Human Activity Recognition
KI-basiertes Gatekeeping im öffentlichen Raum

Gabriele Schabacher und Sophie Spallinger

1. Gatekeeping und Überwachung

Prozesse des Gatekeeping betreffen nicht nur die Frage, wer wo wann etwas tun darf. Sie beziehen sich nicht allein auf die Person, ihren Aufenthaltsort oder einen spezifischen Zeitpunkt, sondern gelten auch der Art und Weise, wie Personen sich *verhalten*. Gatekeeping zielt damit nicht nur auf Formen der Zugangskontrolle, die Subjekte aufgrund bestimmter Körpermerkmale und/oder mitgeführter Dokumente respektive Daten (Ausweis) zulassen oder abweisen. Gatekeeping betrifft auch, so die These dieses Beitrags, die Dimension konformen bzw. devianten Verhaltens und damit die Frage der jeweils erwünschten (öffentlichen) Ordnung, die durch die Regulierung aufrechterhalten oder auch erst errichtet werden soll. Solche verhaltensbezogenen Formen des Gatekeeping operieren deutlich unauffälliger als Verfahren der reinen Zugangskontrolle, was sie im Kontext heutiger Kontrollregime umso attraktiver macht – ihnen fehlt das sichtbare ›Gate‹ und ihr Interesse gilt nicht einzelnen Individuen, sondern (Gruppen-)Aktivitäten im Raum.

Es ist deshalb kein Zufall, wenn Formen und Verfahren der Beobachtung und Überwachung immer schon zu den Elementen von Gatekeeping gehört haben; denn der Torwächter – um beim klassischen Beispiel zu bleiben (vgl. Reichenbecher 2025 und Wietschorke 2025, in diesem Band) – muss zuallererst genau beobachten, wer oder was da in welcher Weise überhaupt auf ihn zukommt, um entscheiden zu können, wem er Zugang gewährt und wem nicht. Dabei sind die in Anschlag gebrachten Kriterien historisch, politisch und kulturell variabel, arbeiten aber stets mit einer Innen-Außen-Unterscheidung, die Akzeptiertes ›hinein‹ lässt, während das Abgewiesene ›draußen‹ bleiben muss. Übersetzt man dies mit Blick auf die Ordnung des öffentlichen Raums, die stets von ihrem Gegenteil (Unordnung, Unübersichtlichkeit, Vermischung) bedroht ist, ließe sich Gatekeeping als Duldung respektive Unterbindung bestimmter Verhaltensweisen verstehen. Die bei Gatekeeping-Prozessen involvierten Überwachungsregime sind dabei

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY-NC

nicht nur auf personale Akteure oder Institutionen (etwa die Polizei) angewiesen, sondern umfassen als infrastrukturelle Ensembles auch architektonische und informationstechnische Komponenten.[1] Unter den Bedingungen der Digitalisierung schließt dies auch KI-basierte Musterkennungssysteme (biometrische Erkennung, Objekterkennung, Verhaltenserkennung) ein, die zur automatischen Auswertung von Live-Videofeeds eingesetzt werden und unter bestimmten, vorab definierten Bedingungen Alarme generieren. Mit solchen ›intelligenten‹ Systemen verschiebt sich das Verhältnis von Überwachung und Gatekeeping, da KI-Technologien zunehmend selbst als Instanzen der Intervention und Entscheidungsfindung gesehen werden.[2] Im Sicherheitsbereich werden sie offiziell als »Unterstützungsinstrument« der Polizeiarbeit bezeichnet (Bundespolizei 2018: 7), das dem exekutiven Vollzug von Gatekeeping vorgelagert bleibt. Insbesondere mit Verhaltenserkennung respektive Aktivitätserkennung von, wie es heißt, polizeilich verdächtigem Verhalten,[3] wird die Hoffnung verbunden, »vor die Lage [zu] kommen« (Scheiwe 2023; vgl. IM BW 2018), die Technologien also präventiv nutzen zu können (vgl. Behr 2016). Gegenüber der bekannten, forensischen Nutzung automatisierter Videoanalyse zur Aufklärung von Straftaten (retrograde Auswertung) wird hier an eine Verhinderung (der Eskalation) von Straftaten gedacht, also eine raschere Intervention (vgl. Golda et al. 2022: 1489). Damit handelt es sich um ein präemptives Regime im Sinne des Predictive Policing (vgl. Kaufmann et al. 2019; Egbert/Leese 2021; Brayne 2021), das zukünftige Delikte verhindern soll. Gemäß der Logik präventiver Vorbeugung (vgl. Bröckling 2012) aber werden Gefühle der Unsicherheit und Sorge adressiert, um den Einsatz der Technologien zu rechtfertigen (vgl. Koch et al. 2016; Kaufmann/Wichum 2016; Grusin 2022).

Der vorliegende Beitrag will solche KI-basierten Videoerkennungssysteme in den Blick nehmen und spezifisch der Rolle von Human Activity Recognition

1 Zum medienkulturwissenschaftlichen Verständnis von Überwachungsregimen als infrastrukturellen Ensembles vgl. Schabacher 2021; zur Arbeit von Kontrollräumen vgl. Boersma 2025, in diesem Band; aus ethnografischer Perspektive zu Überwachungsregimen im Sicherheitskontext (Staatsgrenze, Flughafen, Gated Community) vgl. Low/Maguire 2019.

2 Im Kontext des autonomen Fahrens etwa werden Stufen der Autonomie unterschieden, die sich nach dem Grad der menschlichen Involviertheit beim Steuern des Fahrzeugs (Lenkrad) unterscheiden (*hands-on, hands-off, eyes-off, minds-off, steering-wheel-optional*) (Sprenger 2021: 26 f.). Im Hintergrund steht hier die Debatte um das ›Sehen‹ von Maschinen (vgl. Virilio 1989) und die von ihnen produzierten operativen Bilder (vgl. Farocki 2004; Pantenburg 2017; Parikka 2023; zu deren analoger Vorgeschichte Meyer 2019: 23).

3 Es geht hier also um die Erkennung von Bewegungen im Realraum. Nicht gemeint ist das Nutzungsverhalten bezogen auf den Datenverkehr von Personen, der im Rahmen von *dataveillance* schon systematisch für Profiling und Policing ausgelesen wird. Diese Form der Mustererkennung macht durch die homogeneren Daten weniger Probleme als die Erkennung in realweltlichen Settings.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY-NC

(Verhaltens- bzw. Aktivitätserkennung) für Prozesse des Gatekeeping im öffentlichen Raum nachgehen. Dies ist deshalb ein interessanter Fall, weil die relevanten Unterscheidungsprozeduren – also wer erwünscht ist und wer nicht, wer also als Bedrohung für Sicherheit angesehen wird und wer nicht – unter Absehung von (biometrischen) Identifikationsprozeduren allein durch den Rekurs auf das jeweilige Verhalten geleistet werden sollen.[4] Systeme der Verhaltenserkennung werden insofern auch als »datenschutzschonender« propagiert, als sie Regulierungsarbeit unter Anonymisierungsbedingungen erlauben (Bretthauer 2017: 132 f.; vgl. Golda et al. 2022: 1494). Anhand eines langjährigen Modellversuchs in Mannheim (seit 2018), für den eigens ein solches Verhaltenserkennungssystem entwickelt wurde, untersucht der Beitrag, welchen Bedingungen diese Form eines »distribuierten Gatekeeping« (Reichenbecher/Schabacher 2025: 14, in diesem Band) unterliegt, wie es operativ funktioniert und environmental implementiert ist und welche Reaktionen es zeitigt. Um diese Fragen zu beantworten, geht der Beitrag in fünf Schritten vor.[5] In einem ersten Schritt wird die Genealogie des Modellversuchs vor dem Hintergrund der globalen Entwicklung des Überwachungsdispositivs seit den 1990er Jahren einerseits sowie der spezifisch deutschen Datenschutzbestimmungen andererseits situiert. Unter Rekurs auf die politische Debatte wird zweitens erläutert, wie der Modellversuch mittels Kriminalitätsstatistiken und Bürgerbefragungen die Frage der Un-/Sicherheit – insbesondere die sogenannten ›Kriminalitätsschwerpunkte‹ – konzeptualisiert. In einem dritten Schritt wird skizziert, wie die Verhaltenserkennungssoftware entwickelt wurde und welche devianten Verhaltensweisen sie detektieren sollte. Dabei wird besonderes Augenmerk auf die Verfahren der Posenschätzung, das der Berechnung der Körperhaltungen dient, und der Messkampagnen, die realweltliche Trainingsdaten generieren sollen, gelegt. In einem vierten Schritt werden der praktische Einsatz in der Stadt Mannheim, die Ergebnisse und Fehler-Detektionen der Systeme, aber auch die Reaktionen der Öffentlichkeit untersucht; dabei wird ein angelagerter

4 Vgl. hierzu den Ansatz der Humandifferenzierung, der Unterscheidungen zwischen Menschen auf verschiedenen Ebenen analysiert. Dabei kommen als ›Ansatzpunkte ‹ der Differenzierung auch » individuelle zugerechnete situative Performances« in Betracht (Dizdar et al. 2021: 10).

5 Er kann sich dabei auf verschiedene Typen von Quellenmaterial beziehen, das im Rahmen des DFG-geförderten Forschungsprojekts »Urbane Kontrollregime. Bahnhöfe als Infrastrukturen der Humandifferenzierung« im SFB 1482 von 2021–2024 erhoben wurde. Dabei handelt es sich erstens um Beiträge zur öffentlichen Debatte, d. h. Dokumente des parlamentarischen Prozesses (Informationsvorlagen sowie Anfragen und zugehörige Antworten), Pressemitteilungen, Berichte, Dokumentarfilme und YouTube-Videos. Zweitens wurden zahlreiche Expert:innen-Interviews mit wichtigen Akteur:innen des Feldes (Kommunalpolitiker:innen, Datenschutzbeauftrage, Polizei, kritische Öffentlichkeit, beteiligte Wissenschaftler:innen) geführt und ausgewertet. Drittens fließen Ergebnisse aus der teilnehmenden Beobachtung bei Feldforschungsaufenthalten in Mannheim (2021, 2024) sowie in Hamburg (2023) ein.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY-NC

Test der Software in Hamburg mit einbezogen. Das abschließende Fazit bezieht die dargestellten Überlegungen noch einmal systematisch auf die Relevanz KI-basierter Erkennungssysteme für die Frage des Gatekeeping.

Der Beitrag vertritt die These, dass derartige Modellversuche die Probleme, zu deren Lösung sie antreten, erst herstellen müssen: Dies betrifft die Feststellung von Sicherheitsproblemen an bestimmten Orten ebenso wie die Festlegung, was überhaupt als deviantes Verhalten gelten soll. Angesichts der Tatsache, dass objektive Sicherheit nach wie vor nur im Verbund mit Polizeipräsenz vor Ort erreicht werden kann (vgl. OpenPetition 2018; Belina 2023), ist mit der Implementierung ›intelligenter‹ Überwachungstechnologien deshalb vor allem eine Gewöhnung an infrastrukturell weniger auffällige Gatekeeper verbunden, deren Funktionalität prinzipiell ausbaufähig ist. Es kann gezeigt werden, dass Prozesse des Gatekeeping nicht allein an Schwellen der Zugangskontrolle stattfinden, sondern mit dem Einsatz von Verhaltenserkennungssoftware auf unübersichtlichere und schwerer zu kontrollierende Settings ausgeweitet werden, worin ein Umweltlich-Werden von Gatekeeping-Verfahren zum Ausdruck kommt.

