aufgrund der Platzbeschränkung dieser Arbeit nur in aller Kürze erfolgen. Die Besonderheit unseres Beitrags liegt vor allem in der Kombination von technischem Konzept und multidisziplinärer Betrachtungsweise. Abschnitt 6 beschließt die Arbeit mit einer Diskussion und Ausblick. Dabei wird auch das über Videoaufnahmen hinausgehende generelle Konzept DTK beschrieben.

2 Informatischer Lösungsansatz

Technologien zur Anonymisierung in Überwachungsvideos werden in der technischen Literatur seit längerem diskutiert; z.B. [Se05, DE06, CPV06, Sc07, Hu14, PLCFR15]. Die meisten dieser Ansätze detektieren automatisch bestimmte Bereiche in Überwachungsvideos – wie menschliche Silhouetten, Gesichter oder Nummernschilder – und schwärzen diese unumkehrbar aus. Dabei ist oft das Ziel, dass ein Computeralgorithmus ohne menschliches Zutun erkennt, ob sich auf dem Kamerabild etwas ‚überwachungswürdiges' ereignet, um diesen Bereich dann *nicht* auszuschwärzen bzw. einen menschlichen Beobachter zu

alarmieren. Einige Ansätze (z.B. [Ch09, CKM09, CCK13]) bieten auch die Möglichkeit, die Ausschwärzung eines Bereichs nachträglich wieder aufzuheben.

Dies ist eine essentielle Funktion der Videoanonymisierung, wie sie hier vorgeschlagen wird. Eine automatische Erkennung von ‚überwachungswürdigen' gegenüber ‚harmlosen' Videosequenzen ist jedoch nicht erforderlich. In der einfachsten Variante kann grundsätzlich alles ausgeschwärzt werden, was sich im Bild bewegt, wofür dann kein komplizierterer Bilderkennungsalgorithmus nötig ist. Dennoch kann die hier beschriebene Methode prinzipiell um jeden beliebigen komplizierten solchen Algorithmus erweitert werden, da dies der Funktionsweise keinen Abbruch tun würde. Wie die auszuschwärzenden Bereiche bestimmt werden, steht nicht im Vordergrund dieser Arbeit sondern viel mehr das Verfahren, mit dem die Schlüssel zur Deanonymisierung erstellt und verwaltet werden.

Die Videoaufnahmen werden wie gewöhnlich von einer Kamera gemacht, wobei deren Elektronik so erweitert ist, dass die aufgezeichneten Rohdaten den internen Speicher der Kamera niemals verlassen. Durch Methoden der Hardware-Security bzw. Trusted-Hardware kann die Kamera so gesichert werden, dass es nahezu unmöglich ist, den internen Speicher von außen abzugreifen. Ein solcher Angriff würde es erfordern, nicht nur das Gehäuse der Kamera zu öffnen, das auf klassische Art verplombt sein kann, sondern auch die Kamera in ein Labor zu bringen, wo komplizierte invasive Eingriffe in die Elektronik durchgeführt werden müssten. Zur Abwehr auch solcher Angriffe gibt es mannigfaltige Maßnahmen wie z.B. *tamper-sensing Meshes* [An06] oder *Physically Unclonable Functions* (PUFs) [RDK11]. Erstere sorgen dafür, dass bei einem invasiven Angriff eine Sicherung zerstört wird, die daraufhin die Funktion des Chips deaktiviert. Letztere erzeugen eine eindeutige Chip-Signatur, die durch invasive Angriffe unwiederbringlich verfälscht wird. Eine solche PUF-Signatur kann somit dazu verwendet werden, sicherzustellen, dass eine Kamera mit DTK-Funktionalität nicht manipuliert oder durch eine scheinbar identische ausgetauscht wurde. Die PUF-Signatur des Kamerachips wird dabei nie nach außen kommuniziert, sondern innerhalb des Chips zur Erstellung des kryptographischen *Private-Keys* eines asymmetrischen Kryptosystems [PP10] verwendet. Der DTK-Chip der Kamera kommuniziert lediglich den zu diesem Private-Key gehörenden Public-Key nach außen. Eine mit diesem Public-Key verschlüsselte Anfrage kann nur von dem DTK-Chip plausibel beantwortet werden, wenn er im Besitz des Private-Key ist. Für physikalische Absicherungen wie Verplombung oder Trusted-Hardware gibt es zwar stets theoretische Möglichkeiten, diese auch zu umgehen, aber die Kosten für einen Angriff können durch Gegenmaßnahmen wie die oben genannten beliebig in die Höhe getrieben werden. Wie hoch der Aufwand für einen Angreifer sein soll, kann je nach Sensitivität des Szenarios angepasst werden. Eine bedeutende Herausforderung wird es sein, die ‚Chain of Trust' so zu gestalten, dass jeder von der Videoüberwachung betroffene diesen nachvollziehen und ihm vertrauen kann.

Im Folgenden wird die Hardware der Kamera daher als sicher angenommen, d.h., die von ihr gemachten *Rohdaten-Aufnahmen* sind außerhalb ihres DTK-Chips nicht abgreifbar. Stattdessen werden nur Daten nach außen gegeben, in denen Personen bereits anonymisiert wurden. Dies geschieht dadurch, dass zunächst die zu anonymisierenden Bildbereiche (Regions of Interest, ROIs) in jedem Kamerabild in Echtzeit erkannt werden. Das leistet eine auf dem DTK-Chip arbeitende Bildverarbeitung, die – wie bereits erwähnt – beliebig

kompliziert sein kann. Bereits heute gibt es Algorithmen, mit denen Menschen automatisch in Videos erkannt werden können [DT05, ARS09, WSS10, Be12]. Sollten sich diese Ansätze allerdings als noch zu unzuverlässig oder rechenaufwändig erweisen um in Echtzeit auf in der Kamera eingebetteter Hardware zu laufen, können die ROIs auch durch denkbar simple Algorithmen bestimmt werden; beispielsweise durch die einfache Detektierung von Bewegungen im Bild.

