Verdächtiges Verhalten und automationsunterstützte soziale Kontrolle: "intelligente" Videoüberwachung zur Detektion von Kfz-Delikten

Rothmann, Robert; Vogtenhuber, Stefan

Veröffentlichungsversion / Published Version
Zeitschriftenartikel / journal article

Zur Verfügung gestellt in Kooperation mit / provided in cooperation with:
Centaurus-Verlag

Empfohlene Zitierung / Suggested Citation:
Rothmann, R., & Vogtenhuber, S. (2013). Verdächtiges Verhalten und automationsunterstützte soziale Kontrolle: "intelligente" Videoüberwachung zur Detektion von Kfz-Delikten. *Soziale Probleme*, *24*(2), 271-298. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-441287

Verdächtiges Verhalten und automationsunterstützte soziale Kontrolle

„Intelligente“ Videoüberwachung zur Detektion von Kfz-Delikten

von Robert Rothmann – Stefan Vogtenhuber

Zusammenfassung

Der vorliegende Beitrag präsentiert die soziologische Analyse eines automationsunterstützten sog. „intelligenten“ bzw. „smarten“ Videoüberwachungssystems zur Detektion von Kfz-Delikten. Das Überwachungssystem soll verdächtiges Verhalten in Garagen durch softwarebasierte Videoanalyse eigenständig erkennen und weitere Schritte zur Verfolgung der Täter einleiten. Hierzu ist geplant, das System mit diversen Funktionen und Sensoren aus dem Bereich der Gebäudeautomation zu koppeln. Die Analyse des Überwachungssystems zeigt eine deutliche Diskrepanz zwischen technischer Machbarkeit und den tatsächlichen Anforderungen im Alltag. Trotz der hohen jährlichen Deliktfallzahlen im städtischen Bereich, ist die Zahl an Vorfällen in den einzelnen Garagenobjekten verschwindend gering, vor allem in Relation zur Frequenz an Bewegungen und der Heterogenität an Aktivitäten. Zudem gibt es keinen haltbaren Nachweis darüber, wie typische Verhaltensmuster von Tätern tatsächlich aussehen. Dies hat eine hohe Zahl an Fehlalarmen zur Folge, weil auch normale Situationen als verdächtig eingestuft und als sicherheitskritische Momente vom Überwachungssystem produziert werden. Darüber hinaus gibt es eine Reihe an grund- und datenschutzrechtlichen Problemen. Es besteht die Gefahr diskriminierender automatisierter Einzelentscheidungen mit strafrechtlichen Konsequenzen für die Betroffenen. Der Einsatz eines derart konzipierten „intelligenten“ Überwachungssystems scheint auf Basis der vorliegenden Analyse nicht nur ineffektiv, sondern auch unverhältnismäßig.

1. Einleitung[1]

Wurde Videoüberwachung bisher vorrangig analog betrieben und in Echtzeit übertragen, zeigt sich in jüngster Zeit ein Trend in Richtung IP-basierter Monitoring- und Recording-Systeme. Die Technologie wird zudem von Jahr zur Jahr günstiger, was zu einer immer höheren Kameradichte führt. Bei der kontinuierlichen Sichtung der Monitore ist das Leitstellenpersonal jedoch notorisch überfordert. Die Bilder können nicht dauerhaft und zur Gänze überwacht werden. Mitunter helfen virtuelle Wächterrundgänge, die Vielzahl an Sichtfeldern zu überblicken und jede einzelne Kamera zumindest kurzzeitig im Kontrollraum aufzuschalten. Die Videodaten dienen auf diese Weise weniger der Kriminalprävention als der Einsatzkoordination im Anlassfall, sowie der nachträglichen Indiziensicherung (vgl. Töpfer 2009). Neben der fragwürdigen sicherheitstechnischen Effektivität dieser Anwendungs- und Einsatzweise (siehe z. B. Gill/Spriggs 2005; Welsh/Farrington 2002), gilt das manuelle Durchsuchen des Videomaterials als zeit- und kostenintensiv. Darüber hinaus sind bei der Speicherung und Sichtung des Materials eine Reihe an datenschutzrechtlichen Bestimmungen zu beachten. Missbrauch in Form zweckfremder Auswertung und selektiver Verdächtigung sind immer wieder Thema bei der Handhabe der Videodaten (Norris/Moran/Armstrong 1998; Norris/Armstrong 1999).[2]

1.1. Funktionale Ausrichtung und technische Zielsetzung

Die hier genannten Punkte werden nicht nur von soziologischer, sondern auch von technischer Seite erkannt und vorgebracht. Videoüberwachung wird dabei aber weniger als neoliberale Sicherheitsmaßnahme hinterfragt, sondern als technisch unausgereift verstanden. In Zukunft, so lautet die Vision, soll automationsunterstützte algorithmusbasierte (sog. „intelligente“ bzw. „smarte“) Videoanalyse zur Detektion von Objekten und Ereignissen, gekoppelt mit anderen (Sensor-)Funktionen aus dem Bereich der Gebäudeautomation, Überwachungsprozesse effizienter gestalten und die derzeitigen Schwachstellen beheben. In erster Linie geht es um Unterstützungs- und Filterwerkzeuge für das Leitstellenpersonal. Die Bilddaten müssen lückenlos und dauerhaft analysiert werden, um in Bedrohungsfällen rechtzeitig zielgerichtet Maßnahmen einleiten zu können.

In der hier vorgestellten Studie wird an der visuellen Detektion von Kfz-Delikten in Tiefgaragen und Parkhäusern gearbeitet. Von Seiten der technischen Entwickler steht die Annahme im Raum, ein auffälliges und zudem leicht erkennbares Merkmal von Kfz-Delikten ist das „*von Auto zu Auto Gehen"* als Vorbereitungshandlung der Täter oder Täterinnen bei der Auswahl des geeigneten Fahrzeugs. Dieses Bewegungsmuster soll automatisch erkannt werden und Alarm auslösen. Da Computerprozessoren mittlerweile in ausreichender Leistungsfähigkeit zur Verfügung stehen und Hersteller mehr und mehr dazu über gehen, Rechenkapazität auf der Kamera selbst zu integrieren, wird im hier vorgestellten Konzept zudem versucht, die algorithmusbasierte Analyse der Bilddaten in Echtzeit direkt vor Ort (*on the Spot*, *on Board*) auf dem Prozessor der Kamera durchzuführen. Das Videoüberwachungssystem analysiert permanent in Echtzeit, überträgt die Bilddaten jedoch nur im Anlassfall.

Um eine bedarfsträgergerechte und kostengünstige Lösung zu schaffen, werden die Daten über bereits bestehende Netzwerke der Gebäudeautomation (*Building Automation Systems*) übertragen. Als technische Herausforderung gilt hier die begrenzte Bandbreite derartiger Netzwerke, die bislang den Einsatz von Videostreaming verhindert hat.[3] Da akzeptable Reaktionszeiten auf punktuelle Ereignisse gefordert werden, bedeutet dies in letzter Konsequenz eine Reduktion der Videodaten auf einzelne Bilder oder Text (Ereignis-Code). Die Bildsequenzen wären aber nicht nur ereignisgesteuert, sondern auch bedarfsabhängig (per Knopfdruck) einholbar. Um die Beurteilung einer Situation in der Leitstelle zu erleichtern soll das Bildmaterial zudem aus einem definierten Zeitraum vor dem Alarm angefordert werden können (*Pre-Alarm*), wobei die Länge von den Speichermöglichkeiten im Prozessormodul abhängt. Angestrebt ist eine Datenaufzeichnung der letzten 5 bis 20 Sekunden. Darüber hinaus gehende Features, wie dauerhaftes Speichern des Videomaterials oder Echtzeit-Streaming, sind nicht vorgesehen.

Von technischer Seite wird hier versucht, sich von klassischer Videoüberwachung abzuheben und eine radikale Neuorientierung hin zu bildbasierten Sensoren bzw. „intelligenten" Bewegungsmeldern einzuleiten. Neben Kostenreduktion und Effizienz geht es dabei auch um datenschutzrechtliche Schranken. Durch die Reduktion des Bildmaterials soll die grundrechtliche Eingriffsintensität der Technologie abgemildert werden. Die Kamera analysiert Bilddaten mittels integriertem Prozessor vor Ort. Ein Speichern oder

Übertragen der Bilddaten findet entweder in sehr reduzierter Form oder überhaupt nicht statt, weshalb das technische Gerät nicht mehr als Kamera, sondern als „optischer Sensor“ bezeichnet wird (vgl. auch Belbachir 2010).[4] Dieser kann mit diversen weiteren Funktionen aus dem Bereich der Gebäudeautomation, wie z. B. Bewegungsmeldern, akustischen Sensoren zur Detektion von Glasbruch,[5] der Aktivierung von Alarmsirenen oder automatisierten Lautsprecherdurchsagen sowie der Bedingung von Kassenautomat und Schrankenbereich gekoppelt werden. Auch Kennzeichenerfassung und die visuelle Detektion von Rauch wären über die optischen Sensoren möglich. Es handelt sich hier um Bestrebungen, funktionaler Vernetzung und Automation, wie sie aktuell auch in anderen Projekten und Überwachungssystemen entwickelt und etabliert werden. So wird im *Domain Awareness System* der Stadt New York intelligente Videoüberwachung zur Nummerntafelerkennung mit Strahlungsmessungsstationen und externen Datenbanken für weitere Abgleiche verbunden.[6] Auch im EU-Projekt INDECT wird daran gearbeitet intelligente Videoüberwachung zur Ereigniserkennung mit anderen Funktionen und Datenbanken zur Informationsverarbeitung und automatischen Detektion von Bedrohungsszenarien zu verknüpfen.[7]

1.2. Soziologische Herangehensweise und Analyse

Die hier vorgestellte Zielsetzung und technisch-funktionale Ausrichtung des Überwachungssystems wird im Folgenden einer kritischen soziologischen Analyse unterzogen. Zuerst geht es um die Ermittlung des tatsächlichen Bedarfs zur Detektion von Kfz-Delikten. Es wird gezeigt, wo, wann und wie oft diese Delikte stattfinden und welche Merkmale Tatorte und Tätern aufweisen. Im Weiteren wird dann die Vorgehensweise bei den Einbrüchen spezifiziert. Es wird geklärt, welche Verhaltensweisen im Zuge des Tathergangs (Modus operandi) auftreten und ob es überhaupt markante Merkmale gibt, die dazu geeignet sind, per automationsunterstützter Videoanalyse als abweichend oder verdächtig erkannt zu werden.