2. Zur Genealogie des Mannheimer Modellversuchs

Der Mannheimer Modellversuch, der automatisierte Verhaltenserkennung im öffentlichen Raum testet, stellt vor dem Hintergrund der globalen Entwicklung von algorithmenbasierten Überwachungstechnologien, aber auch mit Blick auf die deutschen Bemühungen einen interessanten Fall dar. Denn einerseits gilt die Entwicklung von Erkennungssystemen, die das Verhalten von Gruppen betreffen und damit eine neue Form von Crowd Control[6] möglich machen sollen, als hochaktuelles Forschungsfeld der Computer Vision (vgl. Gupta et al. 2022). Andererseits reagiert der Mannheimer Versuch auf spezifisch bundesdeutsche Rahmenbedingungen, die den Einsatz automatisierter Videoüberwachungssysteme im öffentlichen Raum strikt regulieren und – im Gegensatz zu anderen Ländern (etwa Australien, Indien, Israel oder, bekanntlich, China) (vgl. Avis et al. 2025; Low/Maguire

6 Während sich Crowd Control maßgeblich auf den Planungsansatz des *Crowd Management* (Fruin 1993; Runkel 2019) bezieht, schließt der vorliegende Beitrag stärker an die Perspektive des *Crowd Monitoring* (Monari et al. 2015) an, bei der die digitale Analyse der Personenströme in Menschenansammlungen ihrer Steuerung und Lenkung dient. Dabei werden im Videomaterial das Gesamtaufkommen, die Personendichte und -verteilung sowie das Bewegungsverhalten der Menschenmenge (etwa Stauungen) softwaregestützt analysiert. Zur medienwissenschaftlichen Perspektive vgl. Meyer 2014; aus den Surveillance Studies und bezogen auf die damit verbundene biopolitische Dimension vgl. Nishiyama 2018.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access -

2019) – nur unter eingeschränkten Bedingungen gestatten, u. a. in realweltlichen Test-Settings (vgl. Schabacher 2021; Marres/Stark 2022).[7]

Sicherheitsfragen sind in der Nachfolge von 9/11 zu einem bevorzugten Anwendungsfeld für KI-Systeme weltweit geworden. Dies betrifft die Überwachung von Verkehrssystemen, kritischen Infrastrukturen, Großveranstaltungen, aber auch von öffentlichen Gebäuden, Plätzen oder Ereignissen im privatwirtschaftlichen Raum. Dabei werden Formen visueller Überwachung mit der Überwachung des Datenverkehrs (*dataveillance*) zu Systemen der »automated video surveillance« verschaltet (Stanley 2019; vgl. Andrejevic 2020), wobei biometrische Erkennungsverfahren (Gesicht, Iris, Gang etc.) wie auch Objekt- und Verhaltenserkennung zum Einsatz kommen. Konkret geht es darum, die Bilder eines (Live-)Videofeeds bezogen auf spezifische Kriterien automatisch auszuwerten und in bestimmten Fällen einen Alarm auszulösen. Insbesondere die Covid-Pandemie hat die Datafizierung auf allen Ebenen vorangetrieben und damit Formen der Zugangsregulierung, die mit automatischer Identifizierung »at a distance« (Andrejevic/Volčič 2021: 142) arbeiten, also etwa mit biometrischer Gesichtserkennung, stark normalisiert. Die betreffenden KI-Unternehmen entwickeln mit der Verarbeitung derartiger Massendaten die Möglichkeit einer »granular biopower« (Andrejevic 2021: 144), die gleichermaßen auf der Ebene des Individuums wie auf der Ebene der Bevölkerung operiert.

Trotz der zunehmenden Normalisierung des Einsatzes von KI gestatten die Datenschutzbestimmungen in Deutschland automatische Erkennungssysteme im öffentlichen Raum nur unter spezifischen Bedingungen, etwa Terrorgefahr und Gefahrenabwehr auf bundespolizeilicher Ebene oder bei Maßnahmen zur Kriminalitätsbekämpfung auf landespolizeilicher Ebene. Erst die Anpassung der betreffenden Polizeigesetze macht die Tests im öffentlichen Raum möglich, die jeweils den länderspezifischen Rechtsgrundlagen, Zugriffsrechten sowie Transparenzpflichten unterliegen.[8] Da Videoüberwachung per se als Eingriff

7 In der Vergangenheit galten in Deutschland datenschutzrechtlich strengere Vorschriften für automatisierte Erkennungssysteme als in anderen Ländern. Diese Sonderrolle ist mit dem ›AI Act‹ der EU, der seit August 2024 hochrisikoreiche KI-Systeme in der EU verbietet, in Bewegung geraten. Allerdings gibt es vermehrt Ausnahmeregelungen, die es gestatten, diese Verbote im Namen der nationalen Sicherheit auszuhebeln (vgl. EU AI Act 2024 Art. 5 Abs. 1 mit Erwägungsgrund 24). In diesen Fällen gilt das jeweilige nationale Recht – im deutschen Kontext die Polizeigesetze der einzelnen Bundesländer. Es ist also bisher nicht einheitlich geregelt, wie das europäische Recht auf nationaler Ebene umzusetzen ist. Die europäische Datenschutzgrundverordnung greift in diesem Fall nicht, da es um Sicherheitsbelange geht (vgl. DSGVO Art. 2 Abs. 2 Buchst. d).

8 In Baden-Württemberg ist es etwa seit der Novelle des Polizeigesetzes vom 15. November 2017 erlaubt, »angefertigte […] Bildaufzeichnungen auch automatisch aus[zu]werten«, insofern dies »auf das Erkennen solcher Verhaltensmuster ausgerichtet [ist], die auf die Begehung

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY-NC

in das grundgesetzlich verbriefte Recht auf informationelle Selbstbestimmung (GG Art. 2 Abs. 1 sowie Art. 1 Abs. 1; BDSG § 4) gilt, muss ihr Einsatz stets zweckgebunden und verhältnismäßig sein, und er ist datenschutzrechtlich streng zu überprüfen. Aufgrund dieser Rahmenbedingungen müssen zahlreiche Aspekte der Testkonstellationen, die in anderen Ländern vergleichsweise ›unsichtbar‹ bleiben, in Deutschland explizit gemacht werden. Dies betrifft die Konzeptualisierung, die Implementierung sowie die Bewertung solcher Technologien für den öffentlichen Raum.

Der Mannheimer Modellversuch stellt nun eine solche bundesdeutsche Testkonstellation dar, die im Zusammenhang mit zwei Pilotprojekten steht, die das Bundesinnenministerium in Zusammenarbeit mit dem Bundeskriminalamt, der Bundespolizei und der Deutschen Bahn am Bahnhof Berlin Südkreuz 2017–2019 durchgeführt hat und die am Markt verfügbare Softwares zur Gesichtserkennung sowie zur Situations- und Verhaltenserkennung testeten:[9] Während es im ersten Test um die Identifikation von Personen ging, sollten im zweiten Test vordefinierte Gefahrensituationen (etwa ›liegende Person‹ oder schnelles Zusammen- oder Auseinanderlaufen von Menschen) erkannt werden. Da im zweiten Fall – anders als bei den in einer Datenbank hinterlegten ›Gesichtsbildern‹ – keine Trainingsdaten für die Systeme zur Verfügung standen, mussten diese erst erzeugt werden, indem die zu erkennenden Situationen durch Darsteller:innen ›aufgeführt‹ und aufgezeichnet wurden. Während Gatekeeping im ersten Fall heißt, durch automatisierte Überwachung in einer Datenbank hinterlegte Personen zu identifizieren, um gegen sie exekutiv vorgehen zu können, meint Gatekeeping im zweiten Fall, Gefährdungssituationen zu erkennen, um die Sicherheit eines Bereichs wieder herzustellen bzw. aufrechtzuerhalten. Entspricht der erste Fall dem ›klassischen‹ Gatekeeping der Zugangskontrolle, steht im zweiten Fall die Regulierung eines an sich offenen Bereichs im Vordergrund, in den unter bestimmten Bedingungen interveniert wird. Trotz der schlechten Performance der Erkennungssysteme wurde als Testergebnis ihr grundsätzlicher Wert als ›Unterstützungsinstrument‹ für die Polizeiarbeit festgehalten und im Fall der Situations- und Verhaltenserkennung sogar statt eines Ergebnisberichts ein weiteres dreijähriges

einer Straftat hindeuten.« (PolG BW 2017 § 21) Jüngstes Beispiel einer solchen Anpassung ist das HSOG (Hessisches Gesetz über die öffentliche Sicherheit und Ordnung). Auch hier wurde am 12. Dezember 2024 beschlossen, die »Erkennung und Auswertung von Bewegungsmustern, die auf die Begehung einer Straftat hindeuten«, explizit aufzunehmen; dabei wird Bewegungserkennung als erste Stufe eines Einsatzes von Bildanalysesoftware verstanden, auf die die automatisierte Nachverfolgung von Personen und die biometrische Identifizierung folgen können (HSOG § 14 Abs. 8).

9 Ausführlicher zu diesen Tests mit Blick auf Konzeption und Ergebnisse sowie ihre Funktion für das Kontrollregime ›Bahnhof‹ vgl. Schabacher 2021, 2023; Schabacher/Spallinger 2023: bes. 44–46.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY-NC

Testvorhaben angeschlossen. Wie wir an anderer Stelle argumentiert haben (vgl. Schabacher/Spallinger 2023: 48–50), dienen die Tests zwar vordergründig der tatsächlichen Erprobung der Funktionalität der betreffenden Systeme, müssen aber in ihrer Wirkung vielmehr als »Medien der Gewöhnung« (ebd. 50) verstanden werden, die eine Art Einübung der infrastrukturellen Anwesenheit von KI-Technologien betreiben, und zwar umso wirksamer, je länger sie dauern.[10]

Dies trifft auch auf den Mannheimer Modellversuch zu, der zunächst für fünf Jahre (2018–2023) angesetzt war und 2023 noch einmal um weitere drei Jahre (2024–2026) verlängert wurde (vgl. Stadt Mannheim 2018b; IM BW 2023a). Der Test findet als Kooperation der Stadt Mannheim, des Polizeipräsidiums Mannheim und des Fraunhofer Institut für Optronik, Systemtechnik und Bildauswertung (IOSB) statt und konzentriert sich auf die Erkennung unstrukturierter Alltagssituationen (viele Menschen an öffentlichen Plätzen). Dies gestaltet den Erkennungsprozess komplex und rechenintensiv und verursacht aufgrund von wechselnden Lichtverhältnissen, vielfältigen Verdeckungen (bezogen auf die Raumtiefe) sowie schnellen Bewegungen Probleme für die Erkennung. Das Fraunhofer IOSB hatte die Aufgabe, ein eigenes KI-System zur polizeilichen Lageeinschätzung für solche komplexen und ungeordneten Umgebungen zu entwickeln – im Unterschied zum Berliner Fall, wo marktgängige Softwares zum Einsatz kamen.

Aus einer medienkulturwissenschaftlichen Perspektive ist an einem Test solcher Dauer besonders interessant, wie das Problem konzeptualisiert wird, auf das die zu entwickelnde Software reagieren soll. Wie zu zeigen sein wird, spielen für diese Konzeptualisierung verschiedene Aspekte eine Rolle: die rechtlichen Rahmenbedingungen (Datenschutz, Änderung des Polizeigesetzes), die Geschichte des bisherigen Einsatzes von Videoüberwachung (»Mannheimer Weg«), die unterschiedlichen politischen Perspektiven auf Innere Sicherheit bei Befürworter:innen und Kritiker:innen, aber auch die technische Machbarkeit bezogen auf den deutschen Entwicklungsstand der KI-Forschung (etwa die vom IOSB bereits seit 2007 entwickelte Basis-Software NEST[11]), infrastrukturelle Gegebenheiten

10 Wir rekurrieren dabei auf ein Verständnis von Gewöhnung, das sich auf die materielle und umweltliche Einbettung von Gewohnheiten bezieht (vgl. Dewey 2008 [1922]; Bennett et al. 2013), und sehen hierin eine Form der ›indirekten‹ Steuerung und Regulierung von Verhalten (vgl. Halpern et al. 2013; Bröckling 2017; Moser/Vagt 2018).

11 NEST (Network Enabled Surveillance and Tracking) ist ein »Eigenforschungsvorhaben« des Fraunhofer IOSB (2025b). Zunächst ging es um Videomonitoring mit Kartendarstellung (2007–2010); NEST-CrowdControl (2010–2015) entwickelte dann Videoanalyseverfahren (Personenzählung, Personendichtemessung, »Bewegungsflussschätzung von Menschenströmen«), die für das Echtzeit-Monitoring von Menschenmengen bei Großveranstaltungen genutzt werden können (Monari/Fischer 2017: 13). Eine Erkennung spezifischer Bewegungen erlaubt dann (ab 2018) NEST Activity Recognition (vgl. Voth 2019: 7).

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY-NC

(Kompatibilität der Software mit der vorhandenen Kameraausstattung) sowie die Versprechen und Narrative, die mit KI-Systemen einhergehen.

3. Kriminalitätsschwerpunkte – zur Konstruktion von Orten

Als die Stadt Mannheim 2018 den Beschluss fasste, die Videoüberwachung mittels ›intelligenter‹ Systeme auszubauen (geplantes Finanzvolumen von 800.000 Euro), schloss dies an ein vorhandenes Sicherheitskonzept an, den sogenannten »Mannheimer Weg« (2001–2007).[12] Während in der ersten Phase (2018–2023) entweder der Ortsbezug (»Mannheimer Weg 2.0«) oder die eingesetzte Technologie (»Intelligente Videoüberwachung«) betont wurde, rückte die Verlängerung des Projekts unter dem Titel »Intelligenter Videoschutz« signifikant von der panoptischen (und kritisch diskutierten) Perspektive der Überwachung ab und betonte mit der Rede vom ›Schutz‹ eine fürsorgende Haltung des Staates – Gate*keeping* wird als bewahrende Pflege der Ordnung inszeniert, wobei die vorausgehenden machtvollen Sortierungsprozesse auf der Ebene der Mustererkennung unsichtbar bleiben: Das Konzept »Videoschutz« soll die Gewaltkriminalität in der Mannheimer Innenstadt präventiv regulieren. Insofern aber eine dauerhafte Videoüberwachung nur an erwiesenen Kriminalitätsschwerpunkten stattfinden und die automatische Erkennung nur auf solche Verhaltensmuster ausgerichtet sein darf, »die auf die Begehung einer Straftat hindeuten« (PolG BW (2017) § 21; PolG BW (2021) § 44), stellt sich die dringliche Frage, was einen solchen Kriminalitätsschwerpunkt auszeichnet und welche Verhaltensmuster als strafverdächtig gelten.