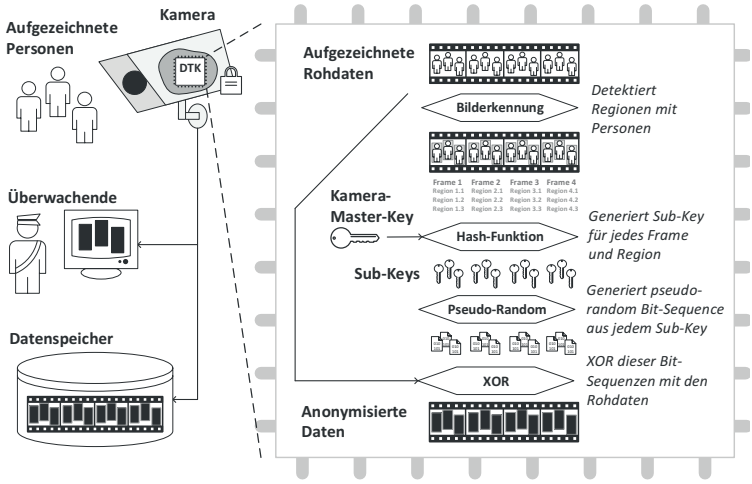

Abb. 1: Der schematische Aufbau des DTK Kamera-Systems.

Abbildung 1 zeigt, wie die Anonymisierung schematisch abläuft. Sie besteht nicht bloß in der Schwärzung eines Bereiches. Damit wären die Aufnahmen zur Strafverfolgung oder kommerziellen Auswertung nutzlos. Stattdessen werden die zu anonymisierenden Bildbereiche kryptographisch verschlüsselt. Jede DTK-Kamera hat ihren eigenen digitalen *Kamera-Master-Key* (KMK), welcher der Verschlüsselung zugrunde liegt und Teil der gesicherten Kamera-Hardware ist. Aus diesem KMK wird für jeden Zeitabschnitt und jeden zu anonymisierenden Bildbereich ein einzigartiger *Sub-Key* generiert. Dies geschieht über eine *Hash-Funktion* [Sh11], welche als Eingabe den KMK sowie die Zeitmarke und die Koordinaten des zu anonymisierenden Bildbereichs bekommt. Starke *Hash-Funktionen* haben die Eigenschaft, dass sich aus ihrem Ausgabewert nicht die Eingabe berechnen lässt. D.h. aus einem *Sub-Key* lässt sich nicht wieder der KMK berechnen. Für die Verschlüsselung, d.h. die Anonymisierung eines Bildbereichs wird aus dem jeweiligen *Sub-Key* ein *Stream-Cipher* generiert, der mit den Rohdaten des zu anonymisierenden Bereiches über ein logisches XOR verknüpft wird. Dies ermöglicht es, dass der gleiche *Sub-Key* auch wieder für die Entschlüsselung, d.h. die Deanonymisierung, verwendet werden kann.

Wie Abbildung 1 zeigt, werden außerhalb der Kamera nur anonymisierte Aufnahmen abgespeichert. Sollte der *Auswertende* es für nötig befinden, eine Person zu deanonymisieren, kann er dies bei der unabhängigen *Schlüsselinstanz* beantragen, die im Besitz des KMK ist (siehe Abbildung 2). Findet diese die Deanonymisierungsanfrage berechtigt, wendet sie ihren KMK zusammen mit den vom *Auswertenden* angegebenen Zeitspanne und Bildbe-

reich auf die *Hash-Funktion* an, um damit die nötigen *Sub-Keys* zu erstellen. Diese kann der *Auswertende* nun lediglich zur Deanonymisierung der von ihm angeforderten Zeitspanne und Bildbereiche verwenden.

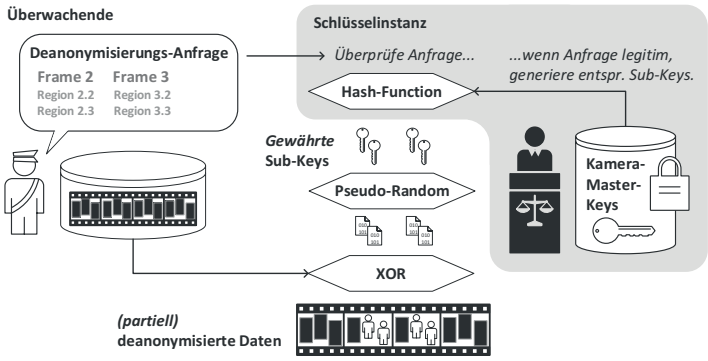

Abb. 2: Deanonymisierung ist nur durch die von der Schlüsselinstanz bewilligten *Sub-Keys* möglich.

Auf den Abbildungen ist bereits angedeutet, dass nicht alle Personen anonymisiert werden. In einem kommerziellen Szenario könnten Personen gegen eine Prämie freiwillig auf ihre Anonymisierung verzichten, und es dem Betreiber somit erlauben, sie auf den Videoaufnahmen zu *tracken*. Wie diese Personen sich dem DTK-System zu erkennen geben können und wie die ökonomischen Anwendungsmöglichkeiten sind, wird in Abschnitt 3 erörtert.

Abb. 3: Ein erster Proof-of-Concept der DTK.

Für einen ersten Proof-of-Concept wurde ein DTK-System als Opt-Out-Variante implementiert. D.h., anstatt dass standardmäßig alle Personen anonymisiert werden und nur solche mit bestimmter Kennzeichnung nicht, war es umgekehrt: Bildbereiche, die sich um eine Infrarot-LED herum befanden, wurden anonymisiert. Grund dieser vorläufigen Vereinfachung war, dass von einer automatischen Identifizierung der ROIs zunächst abstrahiert und der Fokus auf die Daten-Verschlüsselung gelegt wurde. Abbildung 3 zeigt den Aufbau der LED sowie den Anonymisierungs-Effekt auf einem Kamerabild. Durch eine adäquate ROI-Bestimmung lässt sich dieser Prototyp in die oben beschriebene Opt-In-Variante überführen.