Ein wesentlicher Schritt ist dabei der Abgleich der technischen Grundannahme und Definition verdächtigen Verhaltens (*Ground Truth* bei Musik 2011) mit der tatsächlichen Vorgehensweise der Täter und Täterinnen. Die Aufarbeitung erfolgt weiters über die Analyse der polizeilichen Kriminalstatistik, diverse Dokumente und (Beweis-)Videos, bis hin zu insgesamt elf

qualitativen Experteninterviews (vgl. Bogner/Littig/Menz 2002). Dabei wurde mit Softwareentwicklern, Exekutivbeamten, Streifenfahrern eines privaten Sicherheitsdienstes, Garagenbetreibern und Personen aus dem Bereich der Gebäude- und Immobilienverwaltung gesprochen. Zudem wurden drei ethnographische Videoanalysen (vgl. Knoblauch 2006; Knoblauch/Schnetter 2007; Reichertz/Englert 2011) und neun ethnographische Raumanalysen durchgeführt (vgl. Flick 2007; Hitzler 2007), um zu ermitteln, welche Bewegungsmuster mit welcher Frequenz in Garagen auftreten und mit welcher Häufigkeit sich Verhalten zeigt, dass der technischen Annahme bzw. dem Modus operandi (verdächtig) ähnlich ist. Auf Basis dieses Materials erfolgt eine Abschätzung potentieller Implikationen des technischen Einsatzes eines solchen Überwachungssystems. Abschließend werden datenschutzrechtliche Aspekte aufgearbeitet, wobei auf die Frage eingegangen wird, wieviel Autonomie dem Überwachungssystem zugestanden werden darf und wie sich die technische Neuausrichtung und Reduktion des visuellen Materials letztlich auf die grundrechtliche Eingriffsintensität auswirkt.

2. Kfz-Delikte als sicherheitskritisches Szenario

Wird von Kfz-Delikten gesprochen, so ist damit entweder der Einbruch in Fahrzeuge zum Diebstahl von einzelnen Gegenständen, oder der Diebstahl des gesamten Fahrzeugs gemeint. Rechtlich handelt es sich um schweren (gewerbsmäßigen) Diebstahl durch Einbruch (oder mit Waffen) gem. §§129 und 130 StGB. Die Aufarbeitung der Kriminalstatistik für Wien zeigt hierzu, dass von 1975 bis 2010 im Jahr durchschnittlich rund 13.000 Kfz-Einbruchsdiebstähle sowie rund 1.300 Kfz-Diebstähle angezeigt werden.[8] Die größere Fallzahl bei Einbruchsdiebstählen wird u.a. darauf zurückgeführt, dass diese Form des Kfz-Delikts leichter durchführbar ist und daher auch von weniger professionellen Tätern und Täterinnen begangen wird. Laut Aussagen der interviewten Experten findet der Einbruchsdiebstahl in Kraftfahrzeugen häufig spontan statt, wenn Wertgegenstände im Fahrzeug gesehen oder vermutet werden. Dabei spielt auch der geringe Aufwand zur Öffnung des Fahrzeugs durch das Einschlagen der Scheiben eine Rolle. Der Einbruchsdiebstahl in Autos gilt mitunter als Einstiegsdelikt von Jugendlichen. Auch Drogenabhängige werden dem weiteren Kreis der Täter und Täterinnen zugerechnet. Im Vergleich dazu dürften Kfz-Diebstähle, laut Polizei, tendenziell eher von

professionellern Tätergruppen mit entsprechender Hehlerstruktur verübt werden.

Weiters ist von Interesse an welchen Orten Kfz-Delikte vorkommen. Auswertungen des Bundeskriminalamts für das Jahr 2010 zeigen, dass der Einbruchsdiebstahl in Wien nur zu rund 14 Prozent und der Kfz-Diebstahl lediglich zu 3 Prozent in Garagen und Parkhäusern auftritt.[9] Der überwiegende Teil der Delikte passiert auf der Straße oder auf Freiluft-Parkplätzen. Vergleichbare Zahlen lassen sich auch für Großbritannien finden. Webb et al. (1992) stellen auf Datenbasis des *British Crime Survey* fest, dass nur rund 22 Prozent der Kfz-Diebstähle sowie rund 20 Prozent der Kfz-Einbruchsdiebstähle in so genannten *Car Parks* vorkommen.[10] Tilley (1993: 1) berichtet, „that the highest vulnerability to all car crime is found on the street". Es handelt sich hierbei um ein international auffindbares Muster (vgl. Clarke 2010; Hope 1987), welches schlicht dadurch entsteht, dass der überwiegende Teil aller Fahrzeuge auf der Straße abgestellt wird.

Die räumliche Verteilung der im Jahr 2010 in Wien angezeigten Kfz-Delikte zeigt, dass weniger einzelne Garagen sondern eher Gegenden bzw. Stadtteile betroffen sind. Während Kfz-Einbruchsdiebstahl tendenziell auch im Stadtzentrum auftritt, ist der Diebstahl von Fahrzeugen eher in den äußeren Bezirken und am Stadtrand zu finden.[11] Trotz der räumlichen Streuung von Kfz-Einbruchsdiebstählen gibt es spezielle Garagenobjekte, die als besonders anfällig gelten und immer wieder betroffen sind (so genannte *Hot Spots*). Laut Polizei handelt es sich meist um Garagen mit einer Größe von etwa 100 Stellplätzen aufwärts. Einer der wenigen klar objektbezogenen Hot Spots für Kfz-Einbruchsdiebstahl in Wien liegt im 20. Bezirk (Bereich Handelskai/ Millennium Tower). Es handelt sich hierbei um eine Garage, die sich in zwei Bauteile mit je rund 2.500 Stellplätzen untergliedert, die wiederum mit einem Einkaufszentrum, einem Bürogebäude sowie einem Wohnblock verbunden sind. Im Jahr 2010 wurden dort insgesamt 149 Kfz-Einbruchsdiebstähle angezeigt. Die Zahl strafrechtlich relevanter Vorfälle ist jedoch in Relation zur täglichen Frequenz an Fahrzeugen, Personen und Handlungen zu sehen. Laut Angaben des Garagenbetreibers kann pro Tag mit etwa 500 Kunden bzw. Fahrzeugen gerechnet werden, was eine jährliche Zahl von rund 182.500 Fahrzeugen ergibt, die sich in der Garage bewegen.

Vergleichbare Zahlen über bekanntgewordene Vorfälle in Objekten öffentlicher Garagenbetreiber liefern statistische Aufzeichnungen der Wirt-

schaftskammer Wien (WKW). So hat ein Betreiber mit 43 Objekten im Jahr 2010 insgesamt 321 Vorfälle gemeldet, was im Durchschnitt über ein Jahr rund 7 Delikte pro Garage ergibt. Im Fall eines anderen Betreibers sind es 68 Delikte auf 19 Garagenobjekte, also rund vier Delikte pro Jahr und Objekt. Bei den registrierten Vorfällen der WKW handelt es sich jedoch überwiegend um Automatenbetrug, Vandalismus und Anfahrschäden. Kfz-Delikte werden nicht als eigene Kategorien geführt, was darauf hinweist, dass andere sicherheitskritische Ereignisse häufiger vorkommen oder für die Garagenbetreiber wichtiger sind.[12] Es zeigt sich eine tendenzielle Flüchtigkeit des Delikts. Auch wenn in Wien jährlich mehrere tausend Einbrüche gemeldet werden, gestaltet sich die Erfassung eines einzelnen Vorfalls aufgrund der Vielzahl an potentiellen Fahrzeugen, Garagen und Personen relativ schwierig.

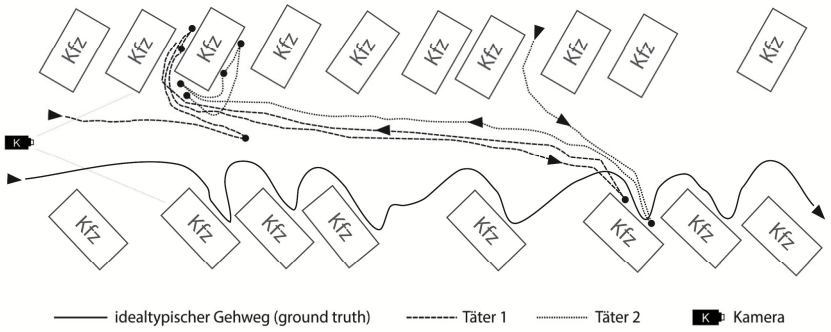
2.1. Modus operandi

Zudem variiert die konkrete Vorgehensweise der TäterInnen je nach Situation. So sind Tatzeit und Dauer bspw. abhängig von Tatort und Diebesgut. Es gilt zwischen dem Ausbau von Gegenständen (z. B. Airbags) und dem Diebstahl von lose zurückgelassenen Wertsachen zu differenzieren. Airbags oder serienmäßig eingebaute Navigationsgeräte werden aufgrund des zeitlichen Aufwands für den ordnungsgemäßen Ausbau (ohne Beschädigung) tendenziell nachts und in großen Wohnhausgaragen gestohlen. In den geführten Interviews wurde auch von einer ganzen Reihe an Autoeinbrüchen in einer Garage gesprochen, woraus sich schließen lässt, dass sich die Täter und Täterinnen, insbesondere bei nächtlichen Einbrüchen in Wohnhausgaragen relativ ungestört im jeweiligen Objekt bewegen und ihrer Arbeit nachgehen.[13] In anderen Fällen ist es gerade die hohe Frequenz von Fahrzeugen und Personen, die es den Tätern ermöglicht, sich unauffällig und anonym zu bewegen.