Ein Kriminalitätsschwerpunkt ist laut Landespolizeigesetz Baden-Württemberg ein Ort, dessen »Kriminalitätsbelastung« deutlich über dem Niveau des übrigen Gemeindegebiets liegt und von dem angenommen werden kann, dass dort auch zukünftig Straftaten stattfinden werden (PolG BW (2021) § 44 Abs. 3) (vgl. Abb. 1).[13] Es geht also um polizeilich definierte und klar abgesteckte Raumausschnitte einer Stadt, die von der Polizei mittels ›Lageerkenntnissen‹, d. h. Einschätzungen örtlicher Revierleiter, und messbarer Kriminalstatistik festgelegt werden. Die kritische Kriminologie sieht in Kriminalitätsschwerpunkten deshalb spezifische Konstruktionen einer präventiven Wende des Policing, die im

12 Hierbei handelt es sich um ein Zusammenspiel aus konventioneller Videoüberwachung, Livebeobachtung im Lagezentrum, polizeilicher Intervention im Verdachtsfall sowie jährlichen Sicherheitsbefragungen der Stadtbevölkerung (vgl. Pietsch/Hauck 2021: 87).

13 Die Kriminalitätsbelastung ergibt sich aus dem Abgleich der Polizeilichen Kriminalstatistik (PKS) mit dem städtischen Lagebild und gibt Delikte der Straßenkriminalität pro Hektar an (vgl. Stadt Mannheim 2017b: 11 f.).

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access -

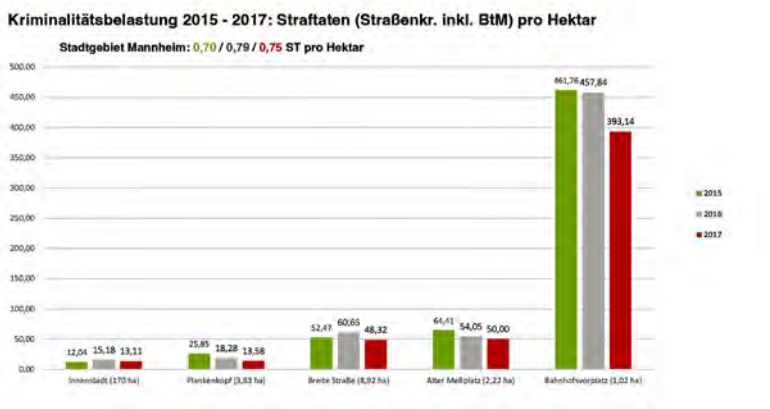

Abb. 1: Kriminalitätsbelastung 2015–2017 in der Mannheimer Innenstadt und an den Kriminalitätsschwerpunkten (Straßen- inkl. Betäubungsmittelkriminalität)

Zusammenspiel von Verordnungen, Medienberichten und Polizeistatistiken geschaffen würden. Es handele sich um »Produkt[e] komplexer Prozesse der Sichtbarmachung, Thematisierung und […] Konstruktion von Bedrohung« (Ullrich/Tullney 2012: 2), die polizeiliche Überwachung legitimieren sollen, und insofern ein machtvolles »Kartografieren des Risikos« (Zurawski 2014) vollziehen. Dabei kommt es zu einer rekursiven Selbstbegründung des Verfahrens: Indem die Tests von Videoüberwachungssystemen an Orten erfolgen müssen, die zuvor als kriminell auffällig ausgewiesen wurden, bestätigt ihre Erkennung krimineller Verhaltensmuster die Argumentation, es handele sich um einen Kriminalitätsschwerpunkt, den es zu überwachen gelte.

Für die Konzeptualisierung des Kriminalitätsproblems, das der Mannheimer Modellversuch beheben soll, spielten zwei Aspekte eine besondere Rolle: erstens die Kriminalitätsrate und zweitens das Sicherheitsgefühl. Bezüglich der Kriminalitätsrate in Mannheim finden sich interessanterweise verschiedene Aussagen: Einerseits soll sie immer schon hoch gewesen sein, was Klaus Pietsch, von 2017 bis 2022 Polizeidirektor des Polizeipräsidium Mannheim und Leiter des Mannheimer Modellversuchs, auf die geografische Lage der Stadt bezieht: »Das ist hier das Dreiländereck, wir haben bestimmte soziale Strukturen. Mannheim ist eine große Einkaufsstadt, das ist ein Drehkreuz, Verkehrsdrehkreuz, ICE-Knotenpunkt. Es ist einfach ein lokaler Brennpunkt, der aufgrund seiner besonderen Struktur kriminalitätsfördernd ist.«[14] Andererseits konstatierte eine Informationsveranstaltung der Stadt Mannheim, die den Modellversuch im Juni 2018 vorstellte,

14 Algorithmenbasierte Kameraüberwachung (D 2022), TC: 00:01:40–00:02:00 (O-Ton Pietsch).

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY-NC

einen »signifikanten Anstieg der Straßenkriminalität«[15] in bestimmten Bereichen der Innenstadt (Stadt Mannheim 2018a: Folie 3). Die Präsentation nennt die als Kriminalitätsschwerpunkte ausgewiesenen Orte (vgl. Abb. 2) Bahnhofsvorplatz, Breite Straße (inkl. Paradeplatz, Marktplatz), Alter Messplatz und Plankenkopf, was mit Statistiken für die Jahre 2015–2017 belegt ist (ebd.: Folie 8). Es steht zu vermuten, dass nicht zuletzt, weil die Zahlen für 2017 leicht rückläufig waren, neben dieser »[o]bjektive[n] Kriminalitätsbelastung« ein weiterer Faktor als Begründung für die Notwendigkeit des Ausbaus automatisierter Überwachung ins Spiel gebracht wurde, nämlich das »subjektive Sicherheitsempfinden« und die Akzeptanz des Überwachungsausbaus in der Bevölkerung (ebd.: Folie 6). Von beiden Aspekten wird behauptet, sie hätten hohe Werte in der Bevölkerung: Die Beeinträchtigung des Sicherheitsgefühls sei »erheblich« und die Akzeptanz der geplanten Maßnahme hoch (ebd.: Folie 7 u. 13).

Um nun diese signifikante Steigerung der »subjektiven Unsicherheit« (ebd.: Folie 11) zu dokumentieren, wird auf sogenannte »Sicherheitsbefragungen« gesetzt. Diese Bürgerbefragungen führt das Institut für Kriminologie der Universität Heidelberg seit 2012 alle vier Jahre durch (2012, 2016, 2020 und 2022/2023). Die Ergebnisse werden veröffentlicht und sind von entsprechenden Gutachten flankiert.[16] Dazu wurden 2016 rund 10.000 Mannheimer Bürger:innen gebeten, hinsichtlich ihres subjektiven Sicherheitsgefühls Auskunft zu geben (ca. 3.300 Personen taten dies dann auch);[17] dabei sollten Aspekte wie die persönliche Risikoeinschätzung, Opfer eines Gewaltdelikts zu werden, Vermeidungsmaßnahmen sowie mögliche Ängste die Messung der sogenannten »Kriminalitätsfurcht« (Hermann 2017: 30, 2021: 26, 2023: 21) ermöglichen. Während die Sicherheitsbefragung von 2012 noch vorwiegend »Störungen der sozialen und normativen Ordnung« als Probleme des Sicherheitsgefühls herausgestellt hatte (Hermann 2012: 5), wurden ab 2016 Aspekte wie Migration und Integration deutlicher einbezogen (vgl. Hermann 2017: 75) und damit auch gesamtgesellschaftliche ›Ängste‹ adressiert, was als zusätzliche Legitimation des geplanten Überwachungsprojekts zu verstehen ist. Außerdem

15 Die Daten der Präsentation basieren auf der Informationsvorlage V450/2017 (vgl. Stadt Mannheim 2017a, 2017b), Lagebilddaten von 2018 sowie der Polizeilichen Kriminalitätsstatistik 2018 (vgl. Polizeipräsidium Mannheim 2019a); zur Berechnung des prozentualen Anstiegs vgl. Polizeipräsidium Mannheim 2019b.

16 Zu den Ergebnissen vgl. die entsprechenden Informationsvorlagen (Stadt Mannheim 2012, 2017c, 2021a, 2023) sowie die Sicherheitsaudits (Hermann 2012, 2017, 2021, 2023).

17 Die Zahl der angefragten Personen wurde dabei kontinuierlich gesteigert: Waren es 2012 noch 6.500 Personen, wurden bei den Sicherheitsbefragungen 2020 bzw. 2023 rund 25.000 Personen angefragt. Gleichwohl erhöhte dies den Grad der Beteiligung nicht (vgl. Hermann 2021: 19 f., 2023: 19). Darüber hinaus handelt es sich um ein stark interpretatives und selektives Verfahren, das potentiell interessierte Personen adressiert und der deutschen Sprache nicht mächtige Personen ausschließt.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY-NC

Abb. 2: Videoüberwachungsbereiche (blau) an den Kriminalitätsschwerpunkten

würden die Sicherheitsbefragungen eine gute Akzeptanz des Vorhabens in der Bevölkerung zeigen;[18] jede:r zweite Bürger:in kenne den Modellversuch (vgl. ebd.: 70). Zwar konstatierte das Sicherheitsaudit, Videoüberwachung führe *nicht* signifikant zur Abnahme der Kriminalitätsbelastung (vgl. ebd.), gleichwohl wurden die Ergebnisse der Sicherheitsbefragung als bestätigendes Argument »für die Implementierung der Videoüberwachung« interpretiert (ebd.: 71).

Öffentlich wurden aber nicht nur die Ergebnisse der Sicherheitsbefragung, sondern auch die Kritik an dem Projekt. Innerhalb der Laufzeit des Modellversuchs wurden wiederholt drei Argumente vorgebracht, die sich gegen die behauptete Verbesserung der subjektiven Sicherheit, der objektiven Sicherheit sowie die potentielle Ausweitung von Überwachung richteten. So betonten die Kritiker:innen erstens, dass Videoüberwachung nicht zu einer Erhöhung des subjektiven Sicherheitsgefühls geführt habe, obwohl sie in konventioneller Form bereits seit vielen Jahren in Mannheim (genauer: am Hauptbahnhof) stattfinde (vgl. Bündnis90/Die Grünen 2020; Stadt Mannheim 2021b). Bekanntlich werde

18 Diese Aussage wird kritisch gesehen, da man nur die allgemeine Zustimmung zu Sicherheitsmaßnahmen erfragt habe; vgl. Interview S. Spallinger mit ehemaligem Bezirksbeiratssprecher Bündnis90/Die Grünen, Neckarstadt Mannheim, 04.10.2021.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY-NC

dies allein durch eine höhere Polizeipräsenz vor Ort oder auch wenig invasive Maßnahmen wie bessere Straßenbeleuchtung gewährleistet (vgl. Grüne Jugend 2019). Zweitens sei auch die objektive Sicherheit durch den Ausbau der Videoüberwachung nicht zu steigern, da die betreffenden Gewaltdelikte an stark frequentierten Plätzen ohnehin schnell auffielen,[19] während die sich stärker heimlich vollziehende Drogen- oder Diebstahlskriminalität durch einen Fokus auf Bewegungsmuster des Fallens, Tretens, Stürzens oder der Gruppenbildung ohnehin nicht zu erkennen sei. Vielmehr sei zu erwarten, dass die »unzähligen Treffen von Familien mit Kindern, die ersten Fahrversuche kleiner radbegeisterter Mannheimer, die ambitionierten Sprünge und Stürze jugendlicher Skater oder Sprints eiliger Studierenden, Arbeitenden und Anwohnern zur Straßenbahn« (OpenPetition 2018) Hinweise auf den Kontrollbildschirmen generieren würden. Wenn dagegen nachts das Sicherheitsgefühl auf solchen Plätzen abnähme, seien auch die Test-Bildschirme nicht besetzt, sodass selbst bei einem algorithmisch korrekt erkannten verdächtigen Verhalten keine Intervention erfolge (vgl. ebd.).[20] Intelligente Videoüberwachung sei also weder ein Mittel der präventiven objektiven Gefahrenabwehr noch eines der Verbesserung des subjektiven Sicherheitsgefühls, sondern allein ein Mittel zur Aufklärung von Straftaten – dies funktioniere aber nur dann effizient, wenn man die Verhaltenserkennung mit biometrischen Erkennungssystemen koppele (vgl. ebd.). Kritisiert wurde der Ausbau der Videoüberwachung also drittens auch, weil er die Infrastrukturen für weitere Überwachungskonstellationen schafft (vgl. Trüper 2017). So warnt ein Mitglied von Digitalcourage e. V. vor der ›beiläufigen‹ Ausweitung solcher Systeme:

> »Es gibt den Begriff des ›Mission Creep‹, der bezeichnet, dass man ein System, eine Überwachungsfunktion mit irgendeinem Zweck, erst mal anfängt einzuführen und dann Stück für Stück sagt: ›Ach, jetzt haben wir ja diese Infrastruktur schon, da könnten wir sie doch auch für das und das verwenden.‹ […] [W]enn so ein System einmal aufgebaut ist und eine softwarebasierte Überwachung stattfindet, dann reicht ein Update, um zu ändern, was das System tut. Das heißt, da wo ich heute sage, ich mache eine Strichpersonenerkennung mit Leuten, die am Boden liegen – was optisch dann einfach Obdachlose sind, die man aus dem öffentlichen Raum vertreibt – kann ich morgen sagen: ›Ach gut, jetzt machen wir doch wieder Gesichtserkennung oder machen irgendeine andere Form der automatisierten Erkennung‹. Das ist dann nur noch ein Software-Update.«[21]

19 Zur sozialen Kontrolle im Sinne von *situational awareness* vgl. Hentschel et al. 2025, zu *lateral surveillance* vgl. Andrejevic 2006: 397.