3 Ökonomische Anwendungsmöglichkeiten

DTK-Systeme können nicht nur dazu verwendet werden, bei der Verbrechensprävention bzw. -aufklärung durch Videoüberwachung die Privatheit der Betroffenen zu schützen. Sie ermöglichen es darüber hinaus auch, ökonomisch motivierte Videoüberwachung privatheitsachtend umzusetzen. Im Folgenden sollen die Anwendungsmöglichkeiten des vorgestellten System im Kontext von Kundenverhaltensanalysen in videoüberwachten Kaufhäusern untersucht werden.

Bereits seit langem verwenden Betreiber von Kaufhäusern Videosysteme nicht nur zur Abschreckung von Kaufhausdieben und zur Beweisfindung im Falle von Delikten innerhalb der Kaufhäuser. Videosysteme bieten zusätzlich die Möglichkeit, Kundenbewegungen und sogar die Blickrichtungen der Kunden detailliert nachzuverfolgen [LH08, Li07]. Dies ermöglicht es Kaufhausbetreibern, Erkenntnisse zu gewinnen, die bei der Ladenplanung, wie auch bei der Durchführung von Werbeaktionen, gewinnbringend angewendet werden können. Die in Deutschland hohen Datenschutzbedenken der Bevölkerung stellen allerdings ein Hindernis bei der Einführung und Nutzung solcher Analysemethoden dar. Das hier vorgestellte DTK-System kann verwendet werden, um die Datenschutzbedenken der Kunden zu adressieren und sicherzustellen, dass nur das Verhalten von Kunden, die videogestützten Analysen ihres Verhaltens zugestimmt haben, ausgewertet wird.

Das hier vorgestellte DTK-System kann analog und komplementär zu den momentan weit verbreiteten ‚Bonuspunktekarten' verwendet werden, um einerseits Verhaltensanalysen auf Kunden einzuschränken, die solchen Analysen zugestimmt haben und andererseits, um Kunden Anreize zu bieten, solchen Analysen zuzustimmen. Dabei bieten sich zwei Optionen. Im momentanen Implementierungsstand des vorgestellten DTK-Systems kann es eingesetzt werden, um Kunden eine leicht umzusetzende Möglichkeit des Opt-Out aus der Überwachung und Analyse ihres Verhaltens zu bieten. Dabei können Kunden durch das Tragen eines entsprechenden Signals, bswp. an der Kleidung oder am Einkaufswagen, signalisieren, dass sie keine Überwachung ihrer Bewegung wünschen. Ein solcher Ansatz würde allerdings nicht in Einklang mit den Forderungen der zukünftig zu beachtenden europäischen Datenschutzgrundverordnung stehen, die einen ‚privacy by design'-Ansatz vorschreibt [Eu12, Art. 23]. Um dieser Anforderung zu genügen, kann das DTK-System allerdings so implementiert werden, dass standardmäßig die komplette Videoaufnahme verschlüsselt wird und nur Bereiche entschlüsselt werden, in denen ein entsprechendes Signal aufgefangen werden kann. Denkbar wäre hier eine Infrarot-LED, deren Lichtimpulse einen der Person zuordenbaren Code an die Kameras senden. Unabhängig von Kameras könnte auch eine Funktechnik eingesetzt werden, durch welche z.B. die ‚Bonuspunkte-Smartcard' einer Person verfolgt würde. Wenn diese Positionsdaten dem DTK-Algorithmus zur Verfügung stehen, kann die Anonymisierung der Person in den entsprechenden Bildbereichen aufgehoben werden.

Ein zu lösendes Problem hierbei besteht in der Wahl einer geeigneten *Schlüsselinstanz*. Des Weiteren muss das vorhandene System erweitert werden, um sicherzustellen, dass im Falle gleichzeitiger Aufnahme von Kunden die in die Analyse ihres Verhaltens eingewilligt haben und solchen, die dies nicht getan haben, der Opt-Out des einen Kunden höher priorisiert wird als der Opt-In des anderen.

4 Ethische Folgenabschätzung

Ethische Technikfolgenabschätzung (TA) zielt darauf ab, insbesondere nicht-intendierte Folgewirkungen technischer Entwicklungen in Bezug auf Grundwerte zu bewerten und dieses Wissen einer (oftmals politischen) Entscheidungsfindung zuzuführen [Ot05]. Ethische TA erarbeitet dabei normative Planungsgrößen [Gr99], kann aber auch – wie im Falle der DTK – konstruktiv genutzt werden, um die Technologieentwicklung selbst wiederum normativ zu prägen [Pe99]. In Bezug auf Videoüberwachung öffentlich zugänglicher Räume lassen sich zunächst zwei Grundperspektiven ethischer Argumentation unterscheiden: (1) Nicht-intendierte Folgen können konkrete Individuen unverhältnismäßig beeinträchtigen, insbesondere hinsichtlich ihrer Grundrechte oder anderer gesellschaftlicher Grundwerte; (2) aus gesellschaftspolitischer Sicht können Nebenfolgen einen Trend hin zu einer restriktiven Gesellschaft bestärken. Letzterer Folgentypus ist insbesondere dann wichtig, wenn bestimmbare Individuen jeweils nur verhältnismäßig gering oder vereinzelt direkt beeinträchtigt werden, in Summe aber dennoch ein erhebliches Risiko für den offenen Charakter einer Gesellschaft besteht. Dies könnte durch eine langsame und kaum merkbare aber dennoch beständige Ausweitung von Sicherheitsmaßnahmen geschehen (populärwissenschaftlich als ‚boiling frog'-Argument bekannt [TZ09]) oder durch eine nachträgliche Ausweitung des Verwendungszwecks (‚mission creep'-Argument [Pe06]). Eine weitere Gefahr der gesellschaftlichen Restriktion könnte darin bestehen, dass Sicherheitsmaßnahmen für Betroffene völlig intransparent sind und sich die jeweiligen staatlichen und privaten Akteure dadurch Rechenschaftspflichten entziehen können. Wertkonflikte vom ersten Typus sollen in der Folge anhand von zwei in der öffentlichen Debatte sehr präsenten Metaphern [GG00] analysiert werden: Der ‚gläserne Kunde' bzw. ‚gläserner Bürger', sowie der ‚Generalverdacht' unter den sich Betroffene gestellt fühlen können. Für die Besprechung des zweiten Typus von nicht-intendierten Folgewirkungen werden die Metaphern ‚orwellsche' und ‚kafkaeske Überwachungsgesellschaft' genutzt [Ly09].