Die von technischer Seite aufgestellte Annahme, über das Bewegungsmuster des „von Auto zu Auto Gehens“, konnte über Gespräche mit der Polizei und die Einsicht in Videomaterial einer Einbruchsserie zwar bestätigt werden, soweit erkennbar dürfte dieses Verhalten aber weniger eindeutig und idealtypisch auftreten, als von den Entwicklern erhofft und ursprünglich angenommen (siehe Abbildung 1). So wird vermutlich selten tatsächlich ein Auto nach dem anderen aus der Nähe begutachtet, sondern vielmehr überblicksmäßig nach speziellen Marken, Typen oder geeigneten Bedingungen

Ausschau gehalten. In einzelnen Fällen wird dann das Fahrzeug genauer inspiziert, wobei es darum geht, Wertgegenstände oder spezielle Airbagtypen und Navigationsgeräte im Fahrzeuginneren zu identifizieren. Abbildung 1 zeigt die idealtypische Bewegungslinie bzw. *ground truth*, sowie die annähernde Rekonstruktion einer Videosequenz mit zwei Tätern, wie sie sich durch das Objekt bewegen. Im Zuge des eigentlichen Einbruchs werden dann sämtliche Seitentüren und der Kofferraum des Fahrzeugs geöffnet. Das Videomaterial zeigt, wie die Täter das Fahrzeug wiederholt von beiden Seiten betreten und daran herumhantieren. Die tonlose Szenerie gleicht einer Autoreparatur.

Abbildung 1: Kfz-Delikt Szenario – (Idealtypische) Bewegungslinien des Auskundschaftens



Die Verifizierung der Grundannahme des „von Auto zu Auto Gehens“ steht demnach auf unsicheren Beinen. Wesentliches Problem ist, dass lediglich in Einzelfällen Videomaterial vorliegt, welches den eigentlichen Tathergang zeigt. Die derzeitige Ausrichtung der Kameras in Garagen dient aus rechtlichen Gründen nicht der Prävention von Kfz-Delikten sondern dem Eigentumsschutz der Garagenbetreiber. Die Einsicht in das Setting ist lückenhaft und meist auf Ein- und Ausfahrten oder Kassenautomaten beschränkt (siehe Kapitel zur ethnographischen Videoanalyse). Die Parkflächen mit den abgestellten Fahrzeugen werden meist überhaupt nicht oder nur grob mit einer

einzelnen Überblickskamera am Kopfende der Parkebene überwacht. Hinzu kommt die schlechte Bildqualität. Jede Handlung, die nicht unmittelbar vor der Kamera passiert, ist kaum mehr erkennbar. In vielen Fällen sind die Täter und Täterinnen überhaupt nur zu sehen, wenn sie das Garagenobjekt betreten oder das Sichtfeld der Kamera kurz durchqueren.

Auf Basis der durchgeführten Recherchen sind im weitesten Sinne unregelmäßiger Gang bzw. atypischer Richtungswechsel sowie wiederholtes Betreten des Nahebereichs von Fahrzeugen als verdächtige Merkmale zu nennen. Zudem können Situationen auffällig sein, in denen kein Kassenautomat benutzt wird oder die Garage zu Fuß betreten und auch wieder ohne Fahrzeug verlassen wird. Auch eine überdurchschnittlich lange Aufenthaltszeit in den Objekten kann verdächtig sein. Die tatsächliche Vorgehensweise im Zuge eines Einbruchs und das Verhalten im Nahebereich der Fahrzeuge bleiben aber weitgehend im Dunklen.

Etwas mehr Evidenz gibt es bzgl. der Techniken zum Öffnen bzw. Aufbrechen eines Fahrzeugs. Diese reichen vom Einschlagen einer (Seiten-) Scheibe, über das Öffnen mittels Schlüsselrohling bis hin zum sog. Abzieher (Ziehfix) oder Schloß-Stich. Wird das Fahrzeug per Fernsteuerung verriegelt, kann der Sperrvorgang auch mittels Funkstörer (*Jammer*) blockiert werden. Die Technik variiert je nach Autotyp, Situation und Täter. Für die videoanalytische Detektion ist letztlich entscheidend, dass sich der Vorgang des Einbrechens in vielen Fällen weder zeitlich noch bewegungstechnisch vom herkömmlichen Aufsperren mit Schlüssel unterscheidet.[14] Dies führt zu einer weiteren Reduktion der detektierbaren Fälle.

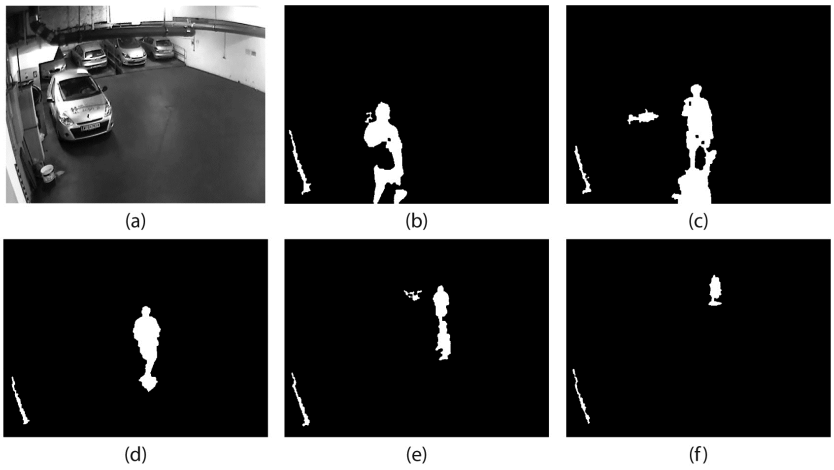
Um die technisch-visuellen Grenzen softwarebasierter Videoanalyse zu verdeutlichen wird in einem nächsten Schritt ein kurzer Blick auf die Methoden zur Detektion abweichenden Verhaltens geworfen.

3. Algorithmusbasierte Videoanalyse und Computer Vision

Die Methoden und Algorithmen rechnergestützter Bildverarbeitung variieren je nach Anwendung, Szenario und Setting (vgl. Adams/Ferryman 2013; Blauensteiner et al. 2010; Dick/Brooks 2003). Laut Angaben der technischen Entwickler kann die softwareseitige Umsetzung zur ereignisgesteuerten Videoüberwachung grundsätzlich wie folgt untergliedert werden: Erster elementarer Schritt ist das Erkennen und Segmentieren von Bewegungen (*Moti-*

on Segmentation). Objekte oder Personen werden so exakt wie möglich vom statischen Hintergrund getrennt, den das System gelernt hat. Das statische Referenz- bzw. Hintergrundbild ist jener Bereich, dessen Pixelwerte sich über mehrere Frames hinweg nicht ändern. Bewegt sich ein Objekt durch den videoüberwachten Ereignisraum wird dies anhand der sich von Frame zu Frame verändernden Pixelwerte erkannt (*Change Detection*), wobei ein Schwellenwert zu definieren ist, ab wann eine Veränderung auch tatsächlich als Bewegung gilt. Die sich bewegenden Bildbereiche bzw. Pixelcluster werden auch *Blobs* (engl. Klecks) genannt (siehe Abbildung 2). Je größer, kompakter und kontrastreicher diese sind, desto besser werden sie maschinell gesehen bzw. erkannt. Durch die Verwendung mathematischer Modelle zur Bewegungsvorhersage werden die sich bewegenden *Blobs* dann von einem Bild zum nächsten verfolgt (*Motion Tracking*). Die so errechneten Korrespondenzen von Bewegungen zwischen aufeinanderfolgenden Frames ermöglichen es, den Bewegungspfad (die Trajektorie) einzelner Objekte zu bestimmen.

Abbildung 2: Referenzbild und einzelne Frames mit segmentierten Bewegungen (Blobs)



In einem finalen Schritt werden die aufgezeichneten Trajektorien mit vorher gelernten Bewegungsmustern bzw. raum-zeitlichen Regeln verglichen (*Event Recognition, Behaviour Analysis*). Abweichungen von der so definierten Norm, wie zum Beispiel zielloses Herumwandern im Garagenobjekt oder wiederholtes Annähern an Fahrzeuge, werden erkannt und als sicherheitskritisches Ereignis gemeldet.

Abbildung 2 zeigt einzelne Frames einer Videosequenz aus dem Test-Setting. Die Bilder lassen erkennen, welchen optischen Irritationen die algorithmusbasierte Videoanalyse ausgesetzt ist. Frame (b) zeigt den segmentierten *Blob* einer Person, die den videoüberwachten Bereich aus der linken unteren Ecke betritt und sich in Richtung der geparkten Fahrzeuge bewegt. Der als Bewegung erkannte Bildbereich ist dabei immer wieder visuellen Störungen ausgesetzt. In Frame (b) fehlen Teile des Körpers, in Frame (c) und (e) werden Schatten bzw. Reflexionen am Boden mitdetektiert. Ähnliche Irritationen sind auch der Grund für die über alle Frames erkennbare Linie in der linken unteren Bildecke. Die segmentierte Person wird schließlich immer kleiner und ist gegen Ende kaum noch als Mensch erkennbar. Frame (f) zeigt jenen Moment, bevor der Bereich zwischen den parkenden Fahrzeugen betreten wird. Die hohe Wahrscheinlichkeit einer völligen Sichtverdeckung zwischen den Fahrzeugen ist offensichtlich.