20 Zu diesem Zeitpunkt waren die Test-Bildschirme Sonntag bis Donnerstag von 11–23 Uhr und Freitag und Samstag von 11–3 Uhr besetzt (vgl. Stadt Mannheim 2017b: 12).

21 Interview S. Spallinger mit Mitarbeitendem von Digitalcourage e. V., 07.12.2023.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY-NC

Zudem bleiben derartige Ausweitungen laut Digitalcourage »sehr intransparent«, da man als gewöhnlicher Mensch nicht sehe, welche Software auf Überwachungskameras laufe; außerdem werde auf Informationsanfragen zeitverzögert und nur selektiv geantwortet, sodass sich die Frage stelle, wie man überhaupt »demokratisch intervenieren« könne, »wenn das einmal so weit gekommen ist.«[22]

Wie sich an diesen Ausführungen zeigen lässt, bestand die erste konzeptuelle Schwierigkeit darin, den Ort zu definieren, an dem der Modellversuch stattfinden sollte, also ›Kriminalitätsschwerpunkte‹ zu konstruieren, da nur hier der Einsatz KI-basierter Videoüberwachung datenschutzrechtlich gestattet ist. Dazu wurden ›objektive‹ Größen wie die Kriminalitätsstatistik herangezogen, vor allem aber ›subjektive‹ Unsicherheitsgefühle in der Bevölkerung, die man mit sogenannten »Sicherheitsbefragungen« erhob und die – wie noch zu zeigen sein wird – im Projektverlauf zunehmend die Rolle einer ›Ergebnisinstanz‹ übernahmen.

4. Human Activity Recognition und deviantes Verhalten

Eine zweite konzeptuelle Schwierigkeit, mit der der Modellversuch umgehen musste, betraf die Frage, was die Erkennungssysteme überhaupt als deviantes Verhalten ansehen sollen. Grundsätzlich ist Human Activity Recognition (HAR) darauf ausgerichtet, festgelegte Bewegungen von Menschen mit Hilfe von Algorithmen zu detektieren, zu klassifizieren und zu erkennen, was die biometrische Identifizierung von Personen einschließen kann. Im deutschen Fall, der insbesondere die Forschungen des Fraunhofer IOSB (2025a) und des Karlsruher Instituts für Technologie (KIT) betrifft (vgl. Golda et al. 2022; Cormier 2021), steht jedoch eine Form der Mustererkennung im Vordergrund, bei der vordefinierte Aktivitäten *ohne* die Identifizierung von Individuen erkannt werden sollen. Dabei wird zwischen »sensor-based HAR« und »vision-based HAR« unterschieden (Gupta et al. 2022: 4760). Der Großteil der Forschung zu *vision-based* HAR konzentriert sich auf Objekte oder Personen, wobei die Trainingsdaten unter Laborbedingungen generiert werden und vergleichsweise homogen sind. Demgegenüber verfolgt das Fraunhofer IOSB einen praxisbezogenen Ansatz, der auf der Basis realweltlicher Aufnahmen von Menschenmengen Bewegungserkennungssysteme für den Sicherheitskontext entwickeln will (vgl. Cormier et al. 2022: 591 f.). Zentral ist dabei, dass die zum Einsatz kommende Verhaltens- und Bewegungsanalyse auf einer ›skelettbasierten‹ Posenschätzung (vgl. ebd.: 591) beruht, die die detektierten Menschen in ›Strichfiguren‹ überführt und so die Anonymitätsbedingungen gewährleisten soll. Dieser Ansatz der Bewegungserkennung basiert auf Tests im Gesundheitswesen zur Detektion stürzender Personen, wird aber auch im

22 Interview S. Spallinger mit Mitarbeitendem von Digitalcourage e. V., 07.12.2023.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY

Bereich des autonomen Fahrens sowie für Sportstätten und im Einzelhandel getestet.[23] Beim Einkaufen im REWE Pick&Go-Testmarkt in Berlin etwa erlaubt die Bewegungserkennung eine Form des Gatekeeping, die ohne Gesichtserkennung funktioniert, gleichwohl aber eng an die betreffenden Personen gekoppelt ist: »Das System ist so gebaut, dass es einzelne Kund:innen voneinander unterscheiden kann und sie während ihres gesamten Einkaufs verfolgt.« (Reuter 2024) Nicht nur erlaubt dies dem Unternehmen die Auswertung weiterer Daten mit Blick auf das Kaufverhalten (Aufenthaltsdauer, Wege, Produkte etc.), sondern eine derartige Bewegungserkennung ist prinzipiell auch zur biometrischen Identifikation einsetzbar, wie die Forschung zu *gait recognition* zeigt (vgl. Teepe et al. 2022).

Für eine Erkennung devianten Verhaltens sind nun konzeptuell verschiedene Aspekte bedeutsam. Wie projektverantwortliche Mitarbeitende des Fraunhofer IOSB beschreiben, geht es um Szenarienspezifizierung, d. h. die Frage, welches Verhalten als Ziel erkannt werden soll, um Datenaufbereitung (Annotation, Posenschätzung durch Abstraktion), um Fragen der Merkmalsextraktion vermittels sogenannter ›Digitalskelette‹, die Herstellung von Trainingsdaten, die Programmierung der Algorithmen, deren Training auf der Basis der skelettierten Bewegungsmuster sowie um Tests zur Überprüfung der technischen Leistungsfähigkeit der Erkennung und deren Interpretation.[24] Hierbei handelt es sich nicht nur um Fragen technischer Funktionalität. Muster devianten Verhaltens sind immer durch kulturell, politisch, sozial und historisch codierte Vorstellungen von Un/Sicherheit und Un/Ordnung informiert. Sie herzustellen, also etwas als deviantes, abweichendes Verhalten softwareseitig festzulegen, verweist deshalb immer gleichzeitig auf Instanzen der Normalisierung und der ›Ordnung‹, in deren Interesse ein solches Gatekeeping stattfindet.

Deviantes Verhalten

Im Sicherheitskontext soll Verhaltenserkennung eine Technisierung des polizeilichen Blicks leisten, wie der Projektleiter vom Führungs- und Lagezentrum des Mannheimer Polizeipräsidiums in einem Interview formuliert:

> »Wenn Sie sich vorstellen, ein Polizeibeamter ist auf einem öffentlichen Platz auf Streife, der lässt seinen Blick schweifen […] und irgendwo bleibt ja dann der Blick

23 So etwa im Gesundheitsbereich beim Prototyp »NurseEye« (vgl. Fraunhofer IOSB 2025c), zur Erkennung der Fahreraktivität im Automobil (vgl. Martin 2023) sowie zur digitalen Badeaufsicht in Schwimmbädern in Wiesbaden und Hamburg (vgl. Klute 2025).

24 Vgl. Interview S. Spallinger mit Projektleiter Gruppe Videobasierte Sicherheits- und Assistenzsysteme, Fraunhofer IOSB, 19.10.2021; Interview S. Spallinger mit projektinternem Informatiker des Fraunhofer IOSB, 09.05.2022.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY-NC

> hängen. Nämlich meistens an den Situationen, wenn er erkennt, hier verhält sich jemand unüblich: Hier ist ein Verhalten, was darauf hindeuten könnte, dass es hier möglicherweise bald zu einer Straftat kommt. Dann guckt er sich das fokussiert an und entscheidet dann, ob er einschreiten muss. Und genau diesen Blick wollen wir mit den Algorithmen herausfiltern, herauskriegen.«[25]

Der polizeiliche Blick bleibt also an solchen Verhaltensweisen hängen, die gegenüber einem als ›normal‹ codierten Verhalten als deviant angesehen werden. Dabei setzt sich dieser Blick nicht nur aus verschiedenen Schritten zusammen – Aufmerksam-Werden (›hängenbleiben‹), Beobachten, Erkennen, Interpretieren, Einschreiten –, er ist auch maßgeblich kulturell und historisch informiert. Denn was Polizist:innen und Ordnungsbeamte ›sehen‹, hängt von ihrer Ausbildung, von ihren Erfahrungen und Skills, aber auch von ihrer jeweiligen Kenntnis des Areals, der dort agierenden Akteur:innen oder von Ereignissen ab, die dort stattgefunden haben. Aus diesem Grund ist die technische ›Übersetzung‹ eines solchen Blicks schwierig bis unmöglich. Zwar unterliegen technische Systeme bestimmten Formen von Fehlern nicht – sie werden etwa im Vergleich zu menschlichen Videobeobachter:innen nicht müde, was häufig im Sinne eines »technological solutionalism« (Morozov 2013) als Begründung für ihre Implementierung angeführt wird (vgl. Pietsch/Hauck 2021: 91; Golda et al. 2022: 1489) –, sie haben dafür aber zahlreiche andere Probleme.

So soll der Algorithmus, wie der Projektleiter ausführt, »Verhaltensweisen erkennen, die auf eine Straftat hindeuten: also unübliche Verhaltensweisen, jetzt wie Schlagen, Treten zum Beispiel oder aggressive Gesten, defensive Gesten.«[26] Doch damit würden Erkennungssysteme auf einem öffentlichen Platz nichts entdecken, was nicht bei entsprechender Polizeipräsenz auch erkannt werden würde (vgl. Pietsch/Hauck 2021: 88).[27] Wie Kritiker:innen argumentieren, liegt also die Schlussfolgerung nahe, dass auch Einsparungsüberlegungen im Hintergrund stehen, wenn man das Überwachen der Technik überlassen könnte und nur die tatsächliche Intervention durch Personen durchführen ließe (vgl. Scheiwe 2023). Insbesondere beim Überblicken schwer einsehbarer Lagen wie Großveranstaltungen oder in belebten Fußgängerzonen sollen KI-Systeme ein schnelleres und gezielteres Agieren gewährleisten (vgl. Golda et al. 2022: 1495; Pietsch/Hauck 2021:

25 Interview S. Spallinger mit Projektleiter »Videoschutz«, Polizeipräsidium Mannheim, 19.06.2024.

26 Interview S. Spallinger mit Projektleiter »Videoschutz«, Polizeipräsidium Mannheim, 19.06.2024. Diese Verhaltensweisen wurden bereits zu Beginn des Projekts festgelegt (vgl. Stadt Mannheim 2017a: 14).

27 Vgl. Interview S. Spallinger mit einem Mitglied des Chaos Computer Club Mannheim, 06.10.2021.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY-NC

91).[28] Damit betrifft Verhaltenserkennung Fragen von Crowd Control bzw. Crowd Management[29] und damit eine Form des Gatekeeping und der Regulierung, die sich nicht auf die Identifizierung von Einzelindividuen oder die Steuerung der Bewegungsflüsse von Menschengruppen richtet, sondern vielmehr auf die Aktivitäten, die einen solchen Flow stören können.