Individuumszentrierte Perspektive Bei räumlich begrenzter Überwachung beschreibt die Metapher des gläsernen Kunden vor allem die Angst, dass das Sammeln und Auswerten von Bildinformationen privatwirtschaftlicher Akteure Einblicke in persönliche Einstellungen und Lebenssituationen von Betroffenen erlaubt oder Rückschlüsse auf deren Wünsche und Intentionen gewährt – obwohl diese von den Betroffenen selbst wie auch von der Gesellschaft grundsätzlich als schützenswert betrachtet werden. Die Schutzwürdigkeit bestimmter als ‚privat' oder gar ‚intim' bestimmter Lebensbereiche gründet dabei einerseits in kulturell geprägten Normen der Zurückhaltung (etwa zu Sexualität oder Krankheit), andererseits aber auch in dem gesellschaftlichen Wunsch, der Gefahr vorzubeugen, dass Einzelne unverhältnismäßig stark benachteiligt werden könnten – etwa aufgrund ihrer finanziellen oder sozialen Situation. Die Metapher des gläsernen Bürgers lässt sich in Abgrenzung hierzu vor allem auf das Sammeln und Auswerten von Informationen durch staatliche Akteure beziehen. Die Schutzwürdigkeit privater Informationen begründet sich dabei zusätzlich darin, dass Einzelne vor dem übermächtigen Zugriff des Staates geschützt werden sollen. Staatliche Videoüberwachung muss daher auch immer in Bezug auf individuelle Abwehrrechte gesehen werden. Das heißt allerdings nicht, dass ein Eingriff in diesen rechtlich geschützten Privatbereich immer illegitim ist. Allerdings sollte dies nicht wahllos geschehen, sondern nur in begründeten Fällen oder mit Zustimmung der Betrof-

fenen – und dies gilt umso mehr, je schutzloser der Betroffene dem Eingriff ausgesetzt ist. Staatliche Eingriffe sind deshalb im Allgemeinen deutlich strenger reglementiert als Eingriffe durch private Akteure. Gesellschaftlich werden in solchen Fällen Eingriffe bewusst zugunsten anderer Werte in Kauf genommen – etwa wenn der Verdacht auf eine Straftat vorliegt, die verfolgt werden soll. Die Metapher des Generalverdachts bezieht sich daher auf die Sorge vor einer anlasslosen Anwendung einer Sicherheitsmaßnahme wie der Videoüberwachung, durch die grundsätzlich jede Person von Eingriffen in schutzwürdige Privatbereiche beeinträchtigt wird – insbesondere bei staatlichen Eingriffen.

Beim klassischen Videobild lassen sich Kunden bzw. Bürger pauschal im Videobild identifizieren (manuell oder auch automatisiert etwa über biometrische Gesichtserkennung oder andere optische Kriterien). Über die Analyse der Bewegungen lassen sich gegebenenfalls automatisiert Rückschlüsse auf Kaufverhalten, Intentionen oder persönliche Lebensumstände ziehen: Wie lange hält sich diese konkrete Kaufhaus-Kundin bei den Kondomen auf, wie häufig besucht sie das Weinregal? Besucht der zufällig auf dem Bild erkannte Nachbar den belebten Platz zu allen Tageszeiten – oder nur außerhalb der regulären Arbeitszeiten? Wie lange unterhält er sich mit dem Prediger – wie lange mit den Leuten vom Wahlkampfstand? Insbesondere durch die Möglichkeiten einer automatisierten Analyse und einer Weiterverwendung der gespeicherten Aufnahmen ergeben sich dabei Beeinträchtigungen schützenswerter Privatbereiche, die gegebenenfalls deutlich darüber hinausgehen, womit Menschen in der Öffentlichkeit ohnehin immer rechnen müssen.

Durch die Unkenntlichmachung der identifizierenden Merkmale auf dem Videobild kann dieser Gefahr effektiv begegnet werden, weil sich die aufgezeichneten Informationen nicht mehr direkt oder zumindest nur noch sehr beschränkt mit konkreten Personen in Verbindung bringen lassen. Abhängig von der konkreten Implementierung der unabhängigen *Schlüsselinstanz* wird ein solcher Eingriff nur ermöglicht, wenn durch sie ein legitimer Grund für diesen Eingriff erkannt wird – etwa zur Nutzung als Beweismittel bei einem Ladendiebstahl oder einer Körperverletzung. Zudem können in einem solchen Fall gegebenenfalls auch nur bestimmte Bildbereiche oder Zeitabschnitte freigegeben werden. Mit Blick auf die im Urteil des Bundesverfassungsgericht zum BKA-Gesetz geforderte unabhängige Datenschutzinstanz zur Sichtung und Freigabe von Videomitschnitten bieten sich ebenfalls mögliche Implementierungen für DTK-Systeme an. Für beide Szenarien zeigt sich somit, dass der Einsatz eines DTK-Systems gegenüber einer klassischen Videoüberwachung die Privatheit Betroffener besser schützen kann und legitime Eingriffe in diesen schutzwürdigen Bereich gezielter vorgenommen werden können.