Es wird klar, dass eine der zentralen Herausforderungen der visuellen Detektion im Annähern der Täter an das Zielfahrzeug liegt. Täter und Täterinnen sind dazu gezwungen, etwas genauer ins Wageninnere zu blicken, um potentielle Wertgegenstände erkennen zu können. Im Zuge dieser Inspektion ergeben sich Verdeckungen durch benachbarte und zum Teil eng geparkte Fahrzeuge. Dies gilt auch für die Bewegungen während des eigentlichen Einbruchs. Wird beispielsweise ein Airbag ausgebaut, muss dazu im Wageninneren herumhantiert, und laut Aussagen der interviewten Experten, zum Teil auch unterhalb des Lenkrads geschraubt werden. Hinzu kommen in Garagen mangelhafte Beleuchtung sowie diverse bauliche Eigenschaften (Säulen, Nischen, Raumhöhe) die robustes Tracking erschweren und einzelne Personen auf den weitläufigen Parkebenen zwischen den zahlreichen Autoreihen verschwinden lassen.

3.1. Grenzen algorithmusbasierter Videoanalyse

Die derzeitige Funktionsfähigkeit „intelligenter" Videoüberwachungssysteme wird generell oft überschätzt, wobei es laut Kammerer (2008) vor allem Halb- und Fehlinformationen über die Medien sind, die zu einer Verzerrung der Debatte beitragen. Bei der Beurteilung der Robustheit von Tracking und Detektion ist grundsätzlich zwischen (hoch) artifiziellen Laborbedingungen und realen Einsatzbereichen im Alltag zu differenzieren (vgl. auch Adams/ Ferryman 2013). Tatsächliche Anwendungen beschränken sich meist auf leicht detektierbare Szenarien in standardisierten oder architektonisch bzw. visuell vorteilhafte Situationen sowie auf Bereiche, in denen aufgrund von fehlenden sicherheitstechnischen Ansprüchen eine gewisse Rate an Fehldetektion nicht weiter stört (z. B. im Social Media-Bereich).

Die Schwierigkeit robuster Objektverfolgung und Verhaltensanalyse liegt an einer Reihe praktischer Probleme (vgl. Dick/Brooks 2003). Bei der Überwachung im Außenbereich sind es vor allem Veränderungen in den Lichtverhältnissen (Wolken, Regen, Sonnenuntergang etc.). Licht und Schatten sind aber auch im Indoor-Bereich ein Problem (Wechsel zwischen Kunst und Tageslicht, intermittierende Lichtquellen und Reflexionen etc.). Als zentrale technische Herausforderung gelten Sichtverdeckungen (*Occlusions*), wie sie auch in der oben beschriebenen Szene auftreten. Verdeckungen können durch verschiedene bauliche Elemente aber auch durch andere Personen verursacht werden und sind besonders in räumlich engen bzw. dichten Settings (*Cluttered Scenes*) ein Problem (Dick/Brooks 2003). Robuste visuelle Überwachung muss in der Lage sein, Objekte trotz partieller Verdeckung zu verfolgen. Robustes Tracking über mehrere Parkebenen und Gebäudeteile wäre eine essentielle Anforderung zur Ermittlung der Aufenthaltsdauer einzelner Personen in den Objekten.

Getrackte Objekte können aber auch ganz aus dem Blickfeld verschwinden und erst einige Zeit später wieder auftauchen, wobei das Überwachungssystem erkennen muss, ob es sich um dieselben Objekte bzw. dieselbe Person wie zuvor handelt. Man versucht das Problem der Verdeckung durch den Einsatz mehrerer Kameras mit überlappenden Sichtfeldern zu reduzieren (*3D Scene Reconstruction*). Dadurch ergeben sich aber weitere Schwierigkeiten durch die notwendige Kalibrierung. Wenn einzelne Kameras mit ihrer Aus-

richtung nach der Kalibrierung bewegt bzw. verrückt werden, kann dies zu Irritationen in der Analyse führen (Adams/Ferryman 2012).

Weitere Herausforderungen sind die Handhabe von Videomaterial in unterschiedlicher und zum Teil schlechter Qualität sowie die Gewährleistung der Analyse in Echtzeit (Dick/Brooks 2003). Auch einzelne Funktionsbereiche wie Einkaufswagen-Sammelstellen, Kassenautomaten oder Waschanlagen gilt es visuell zu definieren. Zudem sollten Personen immer ihrem Fahrzeug zugeordnet werden können. Ähnliches gilt für Personengruppen, die sich in der Garage aufteilen. Lernt das visuelle System selbstständig über die zuletzt getrackten Situationen (*adaptive On-Line Learning*), kann es zudem vorkommen, das die gelernte Norm langsam vom Ausgangswert abweicht (*Drifting*) (Grabner/Leistner/Bischof 2008; Santner et al. 2010).

Ein Problem algorithmusbasierter Ereigniserkennung in Garagen ist auch die längerfristige Differenzierung zwischen Hintergrundbild und Bewegungen im Vordergrund, da nicht bewegte Objekte vom System nach einiger Zeit wieder als Teil des Hintergrunds betrachtet werden (z. B. geparkte Fahrzeuge). Die ethnographische Garagenanalyse macht zudem deutlich, dass die Parameter der Software für eine adäquate Klassifikation von Verhalten, aufgrund der objektspezifischen Unterschiede immer wieder neu adaptiert und an den individuell Bedingungen des Settings ausgerichtet werden müssten.

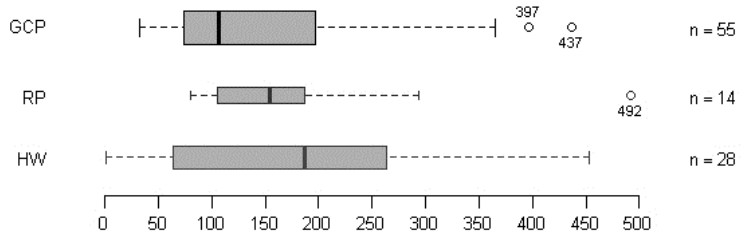
4. Ethnographische Video- und Raumanalysen

Zum tieferen Verständnis erfolgt nun die Darlegung der ethnographischen Raum- und Videoanalysen. Das erste videoanalysierte Objekt ist eine innerstädtische Garage (GCP-Garage) mit 330 Stellplätzen verteilt auf drei Ebenen. Neben Kunden mit Jahresvertrag weist das Objekt auch einen großen Anteil an Kurzparkern auf. Als zweites Objekt wurde eine Wohnhausgarage (RP-Garage) mit Dauerparkerbetrieb auf 150 Stellplätzen und drei Ebenen analysiert. Da es sich um eine Wohnhausgarage handelt ist der Zugang in das Objekt nur für Vertragskunden möglich. Das dritte Objekt ist eine Firmengarage (HW-Garage) mit 16 Stellplätzen auf einer Ebene. Es handelt sich hierbei um die kleinste Garage. Hinzu kommt die technische Besonderheit einer Hebebühne. Die Garage war auch das Test-Setting der technischen Entwickler unseres Projekts (Abbildung 2).

In allen drei Garagen wurde der Gebäudekern als Analyseeinheit herangezogen und das auf der (obersten) Parkebene im Bereich der Stellplätze vorgefundene Verhalten untersucht. Als Stichprobe wurden jeweils Werktage und das Zeitfenster von 17:00 bis 23:00 Uhr gewählt.[15] Tabelle 1 vergleicht die drei analysierten Objekte anhand von Größe (Stellplatzanzahl), Aufenthaltszeit (in Sekunden), und der Zahl an Bewegungen (n). Die Boxplot-Diagramme visualisieren die zeitliche Verteilung und ihre Ausreißer.

Tabelle 1: Deskriptive Statistik und Boxplot-Diagramme zur Aufenthaltszeit in Sekunden

Objekt (Größe)	Min.	1. Quartil	Median	3. Quartil	Max.	n
GCP (330)	32 Sek.	75 Sek.	106 Sek.	197 Sek.	437 Sek.	55
RP (150)	80 Sek.	109 Sek.	154 Sek.	185 Sek.	492 Sek.	14
HW (16)	1 Sek.	66 Sek.	187 Sek.	254 Sek.	453 Sek.	28



GCP-Garage: Innenstadtgarage mit Kurzparkerbetrieb (330 Stellplätze).
RP-Garage: Wohnhausgarage mit Dauerparkerbetrieb (150 Stellplätze).
HW-Garage: Firmengarage mit Geschäftsbetrieb, Test-Setting (16 Stellplätze).

Als zentrale Tendenz bzw. normkonstituierendes Verhalten läßt sich in allen drei Objekten erkennen, dass Personen das Objekt über einen der Personenzugänge betreten, mehr oder weniger direkt zum geparkten Fahrzeug gehen und dann aus der Garage fahren (bzw. umgekehrt bei einer Einfahrt). In der GCP-Garage tritt dieses Bewegungsmuster in 44 von insgesamt 55 Fällen auf. In der RP-Garage war es in zwölf von 14 Fällen zu erkennen. In der HW-Garage in 20 von insgesamt 28 Fällen. In einigen Situationen zeigen sich leichte Varianzen im Bewegungsablauf. So werden teilweise außerhalb des Fahrzeugs Jacken oder Mäntel angezogen oder Gegenstände in den Kof-

ferraum gelegt bzw. aus dem Kofferraum entnommen. In anderen Fällen ist wiederum zu beobachten, wie Beifahrer oder Beifahrerinnen aus dem Fahrzeug aussteigen, bevor dieses geparkt wird. Im Fall der HW-Firmengarage ist der Einfluss der Hebebühne auf die Bewegungsabläufe zu erwähnen, was dazu führt, dass teilweise Gegenstände wie Rucksäcke oder Mappen am Garagenrand abgelegt werden, bevor die Hebebühne hochgefahren und das Fahrzeug (aus-)geparkt wird.