Dabei setzen die betreffenden Erkennungssysteme nicht nur spezifische Vorstellungen von Ordnungswidrigkeiten, kriminellem Agieren und notwendigem Gatekeeping voraus, sondern sie treffen diese Wahl auch aus Gründen technischer Praktikabilität. Dies wird deutlich, wenn man sich dem operativen *Wie* der Erkennung zuwendet. Realweltliche Orte stellen Erkennungssysteme vor etliche Schwierigkeiten, da es sich um »unstrukturierte und unkontrollierbare Alltagssituationen« (Golda et al. 2022: 1490) mit vielen Menschen handelt, also um »uncooperative scenarios« (Cormier et al. 2022: 592), die den Erkennungsprozess aufgrund von Lichtverhältnissen, multiplen Verdeckungen und Hintergründen sowie schnellen Bewegungen komplex und rechenintensiv machen. Gerade für solche realweltlichen Szenarien gab es 2018 noch keine vorgefertigten Lösungen, weshalb die Projektverantwortlichen den »Forschungscharakter« des Modellversuchs unterstrichen.[30] Für den Erkennungsprozess ist wesentlich, dass gemäß einer Figur-Grund-Unterscheidung zunächst die als ›normal‹ verstandenen Bewegungen festgelegt und annotiert werden: Vor dem Hintergrund dieser »Abgrenzungsszenarien« – es brauche ca. 14 bis 15 Arten der Ausführung einer Aktivität (man könne auf sehr verschiedene Weisen stehen, laufen, sitzen, aber eben auch treten, schlagen etc.) – können dann die als deviant und abweichend klassifizierten Aktivitäten »herausstechen«.[31] Mit der Auswahl, Festlegung und Annotierung solcher ›devianten‹ Aktivitäten würden gewissermaßen »Erkennungszeichen« für die Software generiert, bei deren Auftreten eine Geste als ›verdächtig‹ eingestuft werde.[32]

Die Entwicklungsarbeit des Fraunhofer IOSB gilt den verschiedenen Schritten der Verfahrenskette einer solchen Bildauswertungssoftware (vgl. Abb. 3) (vgl. Golda et al. 2022: 1493). Dabei werden in einem ersten Schritt die Bilddaten aus dem Live-Feed einer statischen Überwachungskamera auf erkennbare Perso-

28 Bei Demonstrationen oder Kundgebungen allerdings werden die Kameras aus datenschutzrechtlichen Gründen in eine sogenannte »Demoschaltung« versetzt, d. h. für diesen Zeitraum deaktiviert (Pietsch/Hauck 2021: 90).

29 Vgl. hierzu auch die Homepages von zwei früheren Projekten des Fraunhofer IOSB, »S²UCRE« (2017–2020) und NEST-CrowdControl (2010–2015) (siehe Fraunhofer IOSB 2025d und 2025b).

30 Interview S. Spallinger mit Projektleiter Gruppe Videobasierte Sicherheits- und Assistenzsysteme, Fraunhofer IOSB 19.10.2021.

31 Interview S. Spallinger mit projektinternem Informatiker des Fraunhofer IOSB, 09.05.2022.

32 Interview S. Spallinger mit projektinternem Informatiker des Fraunhofer IOSB, 09.05.2022.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY

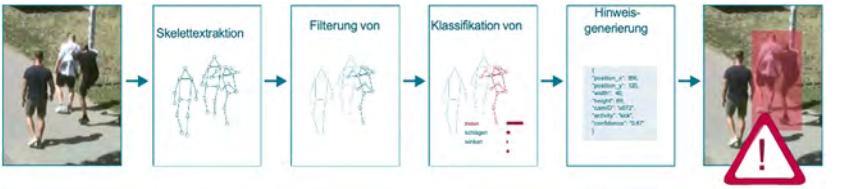

Abb. 3: Verfahrenskette der Verhaltenserkennungssoftware

nen detektiert, die vermittels sogenannter *bounding boxes* markiert werden. Aus datenschutzrechtlichen Gründen werden in einem zweiten Schritt die erkannten Personen in eine nur die Körperstrukturmerkmale zeigende Skelettrepräsentation umgewandelt. Drittens folgt die Filterung der so erzeugten ›Strichfiguren‹ nach Auffälligkeiten (Anomalien), wobei es hier um die Erkennung von Bewegungen geht. Viertens werden die erkannten Auffälligkeiten bezogen auf polizeilich relevante Aktivitäten (Schlagen, Treten) klassifiziert und schließlich wird, fünftens, eine Meldung generiert, wenn es in einem bestimmten Zeitabschnitt zu einer »Akkumulation von ›kritischen‹ Aktivitäten« kommt; in diesem Fall erscheint eine Nachricht auf dem Bildschirm des zuständigen Videosachbearbeiters. Kommt es nicht zu dieser Häufung, werden Daten nach einer definierten Zeit (z. B. einer Minute) gelöscht. Der Videosachbearbeiter selbst sieht stets nur ein Bild mit oder ohne Hinweis, die anderen Schritte erfolgen durch die Software im Hintergrund (vgl. ebd., Hinweis zur Abbildung).

Im Zentrum der Bildauswertungssoftware steht das Verfahren der sogenannten ›Posenschätzung‹ (*human pose estimation*).[33] Die Methode basiert auf der Identifizierung und Klassifizierung von Gelenken des menschlichen Körpers (Ellbogen, Kopf, Rumpf), sogenannten *key points*, von denen angenommen wird, dass ihr Zusammenwirken die betreffende Pose, also die Körperhaltung einer Person beschreibbar macht. Eine normale Überwachungskamera nimmt alle 33 Millisekunden ein neues Bild auf, dessen Verarbeitung je nach Anzahl der zu erkennenden Posen eine entsprechend hohe Rechenzeit erfordert (vgl. Golda et al. 2022: 1491): So verlangt schon das Annotieren einer einzigen Pose in der Regel 40–60 Sekunden (vgl. Cormier et al. 2021: 1649). Insbesondere in unübersichtlichen Settings, etwa auf öffentlichen Plätzen, überlagern sich die *bounding boxes* im Hintergrund. Daher stellt der Live-Betrieb solcher KI-Systeme stets einen Kompromiss zwischen der Genauigkeit der Erkennung (Anzahl der berechneten Gelenke) einerseits und

33 Bei diesem Top-Down-Verfahren werden zunächst Personen in einem Videofeed detektiert, ehe ihre Pose geschätzt wird. Dies hat gegenüber Bottom-Up-Verfahren den Vorteil, keine Probleme bei der Zuordnung von Körperteilen zu Individuen zu verursachen, führe aber zu einer »schnell wachsende[n] Laufzeit in Abhängigkeit zur Größe der Menschenmenge« (Golda et al. 2022: 1495).

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY

der Geschwindigkeit der Erkennung (Rechenzeit) andererseits dar, denn unter Realbedingungen muss der Alarm schnell erfolgen, um Hilfe vor Ort leisten zu können (vgl. Cormier et al. 2022: 591).

Doch nicht nur die Erkennung der jeweiligen Aktivitäten durch die Ermittlung der Körperhaltungen ist für die betreffenden Systeme eine Herausforderung. Hinzu kommt das Fehlen entsprechender Trainingsdaten. Öffentlich steht polizeiliches Videomaterial zu Gewaltdelikten aus datenschutzrechtlichen Gründen nicht zur Verfügung, aus polizeilichen Kontexten selbst stammendes Videomaterial hat häufig einen zu geringen Umfang, um einen validen Trainingsdatensatz zu erstellen.[34] Ausschnitte aus Actionfilmen wiederum, die die betreffenden Bewegungsabläufe enthalten, erwiesen sich aufgrund der hohen Stilisiertheit der Fiktion als ungeeignet: »Das sind typischerweise sehr schön hoch aufgelöste Bilder, die sehr zentriert sind auf das Ziel der Aufmerksamkeit […]. Das entspricht aber nicht wirklich dem, was wir in der Überwachung haben.«[35] Weder Auflösung und Position der Kamera eines Filmsets noch die Frame-Raten, Ausleuchtungssituation oder Hintergründe entsprechen den Bedingungen, unter denen Überwachungskameras ihr Bildmaterial generieren. Deshalb müssen die Trainingsdaten in sogenannten ›Messkampagnen‹ erstellt werden. Dafür ist es (derzeit noch) wichtig, dass das zu Trainingszwecken generierte Videobildmaterial von den Überwachungskameras stammt, auf denen das Erkennungssystem später zum Einsatz kommen soll.[36]

Konstruktion von Daten: Die Messkampagnen

Wie funktioniert eine Messkampagne? In den Natur- und Technikwissenschaften versteht man unter Messkampagnen die umfangreiche, organisatorisch langfristig geplante, zumeist zwischen verschiedenen Institutionen koordinierte, aber zeitlich begrenzte Durchführung von Messreihen zum Zweck der Datengewinnung.[37] In der angewandten Informatik werden Messkampagnen genutzt, um Trainingsdaten unter realweltlichen Bedingungen zu generieren (vgl. Golda et al. 2022: 1498).[38] Damit sind vier Aspekte bedeutsam: der räumliche Bezug (Realworld-Szenario), die zeitliche Begrenzung der Kampagne, die Koordination verschiedener institutioneller Akteur:innen, aber auch der Einfluss infrastruk-

34 Vgl. Interview S. Spallinger mit projektinternem Informatiker des Fraunhofer IOSB, 09.05.2022.

35 Interview S. Spallinger mit projektinternem Informatiker des Fraunhofer IOSB, 09.05.2022.

36 Vgl. Interview S. Spallinger mit projektinternem Informatiker des Fraunhofer IOSB, 09.05.2022.

37 Vgl. etwa Messkampagnen in der Geodäsie (vgl. Marti et al. 1991), der Atmosphärenforschung am KIT (Projekt KITCube) oder in der Metrologie (vgl. MPI für Meteorologie 2021). Zum Konzept der Messreihe vgl. Seiler 1983: 33–42.

38 Vgl. Interview S. Spallinger mit projektinternem Informatiker des Fraunhofer IOSB, 09.05.2022.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY-NC

turell-umweltlicher Größen wie die vorhandene Technikausstattung oder Witterungsverhältnisse.

In Mannheim wurden 2018, 2020 und 2022 an drei öffentlichen Plätzen (u. a. Bahnhofsvorplatz und Alter Messplatz) Messkampagnen durchgeführt.[39] Sie fanden an mehreren Tagen zu unterschiedlichen Zeiten im Jahr statt, wobei die Tageszeiten der Testung wechselten.[40] Auf diese Weise wurden die öffentlichen Plätze in realweltliche »Test beds« (Halpern et al. 2013) verwandelt; sie fungierten als »controlled […] development environment in which to test the operability of new technologies, processes, or theories for large systems« (ebd.: 290).

Aus dem umfangreichen infrastrukturellen Gefüge der Messkampagnen sollen kurz vier Aspekte gesondert betrachtet werden: die Kameras, die menschlichen Beteiligten, das Drehbuch sowie zwei materielle Objekte. Die Videokameras der Marke Sony waren hochauflösend, vernetzt und mit der KI-Software kompatibel, an Masten und Häuserfassaden installiert und filmten aus einer Höhe von fünf bis 25 Meter das Geschehen auf den Plätzen (vgl. Abb. 4). Dabei waren mindestens zwei Kameras gleichzeitig in Betrieb, um Aufnahmen aus verschiedenen Perspektiven zu gewährleisten (vgl. Golda et al. 2022: 1498). Die polizeilichen Akteur:innen stellten sicher, dass keine Unbeteiligten den Aufnahmebereich der Messkampagne betraten, während die Informatiker:innen des Fraunhofer IOSB kontrollierten, *was* im Bildausschnitt zu sehen sein sollte (vgl. ebd.). Dazu wiesen sie Einsatztrainer:innen der Polizei an, welche Bewegungen sie in welcher Weise (Position, Ablauf) und in wie vielen Wiederholungen ausführen sollten. Dies waren etwa »Faustschläge, Fußtritte mit verschiedenen Winkeln an verschiedene Körperteile, aber auch Messerangriffe«[41]; zu Beginn der Softwareentwicklung hatte man auch die Bewegungsabläufe »Hinfallen/Liegen« in Messkampagnen nachgestellt, was aber aufgrund der fehlenden Rechtsgrundlage nicht automatisiert detektiert werden durfte, auch wenn es technisch möglich gewesen wäre.[42] Die polizeilichen Einsatztrainer:innen fungierten hier also als Darsteller:innen, was sich durchaus zu Teilen mit ihren Aufgaben im Bereich des Einsatztrainings deckt, das im Rahmen der Polizei-Ausbildung auf den Einsatz vorbereiten soll (vgl. Staller/Koerner 2021), also ebenfalls in einem Modus des ›als ob‹ stattfindet. Die Rede von Szenarien, Drehbüchern und Darsteller:innen verweist nicht zufällig

39 Auf der Basis von Informationen, die vom Polizeipräsidium Mannheim im Juni 2024 zur Verfügung gestellt wurden, war eine Rekonstruktion der Orte und Zeiten der Messkampagnen möglich; vgl. auch Golda et al. 2022: 1498.

40 Vgl. Interview S. Spallinger mit Projektleiter Gruppe Videobasierte Sicherheits- und Assistenzsysteme, Fraunhofer IOSB, 19.10.2021.

41 Interview S. Spallinger mit Projektleiter »Videoschutz«, Polizeipräsidium Mannheim, 19.06. 2024.

42 Interview S. Spallinger mit Projektleiter »Videoschutz«, Polizeipräsidium Mannheim, 19.06. 2024.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY

Abb. 4: Videoüberwachung in der Mannheimer Fußgängerzone

auf Formen der Aufführungspraxis. So nennt auch der Projektleiter selbst die Messkampagne ein »Nachspielen«.[43]

Die nachzustellenden Aktivitäten und Abläufe waren dabei als ›Szenarien‹ in einem »Drehbuch« dokumentiert (Golda et al. 2022: 1498), das auch die Abgrenzungsszenarien umfasste. Dieses Drehbuch war in einem vorangegangenen, gemeinsamen Workshop der Polizei und des Fraunhofer IOSB erstellt worden, wobei sich die Auswahl der Szenarien an den Gewaltdelikten der Kriminalitätsstatistik sowie am Erfahrungswissen der Polizei orientierte (vgl. ebd.).[44] Damit legte das Drehbuch fest, was als verdächtiges Verhalten verstanden werden sollte und rekurrierte dazu auf das Wissen von bereits erfolgten Straftaten und Statistiken,

43 Interview S. Spallinger mit Projektleiter Gruppe Videobasierte Sicherheits- und Assistenzsysteme, Fraunhofer IOSB, 19.10.2021.