Gesellschaftszentrierte Perspektive Der Begriff ‚Überwachungsgesellschaft' verweist vor allem auf die Allgegenwart von umfassender privater oder staatlicher Beobachtung aller Mitglieder einer Gesellschaft. Wird der Begriff im Kontext von Videoüberwachung gebraucht, so geht es also gerade nicht um vereinzelte Beobachtungen eng umgrenzter Bereiche, sondern um die allmähliche Proliferation dieser Sicherheitsmaßnahme und die Gefahr der schleichenden Vernetzung und Zusammenführung gewonnener Informationen. Auch in diesem Kontext muss staatliche Videoüberwachung immer im Kontext der Begrenzung der staatlichen Übermacht durch die effektive Garantie von Abwehrrechten gesehen werden. In jedem Fall beschreibt die Metapher einer ‚orwellschen Überwachungsgesellschaft'

aber insbesondere die Sorge, die Entwicklung könnte zu einer Situation führen, in der wir nahezu jederzeit beobachtet werden und nie genau wissen können, wie das eigene Verhalten interpretiert wird oder welche negativen Konsequenzen sich eventuell noch ergeben werden. Gesellschaftspolitisch impliziert dies das Risiko, dass die Wahrnehmung mancher Freiheiten einer Form von Selbstkontrolle zum Opfer fallen könnte: Aus der Angst, gespeicherte Informationen könnten zukünftig zu Nachteilen führen – etwa ein negatives privatwirtschaftliches Bonitätsranking oder die Klassifizierung als Hochrisiko-Fluggast – kann ein Normalisierungsdruck entstehen, der die Offenheit einer Gesellschaft de facto deutlich einschränkt. Die Metapher einer ‚kafkaesken Überwachungsgesellschaft' drückt zudem die Angst aus, gegen illegitim erlittene Nachteile effektiv keinerlei Mittel in der Hand zu haben, weil Betroffenen nie ganz klar ist, anhand welcher Informationen und Kriterien nachteilige Entscheidungen getroffen wurden und wie diese angefochten werden können. Durch Weitergabe bzw. Verkauf von Videoüberwachungsdaten ohne Zustimmung der Betroffenen entsteht hier die Gefahr einer umfassenden, kaum noch nachvollziehbaren Zusammenführung und späteren Zweckentfremdung – etwa zur Mustererkennung potentieller Straftäter oder möglicher Versicherungsrisiken.

Bei der klassischen Videoüberwachung lässt sich die Weitergabe, Zusammenführung und Zweckentfremdung gespeicherter Videodaten nur unzureichend einschränken. Auch wenn der Informationspflicht genüge getan und deutlich sichtbar auf die Videoüberwachung hingewiesen wird, kann der Einzelne nur sehr begrenzt absehen, was sich aus einer Zusammenführung von (Bild-)Informationen gewinnen ließe und wofür diese in Zukunft genutzt werden könnten. Zwar lassen sich einige der Risiken durch Selbstbeschränkungen der Betreiber ein Stück weit begrenzen, allerdings ist unklar, worin für private Akteure der Anreiz zu einem solchen Verhalten bestehen soll und welche Sanktionsmöglichkeiten es bei Datenmissbrauch effektiv geben kann. Beim Einsatz eines DTK-Systems lässt sich das Risiko einer Weitergabe, Zusammenführung und Zweckentfremdung der Bilddaten durch die unabhängige *Schlüsselinstanz* hingegen effektiv minimieren – insbesondere, wenn nur jene Bildinformationen entschlüsselt werden, die für den angegebenen Zweck unbedingt notwendig sind. Für private Betreiber einer Videoüberwachungsanlage ergibt sich zudem ein gewisser Anreiz zur Selbstbeschränkung, wenn mit einem erhöhten Schutz privater Kundeninformationen durch eine unabhängige *Schlüsselinstanz* geworben werden kann. Für beide Szenarien zeigt sich somit, dass der Einsatz eines DTK-Systems gegenüber einer klassischen Videoüberwachung die Privatheit der Betroffenen besser schützen kann und Eingriffe in diesen schutzwürdigen Bereich gezielter vorgenommen werden können.

5 Juristische Betrachtung

Gesetzliche Grundlagen für Videoüberwachung sowie Zwecksetzung des Gesetzes Mit § 6b BDSG existiert eine gesetzliche Grundlage, die der Wahrung des informationellen Selbstbestimmungsrechts durch einen Ausgleich angemessener Interessen Rechnung trägt [Bu00b, S. 92]. Auf der einen Seite steht hierbei das jedem Einzelnen zustehende Allgemeine Persönlichkeitsrecht aus Art. 2 I GG, wobei die bei einer Videoaufzeichnung tangierten Rechte im Wesentlichen das Recht am eigenen Bild, das Recht am gesprochenen Wort und das Recht auf informationelle Selbstbestimmung sind. Ziel des BDSG an sich ist es gem. § 3 BDSG auch, zur Datenvermeidung und Datensparsamkeit beizutragen.

Auf der anderen Seite steht die Pflicht der Gefahrenabwehr und der Strafverfolgung als öffentliche Aufgabe, sowie die Interessen Einzelner am Schutz ihres Eigentums oder anderer gefährdeter Rechtsgüter. § 6b I lässt jedoch die Videoüberwachung nur zum Zweck der Aufgabenerfüllung öffentlicher Stellen (Nr. 1), der Wahrung des Hausrechts (Nr. 2) oder zur Wahrung berechtigter Interessen für konkret festgelegte Zwecke (Nr. 3) zu. Daran zeigt sich zwar das gesetzgeberische Ziel, die Videoüberwachung nur in engen Grenzen zuzulassen, andererseits beschreibt Nr. 3 eine eng auszulegende Generalklausel, die eine solche aufgrund jeglicher objektiv bestehenden rechtlichen, wirtschaftlichen oder ideellen Interessen ermöglicht [Be13, Rn. 17]. Um beiden Seiten angemessen Rechnung zu tragen, ist die Videoüberwachung grundsätzlich verboten und nur unter den im folgenden Absatz zu erläuternden Voraussetzungen zulässig.