In den übrigen Fällen (11 Fälle in der GCP-Garage, zwei Fälle in der RP-Garage und acht Fälle in der HW-Garage) waren „abweichende" Situationen zu beobachten. Dabei handelt es sich beispielsweise um Fälle, in denen Personen zu Fuß in die Garage kommen und diese auch wieder ohne Fahrzeug verlassen. Soweit erkennbar, wird dabei etwas ins Fahrzeug gebracht oder etwas aus dem Fahrzeug geholt (z. B. Tasche, Regenschirm). In anderen Fällen kommt es vor, dass Personen einen (markanten) Richtungswechsel vornehmen, während sie durch die Garage gehen, z. B. wenn etwas im Fahrzeug vergessen wurde. Auch Orientierungsversuche auf der Parkebene kommen vor, wobei das abgestellte Fahrzeug oder der Kassenautomat gesucht wird (zeitlicher Ausreißer GCP-Garage mit 397 Sekunden). Es zeigen sich auch Fälle, in denen Personen, nachdem sie ihr Fahrzeug geparkt haben, lange und teils verdeckt im Wageninneren herumkramen oder Gegenstände ein- bzw. ausräumen. Das Fahrzeug wird dabei auch immer wieder von beiden Seiten geöffnet und betreten. In einem dieser Fälle dauert dies auffällig lange (zeitlicher Ausreißer RP-Garage mit 8 Min. bzw. 492 Sek.).

In der HW-Firmengarage treten vermehrt Konversationen (zwischen Mitarbeitern und Mitarbeiterinnen) auf, die bis zu über sieben Minuten (453 Sek.) dauern (zeitliches Maximum HW-Garage). Eine andere atypische Situation zeigt, wie jemand kurz die Tür des Personenzugangs öffnet und für eine Sekunde einen Blick in die Garage wirft ohne diese zu betreten (zeitliches Minimum HW-Garage). In der Wohnhausgarage war zudem eine Situation mit freilaufendem Hund zu beobachten, wobei das Tier in typischer Weise ohne Systematik durch die Garage läuft und damit auch auf menschlicher Seite Varianzen im Bewegungsablauf hervorruft. Wiederum eine andere Situation zeigt, wie zwei Personen nach dem Parken ihres Fahrzeugs auf ein anderes Pärchen warten. Die Wartenden unterbrechen wiederholt ihren (langsamen) Gang und bleiben immer wieder kurz am Seitenrand der Fahrbahn stehen, um durchfahrenden Autos den Weg frei zu machen.

Unterschiedliche Bewegungskulturen

Die Videoanalyse zeigt die tägliche Heterogenität an Bewegungen sowie die Differenz der Bewegungskulturen in den Objekten. So ist in der GCP-Garage aufgrund von Größe, innerstädtischer Lage und Kurzparkerbetrieb die höchste Frequenz an (abweichenden) Bewegungen zu verzeichnen. Die Aufenthaltszeit ist mit durchschnittlich weniger als zwei Minuten (106 Sekunden) jedoch am kürzesten. Die anonyme Innenstadtgarage weist scheinbar die Tendenz zum kurzen Verweilen auf. Die RP-Wohnhausgarage zeigt hingegen für ihre Größe eine auffällig geringe Bewegungsfrequenz. Dies liegt vor allem daran, dass die Nutzung an einen dauerhaften Vertrag gebunden ist. Daraus generiert sich eine Population aus Bewohnern der unmittelbaren Umgebung. Obwohl das Objekt nur etwa halb so groß ist, liegt die durchschnittliche Aufenthaltszeit von rund zweieinhalb Minuten (154 Sekunden) über jener in der innerstädtischen GCP-Garage. Die Bewohner und Bewohnerinnen lassen sich also scheinbar mehr Zeit. Die durchschnittlich längste Aufenthaltszeit mit rund drei Minuten zeigt sich jedoch in der HW-Garage als dem räumlich kleinsten Objekt mit 16 Stellplätzen. Dies ist auf die Hebebühne sowie die Funktion als Firmengarage zurückzuführen.

Funktionale Heterogenität der überwachten Settings

Die über die Videoanalyse hinausgehenden ethnographischen Erkundungen in verschiedenen Objekten und Hot Spots (vgl. Douglas 1976; Flick 2007; Hitzler 2007), bestätigen die funktionale Heterogenität von Garagen als urbanes Setting. Es gibt eine Vielzahl an Typen, die sich nach Standort, Größe und Form (Grundriss), aber auch hinsichtlich Betreiber, Angebot und Management unterscheiden. So findet man innerstädtische Garagen mit abendlichem Theaterpublikum ebenso wie Garagen in der Peripherie mit Park & Ride Funktion zur Stoßzeit. Öffentliche Garagen mit einer hohen Frequenz an Kurzparkern sind weiters von Garagen in Wohnhausanlagen zu unterscheiden. Zudem gibt es Mischtypen in unterschiedlicher Organisationsform. Auch im Management reicht die Bandbreite von vollautomatisiert, über Betreuung zu Zeiten erhöhter Besucherfrequenz bis hin zu dauerhaft besetzt.

In Wien sind neben den zahlreichen Wohnhausgaragen rund 220 öffentlich gewerbliche Parkgaragen mit einer Anzahl von 50 Stellplätzen aufwärts zu finden. Zudem ist eine Vielzahl an Immobilienverwaltungsgesellschaften

und anderen privaten Betreibern im Garagenmanagement tätig. Als Parkprodukte werden Kurz-, Dauer- und Nachtparken, aber auch Kulturparken, Park & Ride, Park & Rail oder Park & Study angeboten.

Innerhalb der Garagen gibt es wiederum eine Reihe an verschiedenen Serviceangeboten wie Autovermietung, Autowaschanlagen, Behindertenparkplatze, Frauenparkplatze, aber auch Kundentoiletten, Regenschirmverleih oder Schuhputzmaschinen.[16] In einigen Garagenobjekten waren Bau- und Reinigungsarbeiten im Gange, in anderen wiederum Übungsautos einer Fahrschule geparkt oder Informationsschreiben des Garagenbetreibers hinter die Scheibenwischer einiger Dauerparker geklemmt. Auch Sammelstellen für Einkaufswägen, die Warenausgabe von Geschäften oder Zugänge zu Lagerräumen sind zu finden. In Wohnhausgaragen kann es vorkommen, dass Bewohner diverse Alltagsgegenstände lagern. Auch Fahrradabstellplätze und Müllsammelstellen sind integriert. In den Interviews wurde auch auf Garagen mit Gebrauchtwagenhandel verwiesen, weshalb in diesen Objekten ein gewisses „Kundentreiben" stattfindet. Viele der Angebote und Nutzungsformen können letztlich Verhaltensweisen und Bewegungsmuster hervorrufen, die dem Modus operandi von Autoeinbrechern ähnlich sind bzw. den als verdächtig definierten Bewegungen gleichen.

Evidenzbasierte Schätzung potentieller Fehlalarme

Die durchgeführte Analyse ermöglicht eine konkrete Abschätzung der Frequenz potentiell verdächtiger Situationen. So sind im Fall der GCP-Garage, auf einer von drei Parkebenen innerhalb eines Zeitfensters von sechs Stunden letztlich rund zehn auffällige Bewegungsmuster identifiziert worden. Geht man auf Basis dieser Daten davon aus, dass in einer Garage mit 300 Stellplatzen auf drei Ebenen innerhalb von sechs Stunden rund 30 auffällige oder abweichende Verhaltensmuster auftreten, ergibt das 120 abweichende Verhaltensmuster in 24 Stunden. Führt man diese Überlegung fort und nimmt an, die Daten werden in einem zentralen Kontrollraum eines privaten Sicherheitsunternehmens mit zehn weiteren etwa gleich großen Objekten gesammelt und sicherheitstechnisch verwaltet, so ergeben sich rund 1200 abweichende Verhaltensmuster in 24 Stunden bzw. pro Stunde durchschnittlich 50 Alarmmeldungen. Eine Detektion von Kfz-Delikten müsste demnach mit sehr hoher Wahrscheinlichkeit zwischen echten Autoeinbrüchen und anderen

möglicherweise in Teilen ähnlichen Verhaltensmustern differenzieren können, um dem Sicherheitspersonal im Alltag als Maßnahme hilfreich zu sein. Dies erscheint schwierig, da selbst die manuelle (analoge) Klassifikation der Bewegungsmuster im Zuge der ethnographischen Videoanalyse nicht immer eindeutig ausgefallen ist. So treten Situationen auf, die verschiedenen Handlungstypen zugeordnet werden können, also nicht trennscharf in eine einzelne Kategorie fallen. Die videoanalytische Beurteilung von Verhalten erfolgt aber auf einer deutlich abstrakteren Ebene und klammert einzelne Bewegungsdetails sowie intentionale Aspekte der Handlungsabläufe zwangsläufig aus. Im Gegensatz zu einer manuellen Beurteilung durch menschliches Personal fehlt dem algorithmusbasierten Überwachungssystem das Hintergrund bzw. Erfahrungswissen zur Einschätzung und Klassifizierung der verschiedenen Verhaltensweisen im jeweiligen Kontext.

Der Algorithmus als entscheidende Instanz

Digitale Systeme operieren grundsätzlich auf Basis binärer Codes (0/1). Der Entstehungsprozeß des Codes zur Verhaltensanalyse ist in einen spezifischen soziokulturellen Kontext eingebetet. Der Algorithmus arbeitet niemals vollkommen objektiv. Die Kriterien und Schwellenwerte zur Beurteilung, wann sich etwas verdächtig bewegt und wann nicht, unterliegen verschiedenen Ansichten und Wertigkeiten, die in die Software eingeschrieben sind und sich gewissermaßen im Code manifestieren (vgl. Bowker/Star 2000; Graham/Wood 2003; Musik 2011). Durch die algorithmusbasierte Videoanalyse erfährt das Verhalten der Individuen eine neue Form digitaler Präsenz auf einer Metaebene binär codierter Daten.