44 Vgl. Interview S. Spallinger mit projektinternem Informatiker des Fraunhofer IOSB, 09.05.2022. In den Messkampagnen 2020 wurden etwa 136 Videosequenzen mit polizeilich relevanten Situationen (u. a. 120 Kampfszenen) für den Trainingsdatensatz erstellt (vgl. IM BW 2023b: 5).

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access -

Abb. 5: Messkampagne in Mannheim, Alter Messplatz

um mittels dieser »Schablone« (Schabacher 2023: 134) das Verhaltenserkennungssystem anzuleiten.

Bei der zeitlich-räumlichen Konturierung der Szenen im Realraum und im Videobild kamen auch bestimmte materielle Objekte zum Einsatz. Absperrbänder und Polizeifahrzeuge dienten der räumlichen Begrenzung des realweltlichen Testsettings, eine rote DIN A4-Pappe sowie eine Bodenmatte fungierten als Markierungen für das Videobild (vgl. Abb. 5). Die rote Pappe verwies auf Beginn und Ende einer Aufnahmesequenz, zeigte also die Szenarien inklusive Wiederholungen an und verdeutlichte damit die zeitliche Struktur der Messkampagnen, deren Exaktheit die nachträgliche Sequenzierung des Videofeeds im Kontrollraum garantierte. Zudem fungierten Pappe und Bodenmatte als Indikatoren dafür, dass es sich um eine gestellte Situation und kein realweltliches Gewaltdelikt handelte.

Als infrastrukturelles Gefüge relationiert die Messkampagne also sehr heterogene Komponenten, um Bewegungsszenarien herzustellen: Aufzeichnungs-, Speicher- und Kommunikationsmedien (Kamera, Drehbuch, Festplatte, Funksprechgerät), materielle Objekte (Pappe, Absperrband), aber auch verschiedene

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY-SA

menschliche Akteur:innen (Polizeibeamte, Informatiker:innen, Operator:innen im Kontrollraum), rechtliche Rahmenbedingungen sowie architektonische und räumliche Gegebenheiten des lokalen Settings. Damit zeigt sich nicht nur die Datendetektion durch Posenschätzung, sondern auch die Datengewinnung durch Messkampagnen als höchst voraussetzungsreiches Unterfangen. Der Mannheimer Modellversuch hat also das Sicherheitsproblem, zu dessen Behebung er antritt, sowohl auf der Ebene des Ortes (›Kriminalitätsschwerpunkte‹) wie auch auf der Ebene des zu erkennenden Verhaltens (›polizeilich relevant‹) aufwendig herzustellen. Verhaltensbezogene Bewegungserkennung im öffentlichen Raum erweist sich so bereits vor jeder konkreten Anwendung als vielfältig distribuierte Form des Gatekeeping.

5. In Situ: Implementierung, Einsatz, Ergebnisse

Doch wie hat sich der konkrete Einsatz der Überwachungstechnologien gestaltet? Wie ist die Bevölkerung mit dem Test umgegangen? Welche Ergebnisse sind erzielt worden?

Für die Bevölkerung war und ist wenig vom Testgeschehen zu ›sehen‹. Denn die Erkennungssoftware lief auf bereits vor Ort vorhandenen Überwachungskameras, so dass sich für die Bürger:innen das jeweilige Setting vor Ort kaum änderte. Doch auch für die involvierten kommunalen Stellen war häufig nicht klar, wann und ob die Kameras anderes taten als konventionell zu überwachen; wiederholte Informationsanfragen zum Versuch wurden nur verzögert beantwortet.[45] Wahrzunehmen war das Geschehen eigentlich nur, wenn tatsächlich Messkampagnen vor Ort[46] durchgeführt wurden oder im Rahmen von Protestkonstellationen. So rief die Aktion »Der stille Tanz«[47] (vgl. Abb. 6) im Mai 2019 dazu auf, die »intelligente Videoüberwachung herauszufordern« (Rauert 2019;

45 Im Februar 2020, also ein Jahr nach Testbeginn, stellte die Fraktion der Grünen eine Anfrage an die Stadtverwaltung Mannheim und die Projektverantwortlichen mit der Bitte um Auskunft zum Testgeschehen (vgl. Bündnis90/Die Grünen 2020). Diese wurde nach mehrmaligen Nachfragen erst im Oktober 2021 beantwortet (vgl. Stadt Mannheim 2021b). Die fehlende Transparenz ist auch Thema im Interview von S. Spallinger mit Stadträtin Bündnis90/Die Grünen Mannheim, 01.10.2021.

46 So berichtet ein Einzelhändler auf Algorithm Watch von einer Messkampagne am Alten Messplatz: »[P]olice vans drive up to the square […] Officers wearing regular clothes got out and started staging fights in front of the new cameras. I thought they were testing the camera angle.« (Lulamae 2023)

47 Die Aktion wurde durchgeführt von einem politischen Aktionsbündnis, zu dem u. a. die Interventionistische Linke Rhein-Neckar, die Grüne Jugend Mannheim, der SDS.Die Linke-Uni Mannheim, die George Orwell Ultras und die Community »Akut+C« gehörten.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access -

Abb. 6: Protestaktion »Der stille Tanz« am 4. Mai 2019, Mannheim (Alter Messplatz)

vgl. Kommunalinfo Mannheim 2019). Auch wenn die Bewegungserkennung zu diesem Zeitpunkt noch nicht auf den Kameras lief, wollte man auf eine Strategie zur Irritation solcher Software hinweisen: Das Tanzen nutzte die Ambiguität von Bewegungen mit Blick auf Tempowechsel, fließende Übergänge sowie Gruppierungen von Personen.[48] Auch bei der späteren Verlängerung des Tests in Hamburg wurde dieses Widerstandsprinzip empfohlen: »Wenn man ein System nicht verhindern kann, muss man es überlasten.;-)«, betonte ein Kommentar auf netzpolitik.org (Rau 2023). Theoretisch brauche man nur so viele Leute, »dass sich alle 15 Minuten jemand auf dem Platz hinsetzt, hinlegt oder umarmt und damit ständig und überwiegend Fehlalarme erzeugt« (ebd.).

Konkret sind beim Mannheimer Modellversuch von den insgesamt 68 Videokameras in der Innenstadt nur wenige tatsächlich mit der Erkennungssoftware des Fraunhofer IOSB ausgestattet – 2022 waren es drei Kameras, 2023 zehn und 2024 dann 16 Kameras.[49] Dabei lief auf diesen Kameras in einer ersten Phase zunächst ›nur‹ Software zur Personen- und Objektdetektion – das System sollte also unterscheiden lernen, ob es sich um einen Menschen oder einen Gegenstand handelt (um dann später nur jene Bewegungen zu ›skelettieren‹, die sich auf Menschen beziehen). Erst in einem zweiten Schritt wurden die Kameras mit Systemen

48 Dies bestätigt auch der Dokumentarfilm All Eyes on You (D 2021) von Michaela Kobsa-Mark. Die Anfangsszene des Films imitiert die Aufnahme einer Überwachungskamera am Marktplatz, die aus erhöhter Position langsam auf eine tanzende Person auf dem Platz zoomt.

49 Zur Anzahl der Kameras im Jahr 2021 vgl. Stadt Mannheim 2021b: 1313, im Jahr 2023 vgl. IM BW 2023a und im Jahr 2024 vgl. Interview S. Spallinger mit Projektleiter »Videoschutz«, Polizeipräsidium Mannheim, 19.06.2024.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY-NC

zur Verhaltenserkennung ausgestattet (Treten, Schlagen).[50] Damit kommt de facto auf 16 von 68 Kameras die Erkennung von polizeilich relevanten Aktivitätsmustern zum Einsatz. Ein ›Echtbetrieb‹ findet also noch an keiner Stelle statt (vgl. Stadt Mannheim 2024: 5).

Die Kameras, auf denen die Systeme getestet werden, sind per Glasfaserverbindung mit dem Führungs- und Lagezentrum des Polizeipräsidiums Mannheim verbunden; eine Internetverbindung ist datenschutzrechtlich nicht möglich. Die Kamerabilder laufen in einem separaten Raum neben dem eigentlichen Kontrollraum zusammen, dem »Videoschutz«-Raum (vgl. Abb. 7). Hier befinden sich zwei Arbeitsplätze mit jeweils sechs Monitoren, auf denen die Überwachungsbilder der 68 Mannheimer Kameras auflaufen (einschließlich der 16 Kameras, die mit Bewegungserkennung ausgestattet sind).[51] Findet in den überwachten Arealen eine Erkennung statt, wird ein Hinweis generiert, der vom Videobeobachter entweder verworfen oder an die Einsatzzentrale weitergegeben wird. Die in dieser Weise verarbeiteten Hinweise werden protokolliert und zusammen mit dem entsprechenden Datenmaterial gespeichert, um für das weitere Training der Systeme genutzt werden zu können. Auch Videomaterial, aus dem sich tatsächlich eine polizeiliche Strafverfolgung ergibt, wird nach strikter datenschutzrechtlicher Überprüfung aufgrund der sensiblen Datenlage von der Einsatzzentrale (auf externen Festplatten) an das Fraunhofer IOSB weitergegeben (vgl. Stadt Mannheim 2017a: 13).[52]

Obwohl das Mannheimer Projekt fünf Jahre lief (2018–2023) und Ende 2023 noch einmal für drei Jahre verlängert wurde (bis Ende 2026), steht eine Evaluation bislang aus – sie wurde für 2027 angekündigt. Zwar soll es einen »Zwischenbericht« geben, aber de facto gilt, wie ein Sprecher vom Chaos Computer Club formuliert: »Weil es nicht funktioniert, wird es verlängert.«[53] Begründet wird das

50 Dieses zweistufige Verfahren war 2019 (Stufe 1) und 2020 (Stufe 2) in kürzeren Testläufen erprobt worden. Dabei kamen 40 Kameras zur Objekt- und Personendetektion (2019) und 20 Kameras zur Testung von Bewegungserkennung auf der Breiten Straße und dem Bahnhofsvorplatz (2020) zum Einsatz (vgl. Landtag von Baden-Württemberg 2020).

51 Hinzu kommen noch 21 Kameras aus Heidelberg, da im Rahmen der Polizeireform 2014 das frühere Mannheimer Polizeipräsidium und die Polizeidirektion Heidelberg zusammengelegt wurden (vgl. Interview S. Spallinger mit Projektleiter »Videoschutz«, Polizeipräsidium Mannheim, 19.06.2024).

52 Vgl. Interview S. Spallinger mit Projektleiter Gruppe Videobasierte Sicherheits- und Assistenzsysteme, Fraunhofer IOSB 19.10.2021 sowie mit Projektleiter »Videoschutz«, Polizeipräsidium Mannheim, 19.06.2024. Vgl. auch das Datenschutzkonzept des Mannheimer Modellversuchs (vgl. Polizeipräsidium Mannheim 2018: 9, 15 und Anlage 2: 9).

53 Interview S. Spallinger mit Sprecher des Chaos Computer Club, 13.12.2023. Ganz ähnlich äußerte sich auch ein Mitglied von Digitalcourage e. V., vgl. Interview S. Spallinger mit Mitarbeitendem von Digitalcourage e. V., 07.12.2023.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY-NC

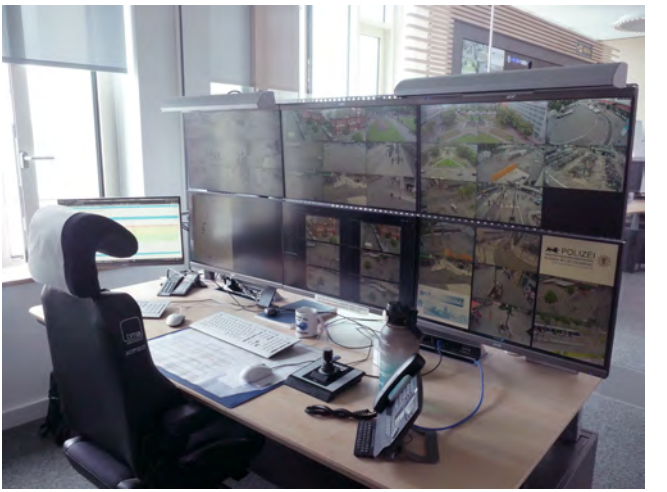

Abb. 7: Arbeitsplatz im »Videoschutz«-Raum des Mannheimer Polizeipräsidiums

Fehlen einer Evaluierung vorrangig damit, dass es sich um ein »Experimentalsystem« (Stadt Mannheim 2017a: 4 u. 15) bzw. ein »lernendes System« (IM BW 2024: 11) handele, das sich ständig in der Entwicklung befinde; aber auch die Covid-Pandemie wird angeführt: Der Verkehr auf den Plätzen sei so massiv eingeschränkt gewesen, dass sich keine Daten hätten generieren lassen (vgl. ebd.: 12).[54] Auch in anderen realweltlichen Testkonstellationen werden Projekte, die zu keinen oder nur sehr mäßigen Ergebnisse führen, als ›erfolgversprechend‹ verlängert; die Fortsetzung der Testungen am Bahnhof Südkreuz etwa folgt diesem Schema (vgl. Schabacher/Spallinger 2023: 46). In Aussicht steht dabei allerdings weniger die Verbesserung der konkreten Ergebnislage. Vielmehr verfolgen derartige Verlängerungen eine umweltliche Temporalisierung des Testgeschehens: Indem eigentlich unausgesetzt ein Test stattfindet, wird er für die öffentliche Wahrnehmung zunehmend ›unsichtbarer‹ und insofern auch unbedenklicher. So findet eine Gewöhnung an das Testgeschehen statt, die es zu einem Teil der städtischen Alltagsinfrastruktur werden lässt, der nicht mehr auffällt.