Voraussetzungen für eine Videoüberwachung Wie oben genannt, ist gemäß § 6b I BDSG die „Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung)“ nur unter den Bedingungen Nr. 1-3 zulässig. Hierbei stellt die Norm zunächst den Anwendungsbereich fest, der sich auf „öffentlich zugängliche Räume” erstreckt. Dieser weit zu verstehenden Begriff bezeichnet insbesondere öffentliche Plätze, Straßen, für Besucher zugängliche öffentlichen Gebäude, Bahnsteige, Schalterhallen, Museen oder Verkaufsräume [Bu00a, S. 38].

Bei der Beobachtung kommt es nicht darauf an, ob es sich um eine zielgerichtete Beobachtung handelt oder ob diese bloße Nebenfolge ist. Entscheidend ist nur, dass diese von einer gewissen Dauerhaftigkeit geprägt ist [GK14]. Optisch-elektronische Geräte sind alle Geräte, die Bewegtbilder bzw. als solche wahrzunehmende Bildfolgen erzeugen und wahrnehmbar machen können [Be13, Rn. 12]. Umstritten ist, ob der Anwendungsbereich des § 6b BDSG nur bei einer Aufzeichnung eröffnet ist, oder ob auch bloße Beobachtung ohne Speicherung unter § 6b BDSG fällt. Angesichts der klaren Gesetzesbegründung, die darlegt, dass bei § 6b die Beobachtung selbst erfasst ist und es nicht auf das Erfordernis einer Speicherung des Bildmaterials ankommt [Bu01, S. 61], dürfte allerdings klar sein, dass auch das bloße Beobachten an die Voraussetzungen des § 6b BDSG gebunden ist. Denn schon ein solches ist geeignet, beim Bürger ein Gefühl des permanenten Beobachtetseins hervorzurufen, das zu erheblichen Verhaltensänderungen führen kann. Dies stellt einen Eingriff in das allgemeine Persönlichkeitsrecht und die allgemeine Handlungsfreiheit dar.

Voraussetzung für die Installation einer Videokamera ist es, einen der in § 6b I Nr. 1-3 BDSG genannten Zwecke zu erfüllen. Angesichts vorrangiger landessepzifischer Regelungen dürfte (Nr. 1), die Videoüberwachung zur Aufgabenerfüllung öffentlicher Stellen zulässt, eine eher untergeordnete Rolle spielen. Wichtiger ist (Nr. 2), die zur Wahrnehmung des Hausrechts eine Videoüberwachung rechtfertigt. Dieses steht im öffentlichen Raum den öffentlich-rechtlichen Stellen zu, erstreckt sich allerdings auch im Privaten auf durch das Hausrecht erfasste Räume. So steht z.B. einem Kaufhausinhaber innerhalb seiner Geschäftsräume ein Hausrecht zu, das eine Videoüberwachung zulässig macht. (Nr. 3) ist ein Generaltatbestand, der zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke eine Videoüberwachung rechtfertigt. Nach der Gesetzesbegründung dürfen sich nur nicht-öffentliche Stellen auf (Nr. 3) berufen [Bu01, S. 62]. Es genügt jedes rechtliche, ideelle oder wirtschaftliche Interesse, sofern es konkret festgelegt ist.

Zudem muss laut Gesetz eine Erforderlichkeitsprüfung sowie Interessenabwägung erfolgen. Entsprechend des allgemeinen Begriffsverständnisses der Erforderlichkeit setzt diese voraus, dass die Videoüberwachung für den jeweiligen Zweck geeignet ist und kein milderes Mittel, das die Zweckerreichung in gleicher Weise fördern kann, zur Verfügung steht [De10, Rn. 236]. Für die Eignung ist es ausreichend, dass die Zweckerreichung gefördert wird. Berücksichtigt werden muss an dieser Stelle, ob es wirtschaftlich zumutbare Alternativen zur Videoüberwachung gibt, was jedoch aufgrund hoher Personalkosten und der relativ kostengünstiger Technik regelmäßig zu verneinen sein wird [Be13, Rn. 21]. Die Interessenabwägung erfolgt anhand einer Verhältnismäßigkeitsprüfung, die die Interessen der Betroffenen im Vergleich zu der Durchsetzung der in Nr. 1-3 genannten Zwecke unter Berücksichtigung der konkreten Umstände des Einzelfalls betrachtet [Be13, Rn. 22].

Veränderung der juristischen Betrachtung aufgrund der *Digitalen Tarnkappe* (DTK) sowie nötige juristische Gesetzesänderungen Bei Etablierung der DTK stellen sich die Fragen, wie sich die Bewertung aus juristischer Sicht verändern würde und ob gesetzliche Änderungen nötig wären. Zunächst ist festzustellen, dass auch das System an sich an der Tatsache der Beobachtung mittels einer optisch-elektronischen Einrichtung nichts verändert. Die DTK ersetzt nicht die Kamera an sich, sondern ist ein zusätzliches nachgeschaltetes technisches System.

Ein *Tracking* zur Kundenprofilerstellung auf Seiten des Kaufhausinhabers wäre aufgrund wirtschaftlicher Interessen gem. § 6b I Nr.3 BDSG denkbar. § 6b II normiert die Pflicht, den Umstand der Beobachtung und die verantwortliche Stelle durch geeignete Maßnahmen kenntlich zu machen. Eine allgemeine Sichtbarkeit der Kamera reicht jedoch hierfür nicht aus, vielmehr wird eine separate deutliche Kennzeichnung mittels Hinweisschildern verlangt [Be13, Rn. 27]. Würde ein DTK-System installiert, könnte auf einem solchen Hinweisschild zusätzlich eine Internetadresse angegeben sein, über die man auf zugehörige, vorab hinterlegte AGBs zugreifen kann und erfährt, wie man am Prämien-Programm teilnehmen und dabei auf seine Anonymisierung verzichten kann.