Die segmentierten Pixelcluster können im Sinne Baudrillards (1983) auch als Hyperrealität gesehen werden. Darunter versteht er die Reproduktion und Simulation des Realen in Form von Codes und Modellen. Simulation erhebt den Anspruch Realität abzubilden, und verschleiert zugleich deren Abwesenheit. Die auf abstrakter Datenebene simulierte Realität wird so zum vorrangigen realitätskonstituierenden Bezugspunkt, zur neuen daseinsbestimmenden Referenzkategorie, während die reale Welt mit ihren verkörperten Personen in den Hintergrund tritt (Baudrillard 1983; Lyon 2001: 116 ff.).

Doch algorithmusbasierte Verhaltenserkennung basiert auf Methoden statistischer Wahrscheinlichkeit. Ein Szenario wird, wenn überhaupt, im Ideal-

fall mit einem Fehlerniveau von $\alpha \leq 1\%$ erkannt. Dies bedeutet letztlich, dass keine Detektion ein eindeutiger Treffer ist. Es handelt sich immer um einen individuell festgelegten Schwellenwert probabilistischer Übereinstimmung. Wird dieser Schwellenwert zu hoch angesetzt, besteht die Gefahr ein sicherheitskritisches Szenario nicht zu erkennen (*false Rejection*). Wird das System jedoch sensibel eingestellt, impliziert dies eine hohe Zahl an Fehlalarmen (*false Acceptance*) (Introna/Wood 2004; Kammerer 2008).

Da Menschen dazu tendieren, die Information eines computerbasierten Systems der Information eines anderen Menschen gleichzustellen (Reeves/Nass 2002, zit. nach Adams/Ferryman 2013), oder dieses der menschlichen Wahrnehmung und Entscheidungsfähigkeit sogar vorziehen, kann angenommen werden, dass im praktischen Einsatz jede Detektion des Systems für gültig und berechtigt gehalten wird. Dies selbst, wenn das System sich getäuscht haben sollte und die Festgehaltenen zu Recht angeben, nicht die zu sein, für die man sie hält und nicht das getan zu haben, was man ihnen fälschlicherweise vorwirft (Introna/Wood 2004; Kammerer 2008). Die Entscheidung des Systems wird somit tendenziell unverhandelbar, was besonders dann ins Gewicht fällt, wenn wie im vorliegenden Konzept geplant, das Bildmaterial zur Verifikation des Szenarios weitgehend eingespart wird. Mit Bezug auf Lawrence Lessig (2001) formuliert Kammerer daher: „Im digitalen Überwachungssystem wird der Code zum Gesetz, wird der Algorithmus zur normsetzenden Kraft im Sozialen“ (Lessig 2008: 205).

5. Datenschutzrechtliche Implikationen

Das vorgestellte Videoüberwachungssystem verarbeitet personenbezogene Bilddaten, weshalb (in Österreich) u. a. das Grundrechte auf Privatsphäre (Art. 8 Abs 1 EMRK) und Datenschutz (§ 1 Abs. 1 DSG 2000) zur Anwendung kommt. Der Einsatz privatrechtlicher Videoüberwachung wird im Wesentlichen über Abschnitt 9a § 50a ff. des Datenschutzgesetzes geregelt. Dieser beinhaltet verschiedene Bestimmungen und Anforderungen (z. B. Zweckbindungsgrundsatz, Protokollierungs- und Löschungspflicht, Meldepflicht, Kennzeichnungspflicht, Verbot des automationsunterstützten Bilddatenabgleichs usw.) die im Fall der Inbetriebnahme einer Videoüberwachungsanlage zu berücksichtigen sind.

Teleologische Neuausrichtung (Kamera vs. Sensor)

Um geltenden datenschutzrechtlichen Bestimmungen auszuweichen und die Anwendung der Überwachungstechnologie weniger eingriffsintensiv zu gestalten, wird von technischer Seite angestrebt, die Kamera in ihrer Funktionsweise einem Sensor anzunähern. Dies vor allem durch die Integration des Prozessors auf der Kamera selbst, wodurch die Analyse ohne Datenübertragung in Echtzeit vor Ort (*on the Spot*) ermöglicht wird. Dies wiederum führt zu einer Reduktion der gespeicherten Bild- bzw. Videodaten. Auf Basis der derzeit gültigen rechtlichen Rahmenbedingungen scheint die technische Neuausrichtung jedoch nicht die gewünschten datenschutzrechtlichen Vorteile zu erbringen. So ist Videoüberwachung gem. § 50a Abs. 1 DSG als systematische, insbesondere fortlaufende Feststellung von Ereignissen durch technische Bildaufnahme- und Übertragungsgeräte definiert. Diese Formulierung trifft auch auf bildbasierte Sensoren zu, selbst dann, wenn diese kein Bildmaterial mehr speichern oder in den Kontrollraum übertragen, sondern lediglich über einen integrierten Prozessor vor Ort (*on Board*) analysieren. In datenschutzrechtlicher Hinsicht handelt es sich trotzdem um eine Videoüberwachungsvariante mit all ihren rechtlichen Bestimmungen. Fällt die Speicherung von Bild- bzw. Videodaten tatsächlich vollständig weg, was für eine teleologische Neukonfiguration in Richtung Sensor am vorteilhaftesten wäre, geht zudem die Sicherung von Beweismaterial, als eine bis dato zentrale Funktion von Videoüberwachung, verloren. Eine derartige Reduktion des visuellen Materials kann mitunter zu rechtlich-ethischen Implikationen führen.

Automatisierte Einzelentscheidung

Durch das Verschwinden der Bild- bzw. Videodaten klassifiziert das Überwachungssystem gänzlich autonom. Die Entscheidung darüber, ob es sich um verdächtiges oder strafrechtlich relevantes Verhalten handelt, findet ohne die Möglichkeit einer nachträglichen Verifizierung unter Ausschluß der menschlichen Wahrnehmung statt. Laut § 49 DSG darf jedoch niemand einer automatisierten Einzelentscheidung unterworfen werden, die rechtliche Folgen nach sich zieht oder zu einer erheblichen Beeinträchtigung führen kann, wenn diese Entscheidung ausschließlich aufgrund einer automationsunterstützten Verarbeitung von Daten zum Zweck der Bewertung einzelner Aspekte der Person oder deren Verhaltens ergeht (vgl. Hornung/Desoi 2011:

157 ff). Es sieht so aus, als würde sich der grundrechtliche Eingriff durch die angestrebte teleologische Neuausrichtung nicht verringern, sondern intensivieren. Letztlich würde eine von menschlicher Wahrnehmung entkoppelte, automationsunterstützte Klassifizierung von Verhalten stattfindet. Die Klassifizierung würde wiederum auf Basis vager Annahmen und unbewiesener Kriterien erfolgen und den Betroffenen kriminelle Absichten unterstellen, die sich aufgrund des fehlenden Bild- bzw. Videomaterials nachträglich nicht widerlegen lassen.

Automationsunterstützter Bilddatenabgleich

Zudem ist § 50a Abs. 7 DSG zur Regelung des sog. automationsunterstützten Bilddatenabgleichs zu erwähnen. Demnach dürfen die mit einer Videoüberwachung gewonnenen Daten von Betroffenen nicht automationsunterstützt mit anderen Bilddaten abgeglichen und nicht nach sensiblen Daten als Auswahlkriterium durchsucht werden. In seiner Bedeutung zielt Abs. 7 auf den Abgleich mit externen Bilddatenbanken. Die Formulierung „mit anderen Bilddaten" umfasst aber auch den Abgleich von Bildern innerhalb eines Videoüberwachungssystems. Dies wäre auch bei zeitlich aufeinanderfolgenden Einzelbildern (Frames) einer einzelnen Kamera der Fall. Der automationsunterstützte Vorher-Nachher-Abgleich auf Basis eines Referenzbildes ist ebenfalls ein Abgleich mit anderen Bilddaten und somit in der Beurteilung der Rechtmäßigkeit eines „intelligenten" Videoüberwachungssystems zu berücksichtigen. Bis dato liegt diesbezüglich jedoch kein Entscheidungsfall vor. Es gibt daher keine verbindliche Interpretation des Absatzes.

Praktische Umsetzung datenschutzrechtlicher Bestimmungen

Der Rechtsbereich hinkt hier der technischen Entwicklung allgemein hinterher. Es kann von klaren Diskrepanzen zwischen datenschutzrechtlichen Bestimmungen und ihrer Umsetzung gesprochen werden. Geltende Vorschriften werden in der Praxis selten in vollem Umfang berücksichtigt und eingehalten. Die Meldepflicht der Datenverarbeitung wird in der Praxis tendenziell vernachlässigt. Auch die Vorgaben im Hinblick auf Speichern und Löschen der Videodaten sind kaum überprüfbar. Von Betreibern und Entwicklern werden die datenschutzrechtlichen Vorschriften mitunter als bürokratisch und praxisfern empfunden. So gibt es ungeachtet der Rechtslage hinsichtlich

§ 50a Abs. 7 Unternehmen, die sich auf die Produktion und den Verkauf „intelligenter“ Videoüberwachungssoftware spezialisiert haben. Widersprüchlicher Weise wurde einer dieser Firmen das *European Privacy Seal* für die Entwicklung eines Software-Moduls zur Anonymisierung von Personen (*Privacy Protector*) verliehen.[17] Dies wirft wiederum fragwürdiges Licht auf derartige Datenschutz-Anreizsysteme.

6. Fazit

Technisches Ziel des Projekts war die Entwicklung eines automationsunterstützten bildbasierten Überwachungssystems zur Detektion von Kfz-Delikten in Garagen. Bei Kfz-Delikten handelt es sich um schweren gewerbsmäßigen (Einbruchs-)Diebstahl der besonders im städtischen Raum hohe Fallzahlen aufweist. Dennoch finden lediglich etwa 14 Prozent aller Kfz-Einbruchsdiebstähle in geschlossenen Settings wie Parkhäusern und Garagen statt. Die jährlichen Deliktfallzahlen in den einzelnen Objekten (*Hot Spots*) sind in Relation zur Größe der Objekte (mehrere hundert bis einige tausend Stellplätze verteilt über mehrere Parkebenen und funktional ausdifferenzierte Gebäudetrakte) und der täglichen Frequenz an Besuchern verschwindend gering. Robuste algorithmusbasierte Videoanalyse zur Ereigniserkennung von Kfz-Delikten in Garagen scheint unter diesen Umständen eine technisch kaum zu bewerkstelligende Herausforderung. Die verschiedenen Aktivitäten lassen sich selbst mittels analog-manueller Videoanalyse nicht immer eindeutig erkennen und klassifizieren.