Auch für den Mannheimer Versuch wird erklärt, die Ergebnisse des Gesamtsystems seien als »sehr zuverlässig und robust« (IM BW 2023b: 2) einzustufen, obwohl – wie gesagt – bislang keine Evaluation stattgefunden hat. Weder gab es die angekündigte soziologische Begleitforschung (vgl. Stadt Mannheim 2017a: 16; Stadt Mannheim 2024: 11 f.) noch sind die skizzierten »Sicherheitsbefragungen« hinsichtlich einer möglichen Reduktion der Kriminalitätsrate durch intelligente

54 Vgl. auch Interview S. Spallinger mit Projektleiter »Videoschutz«, Polizeipräsidium Mannheim, 19.06.2024.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access -

Videoüberwachung aussagefähig. Die Evaluation, so hat es den Anschein, wurde vielmehr in einen weiteren Test ausgelagert, bei dem die Software des Fraunhofer IOSB in Hamburg zum Einsatz kam. Auch dieser deutlich kürzere Test fand an einem sogenannten Kriminalitätsschwerpunkt statt. Von Juli bis September 2023 wurde der Hamburger Hansaplatz, ein Ort, an dem sich viele Obdachlose aufhalten, mit Bewegungserkennung überwacht; dabei kamen vier der insgesamt 22 Kameras des Hansaplatzes zum Einsatz (vgl. Bürgerschaft der Freien und Hansestadt Hamburg 2023: 1 f.). Die Probleme, die sich bei der Detektion ergaben, sind in diesem begrenzteren Test deutlicher als im Mannheimer Fall. So sollten auch hier polizeilich relevante Aktivitäten erkannt werden. Von den rund 1.140 Meldungen, die das System generierte, bezogen sich elf auf polizeilich relevantes Verhalten, wobei davon nur eine tatsächlich kriminalitätsrelevant war (vgl. Abb. 8). Eine weitere, zwölfte Gefahrensituation wurde trotz gegebener polizeilicher Relevanz vom System nicht erkannt. Weil man sich in der Bewertung des Systems allein auf die zwölf polizeilich relevanten Gefahrensituationen bezog, wurde die Trefferrate mit 92 Prozent angegeben. Nicht einbezogen wurden also die 1.128 Meldungen, die das System insgesamt ausgegeben hatte.[55]

Die Verhaltenserkennungssoftware des Fraunhofer IOSB, die polizeilich verdächtige Bewegungen erkennen soll, kennt drei mögliche Formen der Detektion, wie Videobeobachter:innen der Polizei Mannheim erläutern:[56] Es gebe erstens die »Falsch-Detektion«. Hier schätze das System eine Bewegung falsch ein, die Schätzung stimme nicht mit der tatsächlichen Bewegung oder Situation überein. Das habe auch mit der Schwierigkeit zu tun, die Raumtiefe angemessen zu erkennen. Zweitens gebe es »technisch relevante Detektionen«. Hier würden Tret- oder Kick-Bewegungen zwar richtig erkannt, aber falsch klassifiziert. Das liege unter anderem daran, dass der Algorithmus den Zusammenhang von Menschen und Dingen nicht richtig beurteile, also ein Skateboard nicht der betreffenden Person zuordne. Trotz der Tatsache aber, dass das System den Kontext fehlinterpretiert, werden diese Erkennungen gleichwohl *nicht* als Falschmeldungen betrachtet, da die technische Detektion der Bewegung erfolgreich durchgeführt wird. Drittens schließlich gebe es die Detektionen, bei denen die polizeiliche Relevanz von Bewegungen richtig klassifiziert werde (im obigen Beispiel also die elf ›korrekt‹ detektierten Fälle).

55 Zur Rekonstruktionsarbeit vgl. den entsprechenden Artikel auf der Homepage marx.wtf des Sprechers des Chaos Computer Club Hamburg, die Homepage des BündnisHansaplatz sowie Bürgerschaft der Freien und Hansestadt Hamburg 2024.

56 Interview S. Spallinger mit Projektleiter »Videoschutz«, Polizeipräsidium Mannheim, sowie weitere Feldgespräche mit Videobeobachter:innen im Führungs- und Lagezentrums des Polizeipräsidiums Mannheim, 19.06.2024.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access -

1.	Am Boden liegende Person	Person setzte kurz darauf ihren Weg fort
2.	Streitigkeiten in einer Personengruppe	Keine strafprozessualen Maßnahmen vor Ort
3.	Am Boden liegende Person	Keine strafprozessualen Maßnahmen vor Ort
4.	Streitigkeiten zwischen Personengruppe; Trennung durch Passanten	Keine strafprozessualen Maßnahmen vor Ort
5.	Am Boden liegende Person, erheblich gestikulierend	Person nicht mehr angetroffen
6.	Schlägerei zwischen mehreren Personen	Einleitung Strafverfahren wegen gefährlicher Körperverletzung
7.	Tritte zwischen zwei Personen, augenscheinlich „aus Spaß“	Keine strafprozessualen Maßnahmen vor Ort
8.	Am Boden liegende Person	Keine strafprozessualen Maßnahmen vor Ort
9.	Am Boden liegende Person	Gefahrenabwehrende Hilfeleistung
10.	Am Boden liegende Person	Gefahrenabwehrende Hilfeleistung
11.	Am Boden liegende Person	Person setzte kurz darauf Weg fort

Abb. 8: Systemgenerierte Hinweise auf polizeilich relevante Bewegungen, Hansaplatz Hamburg, 21.07–17.09.2023

Die vielen Hinweise, die die Systeme generieren, kommen vermehrt dadurch zustande, dass Menschen nicht in Verbindung mit ›ihren‹ Objekten erkannt werden. Das System ›versteht‹ also bei einem Skateboard oder Fahrrad nicht, dass die Tretrespektive Kickbewegung sich aus der Bedienung des Geräts ergibt. Auch Kinder stellen ein Problem dar: Sie tollen, balgen, raufen sich, fallen um, gestikulieren wild und schreien. Die Erkennungsprobleme bei der Raumtiefe führen dann etwa dazu, dass die Hinweis-Bewegung einer Erzieherin als ein Dem-Kind-auf-den-Kopf-Schlagen gedeutet wird, was einen Alarm auslöst:

> »Der Algorithmus hat hier den Hinweis ›Punch‹ geschaltet […]. Der Arm der Frau ist auf derselben Höhe wie der Kopf des Kindes, sie überlappen sich auf der zweidimensionalen Bildoberfläche, weil sie hintereinanderstehen. […] Es ist aber eindeutig eine Fehlermeldung. Mit bloßem Auge erkennt man, dass die Frau irgendwo hindeutet und das Kind auch räumlich weiter weg steht.«[57]

Jeder Mensch kann also sofort sehen, dass die Erzieherin nur auf etwas zeigt, aber das System betreibt keine Gestaltwahrnehmung, sondern berechnet *key points* sowie Vektor- und Skalarfelder (Golda et al. 2022: 1498). Entsprechend ist am Bahnhofsvorplatz die Differenz von Würgen und Umarmen für die Verhaltenserkennungssoftware nur schwer auszumachen. Deshalb wird auf Algorithm Watch bezweifelt, dass die Systeme tatsächlich so erfolgreich sind, wie offiziell behauptet

57 Feldgespräche S. Spallinger mit Videobeobachter:innen im Führungs- und Lagezentrums des Polizeipräsidiums Mannheim, 19.06.2024.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access -

wird – die Polizeibeamten hätten die Software teilweise nicht genutzt, da sie einfach zu viele Hinweise generiert hätte: »Initially […] officers would switch the ›AI surveillance‹ feature off, because so many movements were flagged.« (Lulamae 2023) Die Detektionsbeispiele verraten, welche Schwierigkeiten die Ambiguität von Bewegungen den Maschinen respektive der Software bereitet. Sie ist dafür verantwortlich, dass Devianz ›erkannt‹ wird, wo keine ist.

Vor diesem Hintergrund mutet die Vision vom »schwarzen Überwachungsmonitor« (IM BW 2023a),[58] die Projektleitende als Ziel des Projekts formulieren, eher verstörend an. Gedacht ist an eine Konstellation, in der Erkennungssysteme so perfekt funktionieren, dass sie im Hintergrund arbeiten, ohne dass sie noch jemand beaufsichtigen müsste.[59] Nur wenn sie tatsächlich etwas Verdächtiges erkennen, generieren sie einen Hinweis, und der Monitor schaltet sich an. Unabhängig davon, dass dies auf längere Sicht auch Personal einsparen soll, entspringt die Annahme, dass eine solche Konstellation einen besseren Datenschutz verspreche (weil nicht ständig alle beobachtet würden), einem Technikverständnis, das im Einsatz komplexer Systeme eine Vereinfachung der Gesamtkonstellation vermutet. Damit ist hier nicht nur erneut *technological solutionism* am Werk, der Technikinnovationen per se als Verbesserung und Fortschritt versteht, sondern die Vision vom ›Schwarzen Monitor‹ kann als eine Form von »sociotechnical imaginaries« (Jasanoff/Kim 2015: 4) verstanden werden, d. h. als ein Zukunftsbild, in dem sich Erwartungen an Technologie kondensieren. Dass der Monitor ausgerechnet schwarz ist, lässt sich dabei nicht allein auf die negativen Kehrseiten einer solchen Entwicklung beziehen. Vielmehr versinnbildlicht das Schwarze des Monitors auch ein Abgeben der Verantwortung für Gatekeeping-Prozesse an Instanzen, deren Entscheidungsprozesse grundlegend opak und undurchdringlich sind.

Die jüngsten Anschläge in Mannheim, die im Mai 2024 und im März 2025 stattfanden, haben die öffentliche Aufmerksamkeit erneut auf das Projekt gelenkt; nicht zuletzt, da der erste Anschlag im Mai 2024 am Marktplatz geschah und damit an einem der ausgewiesenen innerstädtischen Kriminalitätsschwerpunkte des Mannheimer Modellversuchs. Es konnte allerdings kein Videomaterial zum Tathergang zur Verfügung gestellt werden, da die Kameras deaktiviert waren (Demoschaltung), da an diesem Tag auf dem Marktplatz eine Kundgebung stattfand. Gleichwohl ließ allein die Dauer des Modellversuchs die Bevölkerung automatisch annehmen, die intelligente Überwachung sei eigentlich immer in Betrieb. Dies deutet umgekehrt darauf hin, dass – will man eine Gewöhnung an Überwachungskonstellationen erreichen – ein langjähriger Testeinsatz die rich-

58 Zum Teil ist auch vom »schwarzen Bildschirm« die Rede (Interview S. Spallinger mit Projektleiter »Videoschutz«, Polizeipräsidium Mannheim, 19.06.2024).

59 Vgl. Interview S. Spallinger mit Projektleiter »Videoschutz«, Polizeipräsidium Mannheim, 19.06.2024.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access -

tige Maßnahme ist, um eine Habitualisierung der Situation des Überwacht-Werdens herbeizuführen. Damit handelt es sich um eine Strategie, die auch sonst bei der Erprobung von KI-Systemen (etwa im Bereich des autonomen Fahrens, bei Bezahlvorgängen etc.) zum Einsatz kommt und die den öffentlichen Raum zunehmend in ein auf Dauer gestelltes Test-Szenario und unsere Kultur in eine »Testgesellschaft« (Marres/Stark 2020: 425; Gießmann/Gerlitz 2023: 10) transformiert.