Bezüglich der Erforderlichkeit stellt sich die Frage, ob das DTK-System ein gleich geeignetes, milderes Mittel ist. Aufgrund der standardmäßigen Anonymisierung aller Personen, wäre durch die DTK die Persönlichkeitsrechtsverletzung behoben und ein hoher Persönlichkeitsrechtsschutz gewährleistet. Damit wäre die Verwendung einer Kamera samt DTK ein milderes Mittel. Fraglich ist allerdings, ob das System auch gleich geeignet ist. In öffentlich zugänglichen Räumen soll eine Videokamera meist auch der Gefahrenabwehr dienen, insbesondere die Strafverfolgung erleichtern und einen Abschreckungseffekt erzielen. Videoüberwachung ist für die Strafverfolgungsbehörden wichtig, weil Täter identifiziert und ihnen eine Straftat nachgewiesen werden kann. Bei der Speicherung anonymisierter Bildaufnahmen kann eine solche Identifizierung erst nach einer Deanonymisierung erfolgen. Bei konkreten Anhaltspunkten für eine begangene Straftat kann die Polizei einen Schlüssel zur Deanonymisierung anfordern, der mittels einer staatsanwaltschaftlichen Verfügung oder eines richterlichen Beschlusses erteilt werden könnte. Dadurch könnte es zwar vereinzelt zu einer insgesamt längeren Speicherung der Aufnahmen kommen, dies ist hinsichtlich des erhöhten Persönlichkeitsrechtsschutzes jedoch eine hinnehmbare Nebenfolge. Auch die kurzen zeitlichen Verzögerungen bei der Identifizie-

rung der Täter fallen angesichts heutzutage langwieriger Strafprozesse nicht weiter ins Gewicht. Bezüglich des Abschreckungseffektes würden sich keine Änderungen ergeben, da die Anonymität auf den Aufnahmen nur so lange besteht, wie die *Schlüsselinstanz* nicht der Deanonymisierung zugestimmt hätte, und dies einem möglichen Täter bewusst wäre. Das System kann somit aufgrund seiner Gewährung eines hohen Persönlichkeitsrechtsschutzniveaus unter Wahrung der staatlichen Strafverfolgungsinteressen überzeugen. Es bedürfte lediglich einer gesetzlichen Ausgestaltung, die die Herausgabemöglichkeit der Deanonymisierungs-Schlüssel normiert.

6 Diskussion und Ausblick

Wie in der Einleitung erwähnt, ist das Konzept DTK keinesfalls auf Kamerasysteme beschränkt. Das Prinzip verschlüsselt abgespeicherter Daten, die nur durch eine unabhängige *Schlüsselinstanz* freigegeben werden können, lässt sich auf jegliches Szenario anwenden, bei dem sensible personenbezogene Daten anfallen. Das gleiche gilt bedingt für das Prinzip, dass Personen freiwillig ihrer eigenen Deanonymisierung zustimmen. Hierbei ist szenariospezifisch zu prüfen, wie sich diese Personen dem DTK-System zu erkennen geben. Entscheidend für den erfolgreichen Einsatz ist, dass das User-Interface sowohl für potentiell aufgezeichnete Personen, die *Auswertenden* als auch die *Schlüsselinstanz* leicht zu verstehen und intuitiv zugänglich ist.

Ziel dieser Arbeit war es, einen Anstoß für Technologien und multidisziplinäre Auseinandersetzungen zu geben in Richtung von mehr Transparenz und Selbstbestimmung über personenbezogenen Daten. Eine über den Prototyp hinausgehende Nutzung des vorgestellten DTK-Kamerasystems erfordert ausgefeilte automatische Bilderkennungsalgorithmen. Die entsprechende Technik steht oder wird in absehbarer Zukunft zur Verfügung stehen! Es ist den Autoren bewusst, dass eine Ausschwärzung auf Videos keine absolute Anonymität bedeutet, da eine ausgeschwärzte Person z.B. an ihrem Hund erkannt oder bei flächendeckender Überwachung ab ihrer Wohnung verfolgt werden könnte. Wie gezeigt wurde, birgt das Konzept in vielen Szenarien jedoch Vorteile gegenüber klassischer Überwachung, was ein wichtiger Schritt zu zielgenaueren Eingriffen, mehr Bewusstsein und größerer persönlicher Autonomie im Zeitalter von ‚Big Data' und Terrorbekämpfung ist.

Literaturverzeichnis

[An06] Anderson, R.; Bond, M.; Clulow, J.; Skorobogatov, S.: Cryptographic Processors - A Survey. Proceedings of the IEEE, 94(2):357–369, Feb 2006.

[ARS09] Andriluka, Mykhaylo; Roth, Stefan; Schiele, Bernt: Pictorial structures revisited: People detection and articulated pose estimation. In: Proc. CVPR. IEEE, S. 1014–1021, 2009.

[Be12] Benenson, Rodrigo; Mathias, Markus; Timofte, Radu; Gool, Luc Van: Pedestrian detection at 100 frames per second. In: Proc. CVPR. IEEE, S. 2903–2910, 2012.

[Be13] Becker, Thomas: In (Plath, Kai-Uwe, Hrsg.): Kommentar zum BDSG sowie Datenschutzbestimmungen des TMG und TKG. Verlag Dr. Otto Schmidt, 1. Auflage, 2013.

[BMP12] Becker, Bernd; Müller, Günter; Polian, Ilia: Digital Tarnkappe: Stealth Technology for the Internet of Things. In (Gander, Hans-Helmuth; Perron, Walter; Poscher, Ralf; Riescher, Gisela; Würtenberger, Thomas, Hrsg.): Resilienz in der offenen Gesellschaft. Nomos, 2012.

[Bu00a] Bundestags-Drucksache 14/4329, 13. Oktober 2000.

[Bu00b] Bundestags-Drucksache 461/00, 18. August 2000.

[Bu01] Bundestags-Drucksache 14/5793, 4. April 2001.