Die ethnographische Videoanalyse bestätigt zwar, dass der überwiegende Teil aller Personen mehr oder weniger direkt vom Fahrzeug zum Ausgang bzw. umgekehrt vom Eingang zum Fahrzeug geht. Dennoch ist etwa ein Fünftel aller Bewegungen als abweichend zu bezeichnen und dem kriminellen Vorgehen der Täter und Täterinnen (Modus operandi) verdächtig ähnlich. Diese Fälle inkludieren Bewegungsmuster wie Hinein und Hinausgehen ohne Auto, unregelmäßiger Gang und Unterbrechen des Gangs, grober Richtungswechsel sowie wiederholtes Annähern und Betreten des Nahebereichs von Fahrzeugen. Auch überdurchschnittlich langes Verweilen in den Objekten zählt dazu. Die tatsächliche Vorgehensweise der Täter und Täterinnen bleibt jedoch unbestimmt. Es gibt letztlich keine haltbare Evidenz darüber, wie sich Täter und Täterinnen im Zuge von Kfz-Delikten auf der Parkebene wirklich

verhalten. Zudem können verdächtige Verhaltensmuster nicht trennscharf von anderen abgegrenzt werden.

Unternimmt man auf Basis der oben genannten Bewegungsmuster eine Schätzung potentieller Fehlalarme, so können sich im Fall der Verwaltung mehrerer Objekte über einen zentralen Kontrollraum, mitunter 50 verdächtige Situationen pro Stunde ergeben. Die Detektion müßte daher sehr exakt zwischen tatsächlichen Einbrüchen und anderen, teilweise ähnlichen Verhaltensmustern differenzieren können, um dem Kontrollpersonal als Maßnahme hilfreich zu sein. Um Fehlalarme zu vermeiden, wäre auch denkbar einen Verhaltenskatalog für das überwachte Setting aufzustellen. So ließe sich die max. Aufenthaltsdauer in bestimmten Objekten bspw. auf 10 Minuten beschränken. Freilaufende Hunde, Autoreparaturen, Reinigungsarbeiten oder übermäßiges Herumhantieren bzw. Ein- und Ausladen von Gegenständen, gälte es ebenfalls zu regulieren. Derartige (Haus-)Regeln und Maßnahmen sozialer Kontrolle scheinen aber wenig wünschenswert. Zudem stellt sich die Frage, wie diese Verhaltensregeln kommuniziert werden sollen. Sind die Regeln einmal bekannt, können sich Täter und Täterinnen darauf einstellen und ihr Vorgehen danach ausrichten.

Durch die technische Neuausrichtung des Überwachungssystems, welche eine Reduktion von Bilddaten vorsieht, würde die Möglichkeit zur Beweissicherung und Identifikation als bis dato zentrale Eigenschaft von Videoüberwachung wegfallen. Die Einsicht in das Setting zur Beurteilung des aktuellen Geschehens wird eingeschränkt. Die Analyse des Verhaltens wird der menschlichen Wahrnehmung weitgehend entzogen und auf das Überwachungssystem ausgelagert. Im Zuge visueller algorithmusbasierter Ereigniserkennung wird Verhalten auf Basis raum-zeitlicher Koordinaten und dem Verlauf von Bewegungslinien (Trajektorien) klassifiziert. Bewegungsdetails und Handlungsintentionen werden nicht berücksichtigt. Eine derartige Reduktion von Komplexität geht immer auch einher mit einer ungenauen Erfassung der sozialen Wirklichkeit. Insgesamt führt dies zu einer Automation von Verdächtigung. Auf individueller Ebene kann die Maßnahme falsche Anschuldigungen (*mistaken Identifikation*) zur Folge haben. Auf sozialer bzw. gesellschaftlicher Ebene kann automationsunterstützte Überwachung Verhaltensweisen unverhältnismäßig disziplinieren und einschränken (*chilling Effects*) und mittelfristig zu einem demokratiepolitischen Problem werden (vgl. Bennett/Raab 2006: 21; Peissl 2003).

Ungeachtet der kriminalpräventiven Effizienz und Trefferquote der diversen Softwaremodule stellt algorithmusbasierte Videoüberwachung aus soziologischer Perspektive eine Konkretisierung von Überwachungsprozessen dar. Videoüberwachung transformiert sich von einer allgemein-passiven Sicherheitsmaßnahme in eine spezifisch-aktive Technologie. An Stelle der sporadischen Beobachtung mit lediglich optionaler Auswertung des Bildmaterials tritt permanente Verhaltensanalyse mit Fokus auf speziell vordefinierte Merkmale. Dabei werden bestimmte Verhaltensfiguren für das System als verdächtig festgelegt. Diese in der Software eingeschriebenen Kriterien sind letztlich Verhaltensrichtlinien, die zu einer Verringerung der sozialen Varianz im jeweiligen Setting beitragen. Das Vermeiden potentiell verdächtiger Verhaltensfiguren reduziert die Kontingenz des Handelns (Krasmann 2005) und spezifiziert zugleich die gewünschte Norm. Dies vor allem dann, wenn das System mit weiteren Komponenten der Gebäudeautomation gekoppelt ist und in Teilen selbstständig operiert. Statt einem unspezifischen suggerieren allgemeiner Ordnung wird der Überwachungsvorgang in Form raumzeitlicher Koordinaten auf bestimmte Bewegungsmuster zugespitzt und mit weiteren Sensorfunktionen zur automationsunterstützten sozialen Kontrolle in Echtzeit ausgestattet.

Anmerkungen

1 Grundlage des Artikels ist das interdisziplinäre Forschungsprojekt *Networked mini-SPOT* (vgl. Rothmann/Vogtenhuber 2012). Als Teil der KIRAS Programmlinie wurde das Projekt durch die Österreichische Forschungsförderungsgesellschaft (FFG) und das Bundesministerium für Verkehr, Innovation und Technologie (BMVIT) finanziert. Das Projektkonsortium setzt sich zusammen aus dem Institut für Höhere Studien (IHS) in Wien (Abteilung für Soziologie, Arbeitsgruppe EQUI), dem Institut für Rechnergestützte Automation (*Automation Systems Group* und *Computer Vision Laboratory*) der TU Wien sowie dem Softwareunternehmen *CogVis Software und Consulting GmbH* und dem privaten Sicherheitsdienst *Hel-Wacht Bewachungsdienst GmbH*. Zusätzlich erfolgte eine externe Kooperation mit dem Garagenbetreiber *Best in Parking – Holding GmbH*.

2 Vgl. Wiener Zeitung, Printausgabe (14.10.2008): „Datenmißbrauch in U-Bahn-Stationen: Indizien erschüttern Vertrauen in Überwachung – U-Bahn-Bilder nicht sicher". [http://www.futurezone.orf.at], (28.10.2008): „Wieder Vorwurfe gegen Wiener Linien", [http://www.fuzo-archiv.at/artikel/317995v2].

3 Im Zuge des Projekts wurden u. a. die Protokolle KNX und ZigBee auf ihre Leistungsfähigkeit zur Übertragung von Bilddaten getestet (vgl. Schuster 2011). Für ein Bild mit einer

Größe von 30 KB benötigt das Protokoll KNX (TP1) rund 43 Sekunden und ZigBee als drahtloser Kommunikations-Standard rund 1,9 Sekunden.

4 Der Standard (13.7.2012): „Kamera ohne Bilder: Forscher entwickeln neuen Sensor". [http://derstandard.at/1342138998146/Kamera-ohne-Bilder-Forscher-entwickeln-neuen-Sensor]. Vorangetrieben werden derartige Anwendungen, z. B. auch im Bereich des *Ambient Assisted Living*, zur automationsunterstützten Sturzerkennung alter Menschen in ihrer Wohnung. Die Intimität und Sensibilität des Szenarios verlangt nach einer datenschutz- und privatsphärefreundlichen Lösung, die in der Entwicklung bildbasierter Sensoren gesucht wird (vgl. Fearless Project 2011-2013: [http://www.fearless-project.eu/].

5 Vgl. hierzu auch die akustische Detektion von Schüssen in den USA: [http://www. shotspotter.com/].

6 Vgl. Heise.de (2.08.2012): New York: Mit dem „Domain Awareness System" potentielle Terroristen und Verbrecher aufspüren: [http://www.heise.de/tp/blogs/8/152509].

7 Vgl. INDECT Project: [http://www.indect-project.eu/].

8 Polizeiliche Kriminalstatistik, Bundesministerium für Inneres, Abteilung II/9; Kriminalitätsbericht – Statistik und Analyse, Bundesministerium für Inneres/Bundeskriminalamt (1975-2010); vgl. auch Polizeiliche Kriminalstatistik 2010, BKA, Abteilung 4 – Kriminalanalyse; Spitzenwerte zeigen sich für das Jahr 2004 mit 32.818 Kfz-Einbruchsdiebstählen und für 2005 mit 4.028 angezeigten Kfz-Diebstählen.

9 Angaben lt. Bundeskriminalamt Wien (Referat 4.1.2) Strategische Kriminalanalyse.

10 Der Ausdruck *Car Park* umfasst in Großbritannien auch Freiluft-Parkplätze.

11 Angaben lt. Bundeskriminalamt Wien (Referat 4.1.2) Strategische Kriminalanalyse.

12 Quelle: WK Wien; vgl. Rothmann & Vogtenhuber 2012.

13 Vgl. Bundeskriminalamt Wien, Kriminalprävention, Kfz-Diebstahl/Einbruch: [http://www.bmi.gv.at/cms/BK/praevention_neu/vermoegen/KFZ_Diebstahl.aspx].