[CCK13] Cichowski, Janusz; Czyżewski, Andrzej; Kostek, Bożena: Visual Data Encryption for Privacy Enhancement in Surveillance Systems. In (Blanc-Talon, Jacques; Kasinski, Andrzej; Philips, Wilfried; Popescu, Dan; Scheunders, Paul, Hrsg.): Advanced Concepts for Intelligent Vision Systems: 15th International Conference, ACIVS 2013, Poznań, Poland, October 28-31, 2013. Proceedings. Springer International Publishing, S. 13–24, 2013.

[Ch09] Cheung, S.-C.S.; Venkatesh, M.V.; Paruchuri, J.K.; Zhao, J.; Nguyen, T.: Protecting and Managing Privacy Information in Video Surveillance Systems. In (Senior, Andrew, Hrsg.): Protecting Privacy in Video Surveillance. Springer London, London, S. 11–33, 2009.

[CKM09] Carrillo, Paula; Kalva, Hari; Magliveras, Spyros: Compression Independent Reversible Encryption for Privacy in Video Surveillance. EURASIP J. Inf. Secur., 2009:5:1–5:13, Januar 2009.

[CPV06] Cucchiara, Rita; Prati, Andrea; Vezzani, Roberto: A system for automatic face obscuration for privacy purposes. Pattern Recognition Letters, 27(15):1809 – 1815, 2006. Vision for Crime Detection and Prevention.

[DE06] Dufaux, F.; Ebrahimi, T.: Scrambling for Video Surveillance with Privacy. In: 2006 Conference on Computer Vision and Pattern Recognition Workshop (CVPRW'06). S. 160–160, June 2006.

[De10] Detterbeck, Steffen: Allgemeines Verwaltungsrecht. Verlag C.H.Beck, 8. Auflage, 2010.

[DT05] Dalal, Navneet; Triggs, Bill: Histograms of Oriented Gradients for Human Detection. In: Proc. CVPR. IEEE, S. 886–893, 2005.

[Eu12] Europäische Kommission: Vorschlag für Verordnung des europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung). 2012.

[GG00] Grin, John; Grunwald, Armin, Hrsg. Vision assessment: shaping technology in 21st century society towards a repertoire for technology assessment. Springer, 2000.

[GK14] Gola, Peter; Klug, Christoph: Zur datenschutzrechtlichen Zulssigkeit der Videoberwachung. Recht der Datenverarbeitung, S. 65–74, 2014.

[Gr99] Grunwald, Armin: TA-Verständnis in der Philosophie. In (Bröchler, Stephan; Simonis, Georg; Sundermann, Karsten, Hrsg.): Handbuch Technikfolgenabschätzung, S. 73–81. Edition Sigma, 1999.

[Hu14] Huber, Matthias; Müller-Quade, Jörn; Nilges, Tobias; Thal, Carolin: A Provably Privacy Preserving Video Surveillance Architecture for an Assisted Living Community. In: 44. Jahrestagung der Gesellschaft für Informatik, Informatik 2014, Big Data - Komplexität meistern, 22.-26. September 2014 in Stuttgart, Deutschland. S. 563–574, 2014.

[LH08] Leykin, A.; Hammoud, R.: Real-time estimation of human attention field in LWIR and color surveillance videos. In: Proc. CVPRW. IEEE, S. 1–6, 2008.

[Li07] Liu, Xiaoming; Krahnstoever, N.; Yu, Ting; Tu, P.: What are customers looking at? In: Proc. AVSS. IEEE, S. 405–410, 2007.

[Ly09] Lyon, David: Surveillance Studies. An Overview. Polity Press, 2009.

[Ot05] Ott, Konrad: Technikethik. In (Nida-Rümelin, Julian, Hrsg.): Angewandte Ethik: die Bereichsethiken und ihre theoretische Fundierung: ein Handbuch, S. 568–647. Kröner, 2. Auflage, 2005.

[Pe99] Petermann, Thomas: Technikfolgen-Abschätzung – Konstituierung und Ausdifferenzierung eines Leitbilds. In (Bröchler, Stephan; Simonis, Georg; Sundermann, Karsten, Hrsg.): Handbuch Technikfolgenabschätzung, S. 17–49. Edition Sigma, 1999.

[Pe06] Pegarkov, Daniel D.: National Security Issues. Nova Publishers, Januar 2006.

[PLCFR15] Padilla-Lopez, Jose Ramon; Chaaraoui, Alexandros Andre; Florez-Revuelta, Francisco: Visual privacy protection methods: A survey. Expert Systems with Applications, 42(9):4177 – 4195, 2015.

[PP10] Paar, Christof; Pelzl, Jan: Introduction to Public-Key Cryptography. In: Understanding Cryptography. Springer, 2010.

[RDK11] Ruhrmair, Ulrich; Devadas, Srinivas; Koushanfar, Farinaz: Security based on Physical Unclonability and Disorder. In: Introduction to Hardware Security and Trust. Springer, S. 65–102, 2011.

[Sc07] Schiff, J.; Meingast, M.; Mulligan, D. K.; Sastry, S.; Goldberg, K.: Respectful cameras: detecting visual markers in real-time to address privacy concerns. In: 2007 IEEE/RSJ International Conference on Intelligent Robots and Systems. S. 971–978, Oct 2007.

[Se05] Senior, A.; Pankanti, S.; Hampapur, A.; Brown, L.; Tian, Ying-Li; Ekin, A.; Connell, J.; Shu, Chiao Fe; Lu, M.: Enabling video privacy through computer vision. IEEE Security Privacy, 3(3):50–57, May 2005.

[Sh11] Shi, Zhijie; Ma, Chujiao; Cote, Jordan; Wang, Bing: Hardware Implementation of Hash Functions. In: Introduction to Hardware Security and Trust. Springer, S. 27–50, 2011.

[TZ09] Trojanow, Ilija; Zeh, Juli: Angriff auf die Freiheit: Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte. Hanser, 2009.

[WSS10] Walk, Stefan; Schindler, Konrad; Schiele, Bernt: Disparity Statistics for Pedestrian Detection: Combining Appearance, Motion and Stereo. In: Proc. ECCV. IEEE, S. 182–195, 2010.