14 Siehe z. B. YouTube: „Polenschlüssel im Einsatz am Schloss von Skoda Porsche Seat Audi VW VAG Ford": [http://www.youtube.com/watch?v=sUXFUB6fR4E].

15 Fahrzeuge die lediglich die analysierte Ebene durchquerten (um auf eine der unteren Parkebenen zu kommen oder um von einer der unteren Parkebenen aus der Garage zu fahren) wurden gefiltert und nicht in die Analyse aufgenommen.

16 Wirtschaftskammer Wien (2008): Parken in Wien. Broschüre.

17 Vgl. EuroPriSe (*European Privacy Seal for KiwiVision Privacy Protector*): [https://www.european-privacy-seal.eu/awarded-seals/de-090017].

Literatur

Adams, Andrew A./Ferryman, James M., 2013: The Future of Video Analytics for Surveillance and its Ethical Implications. Security Journal (online publication 14 January 2013).

Baudrillard, Jean, 1983: Simulations. New York. Semiotext(e).

Belbachir, Ahmed N., 2010: Smart Cameras. Springer.

Bennett, Colin J./Raab, Charles D., 2006: The Governance of Privacy. Policy Instruments in Global Perspective. Cambridge, Mas.: The MIT Press.

Blauensteiner, Philipp/Kampel, Martin/Musik, Christoph/Vogtenhuber, Stefan, 2010: A Socio-Technical Approach for Event Detection in Security Critical Infrastructure (International

Workshop on Socially Intelligent Surveillance and Monitoring (SISM 2010) in conjunction with IEEE Intl. Conference on Computer Vision and Pattern Recognition (CVPR 2010)). San Francisco, CA, USA, June 2010.

Bogner, Alexander/Littig, Beate/Menz, Wolfgang, 2002: Das Experteninterview. Theorie. Methode. Anwendung [2. Auflage]. VS Verlag für Sozialwissenschaften.

Bowker, Geoffrey C./Leigh Star, Susan, 2000: Sorting Things Out. Classification and its Consequences. Cambridge, Mass: The MIT Press.

Clarke, Ronald V., 2010: Theft of and from Cars in Parking Facilities (Problem-Specific Guides Series No. 10). Washington, DC: U.S. Department of Justice. Office of Community Oriented Policing Services.

Dick, Anthony R./Brooks, Michael J., 2003: Issues in Automated Visual Surveillance. School of Computer Science, University of Adelaide, Australia.

Douglas, Jack, 1976: Investigative Social Research. Beverly Hills, CA: Sage.

Flick, Uwe, 2007: Qualitative Sozialforschung. Eine Einführung. Reinbeck: Rohwolt.

Gill, Martin/Spriggs, Angela, 2005: Assessing the Impact of CCTV. Home Office Research Study 292.

Grabner, Helmut/Leistner, Christian/Bischof, Horst, 2008: Semi-Supervised On-Line Boosting for Robust Tracking. S. 234-247 in: Computer Vision – ECCV 2008. 10th European Conference on Computer Vision, Marseille, France, October 12-18, 2008, Proceedings, Part I.

Graham, Stephen/Wood, David, 2003: Digitizing Surveillance. Categorization, Space, Inequality. Critical Social Policy 23/2: 227-248.

Hitzler, Ronald, 2007: Ethnographie. S. 207-218 in: Buber, R./Holzmüller, H.H. (Hrsg.), Qualitative Marktforschung, Konzepte – Methoden – Analysen. Wiesbaden: Gabler.

Hope, Tim, 1987: Residential Aspects of Autocrime. Home Office Research and Planning Unit Research Bulletin 23: 28-33.

Hornung, Gerrit/Desoi, Monika, 2011: „Smart Cameras" und automatische Verhaltensanalyse. Verfassungs- und datenschutzrechtliche Probleme der nächsten Generation der Videoüberwachung Kommunikation & Recht 3: 153-158.

Introna, Lucas D./Wood, David M., 2004: Picturing Algorithmic Surveillance. The Politics of Facial Recognition. Surveillance & Society 2/2-3: 177-198.

Kammerer, Dietmar, 2008: Bilder der Überwachung. Frankfurt/M.: Suhrkamp.

Knoblauch, Hubert, 2006: Videography. Focused Ethnography and Video Analysis. S. 69-83 in: Knoblauch, H./Schnettler, B./Raab J./Soeffner, H.-G. (Hrsg.) Video-Analysis. Methodology and Methods. Qualitative Audiovisual Data Analysis in Sociology. Frankfurt/M.: Peter Lang.

Knoblauch, Hubert/Schnettler, Bernt, 2007: Videographie. Erhebung und Analyse qualitativer Videodaten. S. 583-601 in: Buber, R./Holzmüller, H.H. (Hrsg.), Qualitative Marktforschung. Konzepte – Methoden – Analysen. Wiesbaden: Gabler.

Krasmann, Susanne, 2005: Mobilität: Videoüberwachung als Chiffre einer Gouvernementalität der Gegenwart. S. 308-324 in: Hempel, L./Metelmann, J. (Hrsg.): Bild-Raum-Kontrolle. Videoüberwachung als Zeichen gesellschaftlichen Wandels. Frankfurt/M.: Suhrkamp.

Lyon, David, 2001: Surveillance Society. Monitoring Everyday Life. Buckingham, Phil.: Open University Press.

Lessig, Lawrence, 2001: Code und anderer Gesetze des Cyperspace. Berlin: Berlin Verlag.

Musik, Christoph, 2011: The Thinking Eye is only half the Story. High-Level Semantic Video Surveillance. Information Polity 16/4: 339-353.

Norris, Clive/Moran, Jade/Armstrong, Gary, 1998: Algorithmic Surveillance. The Future of Automated Visual Surveillance. S. 255-276 in: Norris, C./Moran, J./Armstrong, G. (Hrsg.): Surveillance. Closed Circuit Television and Social Control. Brookfield, VT: Ashgate.

Norris, Clive/Armstrong, Gary, 1999: CCTV and the Social Structuring of Surveillance. S. 157-178 in: Painter, K./Tilley, N. (Hrsg.), Surveillance of Public Space. CCTV, Street Lighting and Crime Prevention Crime Prevention Studies, Volume 10. Monsey, N.Y.: Criminal Justice Press.

Peissl, Walter 2003: in Österreich: Eine Bestandsaufnahme, in: Peissl, Walter (Hg.) Privacy. Ein Grundrecht mit Ablaufdatum? Interdisziplinäre Beiträge zur Grundrechtsdebatte. Verlag der Osterreichischen Akademie der Wissenschaften. S. 155-177.

Polizeiliche Kriminalstatistik, Bundesministerium für Inneres, Abteilung II/9; Kriminalitätsbericht – Statistik und Analyse (1975-2010). Wien: BMI /BKA.

Reeves, Byron/Nass, Clifford, 2002: How People Treat Computers, Television, and New Media like Real People and Places [2. Auflage]. Standford, CA: CSLI.

Rothmann, Robert/Vogtenhuber, Stefan, 2012: Videoüberwachung, Ereigniserkennung und Automation. Eine sozialwissenschaftliche Machbarkeitsanalyse automationsunterstützter Videoüberwachung in Garagen und Aufzügen (Projektbericht). Institut für Höhere Studien, Wien.

Schuster, Felix, 2011: Transmitting Video Data over Narrow Bandwidth Control Networks. Diplomarbeit. Technische Universität Wien.

Santner, Jakob/Leistner, Christian/Saffari, Amir/Pock, Thomas/Bischof, Horst, 2010: PROST: Parallel Robust Online Simple Tracking. S. 723-730 in: Computer Vision and Pattern Recognition, 2010 IEEE Conference on 13-18 June 2010, Conference Publications.

Tilley, Nick, 1993: Understanding Car Parks, Crime and CCTV. Evaluation Lessons From Safer Cities. Police Research Group. Crime Prevention Unit Series Paper No. 42. London: Home Office Police Department.

Töpfer, Eric, 2009: Videoüberwachung als Kriminalprävention? Plädoyer für einen Blickwechsel. Kriminologisches Journal 4: 272- 82.

Webb, Barry/Brown, Ben/Bennett, Katherine, 1992: Preventing Car Crime in Car Parks. Police Research Group. Crime Prevention Unit Series: Paper No. 34. London: Home Office Police Department.

Welsh, Brandon C./Farrington, David P., 2002: Crime Prevention Effects of Closed Circuit Television. A Systematic Review. London: Home Office Research, Development and Statistic Directorate.

Suspicious Behaviour and Automated Social Control – Detecting Car Crime with "Smart" Video Surveillance

Abstract

The paper presents the sociological analysis of an automation-supported so-called "intelligent" or "smart" video surveillance system for the detection of car crime. The surveillance system aims to recognize suspicious behaviour in garages by software-based video analysis and to take steps to prosecute the perpetrators. For this purpose, the system is coupled with various functions and sensors of the building automation. The analysis of the surveillance system shows a discrepancy between the technical feasibility and the actual demands of everyday life. Despite the high annual number of car crime in urban areas, the number of incidents in each car park appears negligible, especially in relation to the frequency of situations and the heterogeneity of activities. There is no tenable evidence about what the so-called suspicious behaviour pattern of perpetrators actually looks like, and often ordinary situations could be regarded as suspicious producing security critical moments and leading to a high number of false positives. Moreover, the system faces a series of fundamental rights and data protection issues. There is a risk of automated discrimination with legal consequences for those concerned. The use of "smart" surveillance systems seems not only ineffective, but also disproportionate.

Robert Rothmann

MEDIACULT
Internationales Forschungsinstitut für Medien, Kommunikation und kulturelle Entwicklung
Marxergasse 48/8, A-1030 Wien

rothmann@mediacult.at

Stefan Vogtenhuber

Institute for Advanced Studies
Department of Sociology
Stumpergasse 56, A-1060 Wien

vogten@ihs.ac.at