6. Fazit

Selbst wenn man unberücksichtigt lässt, dass die im Modellversuch Mannheim detektierten Bewegungen so offensichtlich sind, dass dafür keine Erkennungssysteme nötig wären, während die vielen ›kleineren‹ Bewegungen (etwa der Drogenkriminalität) außen vor bleiben (u. a. weil sie die Falscherkennungsrate drastisch steigen ließen), bleiben weitere Probleme: Denn infrage steht, was ein Erkennungssystem als ›deviant‹ lernt, was also die Muster und Stereotypen dessen sind, was wir als irreguläres Verhalten aus unserer Öffentlichkeit ausschließen wollen. Unter Verweis auf Sicherheitsversprechen bleiben diese grundsätzlichen Fragen der Mustererkennung zumeist unberücksichtigt, auch wenn die gesellschaftlich-kulturelle Konstruktion im Fall von Bewegungsmustern wesentlich deutlicher zutage tritt als bei biometrischen Mustern wie Gesicht oder Fingerkuppen. Dies zeigt der Mannheimer Modellversuch in der Aushandlung der Bedingungen, unter denen er stattfindet (›Kriminalitätsschwerpunkte‹, ›deviantes Verhalten‹), mit Blick auf die Perspektiven, welche Probleme er zu beheben trachtet (›Unsicherheit‹), aber auch bezogen auf die buchstäblich undurchsichtige Ergebnislage.

Gatekeeping im Sicherheitsbereich geht stets mit Prozeduren der Überwachung einher. War dies bereits für klassische Torwächter der Fall, so gehen elektronische und neuerdings KI-basierte Systeme einen Schritt weiter. Denn die Zugangsregulierung z. B. auf Basis biometrischer Erkennungssysteme hat grundlegende Effekte auf Grenzregime, die vielfach herausgearbeitet worden sind: Solche Systeme wirken deterritorialisierend, insofern sie die Grenze mobilisieren und gewissermaßen in das Individuum (bzw. sein *data double*) verlegen, das die Grenzen passieren will (vgl. Amoore 2024, 2006; Andrejevic/Volčič 2021). Mit Blick auf die Frage des Gatekeeping ließe sich hier davon sprechen, dass die ›Gates‹ mobilisiert und dezentralisiert werden, indem Datenabgleich prinzipiell überall und nicht nur an den eigentlichen Türen und Toren stattfinden kann. Verhaltenserkennungssysteme gehen insofern darüber hinaus, als sie sich nicht mehr auf Prozesse der Identifizierung von Individuen richten, sondern der Regulierung von Räumen dienen. Das ›Gate‹ wird hier also nicht nur mobilisiert, sondern flexibel, insofern es gewissermaßen umweltlich diffundiert. Nicht mehr einzelnen

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY-NC

Subjekten wird der Zugang zu einem Raum gestattet oder verwehrt, sondern in Bezug auf einen gegebenen Raum erfolgt ein Monitoring von Gruppen und Crowds, bei denen nicht-konformes Verhalten aussortiert wird. Zwar kann man auch für diesen Prozess von einem Filter (vgl. Apprich 2024) sprechen, aber dieser Filter funktioniert invers. Vor dem Eingang befindet sich keine Traube mehr, von der Einzelne bzw. Einige eingelassen werden, sondern vielmehr sind alle schon da und Einzelne werden herausgenommen. Selbstverständlich kann dies in einem zweiten Schritt auch die Identifikation von einzelnen Subjekten bedeuten, wie die Rede von »granular biopower« (Andrejevic 2022) bereits andeutet. Die Wirksamkeit der Human Activity Recognition liegt jedoch auf einer anderen Ebene: Überwacht werden große Räume und Versammlungen mit vielen Menschen, für die es zunächst gar keine Rolle spielt, um wen es sich konkret handelt. Vielmehr ist das Ziel, bestimmte als deviant definierte Verhaltensweisen zu markieren, um eine gegebene öffentliche Ordnung zu stabilisieren und die Medien eines umweltlichen Gatekeeping, die ihrer Aufrechterhaltung dienen, zu normalisieren.

Literatur

Amoore, Louise (2006): »Biometric Borders: Governing Mobilities in the War on Terror «, Political Geography 25 (3), S. 336–351.

Amoore, Louise (2024): »The Deep Border «, in: Political Geography 109, S. 1–9.

Andrejevic, Mark (2006): »The Discipline of Watching. Detection, Risk, and Lateral Surveillance«, in: Critical Studies in Media Communication 23 (5), S. 391–407.

Andrejevic, Mark (2020): Automated Media, New York/London: Routledge.

Andrejevic, Mark (2021): »Granular Biopower: Touchlessness, Mass-Recognition and Milieu Modulation in Pandemic Times«, in: Gay Hawkins/Ned Rossiter (Hg.), Contagion Design: Labour, Economy, Habit, Data, London: Open University Press, S. 148–160.

Andrejevic, Mark/Volčič, Zala (2021): »Seeing Like a Border: Biometrics and the Operational Image«, in: Digital Culture & Society 7 (2), S. 139–158.

Apprich, Clemens (2024): »Always Be Filtering«, in: Ralf Adelmann/Tobias Matzner (Hg.), Filter. Medienwissenschaftliches Symposium der DFG 4, Paderborn: Universität Paderborn, S. 1–10.

Avis, Maya/Marciniak, Daniel/Sapignoli, Maria (Hg.) (2025): States of Surveillance. Ethnographies of New Technologies in Policing and Justice, London/New York: Routledge.

Behr, Rafael (2016): »Präventionsstrategie(n) der deutschen Polizei im Wandel der letzten 25 Jahre«, in: Stephan Voß/Erich Marks (Hg.), 25 Jahre Gewaltprävention im Vereinten Deutschland – Bestandsaufnahme und Perspektiven, Berlin: Pro BUSINESS, S. 99–109.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access -

Belina, Bernd (2023): »Gefährliche Abstraktionen. Zur Einleitung (2023/2005)«, in: ders.: Gefährliche Abstraktionen. Regieren mittels Kriminalisierung und Raum, Münster: Westfälisches Dampfboot, S. 10–53.

Bennett, Tony/Dodsworth, Francis/Nobel, Greg/Poovey, Mary/Watkins, Megan (2013): »Habit and Habituation: Governance and the Social«, in: Body & Society 19 (2/3), S. 3–29.

Boersma, Asher (2025): »Leitstellen als öffentliche Orte: Gatekeeping zwischen Prestige, Konzentration und Resignation«, in: Franziska Reichenbecher/Gabriele Schabacher (Hg.), Medien des Gatekeeping. Akteure, Architekturen, Prozesse, Bielefeld: transcript, S. 329–350.

Brayne, Sarah (2021): Predict and Surveil: Data, Discretion, and the Future of Policing, New York: Oxford University Press.

Bretthauer, Sebastian (2017): Intelligente Videoüberwachung. Eine datenschutzrechtliche Analyse unter Berücksichtigung technischer Schutzmaßnahmen, Baden-Baden: Nomos.

Bröckling, Ulrich (2012): »Dispositive der Vorbeugung: Gefahrenabwehr, Resilienz, Precaution«, in: Christopher Daase/Philipp Offermann/Valentin Rauer (Hg.), Sicherheitskultur. Soziale und politische Praktiken der Gefahrenabwehr, Frankfurt a. M.: Campus, S. 93–108.

Bröckling, Ulrich (2017): Gute Hirten führen sanft. Über Menschenregierungskünste, Frankfurt a. M.: Suhrkamp.

Bundespolizei (2018): Abschlussbericht des Bundespolizeipräsidiums Potsdam zum Teilprojekt 1 »Biometrische Gesichtserkennung«, 11.10.2018, https://www.bundespolizei.de/Web/DE/04Aktuelles/01Meldungen/2018/10/181011_abschlussbericht_gesichtserkennung_down.pdf (zuletzt abgerufen 18.09.2020).

Bündnis90/Die Grünen (2020): Anfrage A035/2020 »Videoüberwachung in Mannheim«, 20.02.2020, https://buergerinfo.mannheim.de/buergerinfo/getfile.asp?id=8130662 (zuletzt abgerufen 14.05.2025).

Bürgerschaft der Freien und Hansestadt Hamburg (2023): Drucksache 22/12180 »Einsatz von künstlicher Intelligenz bei der Überwachung des Hansaplatzes«, Schriftliche Kleine Anfrage (DIE LINKE) und Antwort des Senats, 16.06.2023, www.buergerschaft-hh.de/parldok/dokument/84096/einsatz_von_kuenstlicher_intelligenz_bei_der_ueberwachung_des_hansaplatzes.pdf (zuletzt abgerufen 09.04.2025).

Bürgerschaft der Freien und Hansestadt Hamburg (2024): Drucksache 22/14472 »Einsatz von künstlicher Intelligenz bei der Überwachung des Hansaplatzes (VI)«, Schriftliche Kleine Anfrage (DIE LINKE) und Antwort des Senats, 23.02.2024, https://www.buergerschaft-hh.de/parldok/dokument/86533/22_14472_einsatz_von_kuenstlicher_intelligenz_bei_der_ueberwachung_des_hansaplatzes_vi#navpanes=0 (zuletzt abgerufen 24.04.2025).

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY

Cormier, Mickael (2021): »A Data Annotation Process for Human Activity Recognition in Public Places«, in: Jürgen Beyerer/Tim Zander (Hg.), Proceedings of the 2020 Joint Workshop of Fraunhofer IOSB and Institute for Anthropomatics, Vision and Fusion Laboratory, Karlsruhe: KIT Scientific Publishing, S. 33–51.

Cormier, Mickael/Röpkel, Fabian/Golda, Thomas/Beyerer, Jürgen (2021): »Interactive Labeling for Human Pose Estimation in Surveillance Videos«, in: Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV) Workshops, Online, S. 1649–1658.

Cormier, Mickael/Clepel, Aris/Specker, Andreas/Beyerer, Jürgen (2022): »Where are we with Human Pose Estimation in Real-World Surveillance?«, in: IEEE/CVF Winter Conference on Applications of Computer Vision Workshops (WACVW), Waikoloa, HI, USA, S. 591–601.

Dewey, James (2008 [1922]): »Human Nature and Conduct«, in: Jo Ann Boydston (Hg.), The Collected Works of John Dewey, Bd. 14, Carbondale/Edwardsville: University Press.

Dizdar, Dilek/Hirschauer, Stefan/Paulmann, Johannes/Schabacher, Gabriele (2021): »Humandifferenzierung. Disziplinäre Perspektiven und transdisziplinäre Anschlüsse«, in: dies (Hg.), Humandifferenzierung. Disziplinäre Perspektiven und empirische Sondierungen, Weilerswist: Velbrück, S. 7–31.

DSGVO (Datenschutzgrundverordnung) (2018), Fassung vom 27.04.2016, gültig ab 25.05.2018, https://dsgvo-gesetz.de (zuletzt abgerufen 26.04.2025).

Egbert, Simon/Leese, Matthias (2021): Criminal Futures. Predictive Policing and Everyday Police Work, London/New York: Routledge.

EU AI Act (EU Artificial Intelligence Act) (2024), Fassung vom 13.06.2024, gültig ab 01.08.2024, http://data.europa.eu/eli/reg/2024/1689/oj (zuletzt abgerufen 26.04.2025).

Farocki, Harun: (2004): »Phantom Images«, in: Public 29, S. 12–24.

Fruin, John (1993): »The Causes and Prevention of Crowd Disasters«, in: Roderick Smith/Jim Dickie (Hg.), Engineering for Crowd Safety, Proceedings of the International Conference on Engineering for Crowd Safety, London: Elsevier Science Publishers BV, S. 99–108.

Gießmann, Sebastian/Gerlitz, Carolin (2023): »Test. Einleitung in den Schwerpunkt«, in: Zeitschrift für Medienwissenschaft 29, S. 9–19.

Golda, Thomas/Cormier, Mickael/Beyerer, Jürgen (2022): »Intelligente Bild- und Videoauswertung für die Sicherheit«, in: Helmut Siller/Dieter Wehe (Hg.), Handbuch Polizeimanagement. Polizeipolitik – Polizeiwissenschaft – Polizeipraxis, 2. Aufl., Wiesbaden: Springer, S. 1487–1507.

Grüne Jugend (2019): »›Silent-Dance‹ gegen Videoüberwachung«, Pressemitteilung, 04.05.2019, https://www.gj-mannheim.de/pressemitteilungen (zuletzt abgerufen 09.04.2025).

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY

Grusin, Richard (Hg.) (2022): Insecurity. Investigating Insecurity as the Predominant Logic of Life in the Present Moment, Minneapolis: University of Minnesota Press.

Gupta, Neha/Gupta, Suneet K./Pathak, Rajesh K./Jain, Vanita/Rashidi, Parisa/Suri, Jasjit S. (2022): »Human Activity Recognition in Artificial Intelligence Framework: A Narrative Review«, in: Artificial Intelligence Review 55, S. 4755–4808.

Halpern, Orit/LeCavalier, Jesse/Calvillo, Nerea/Pietsch, Wolfgang (2013): »Test-Bed Urbanism«, in: Public Culture 25 (2), S. 273–306.

Hentschel, Christine/Krasmann, Susanne/Zebrowksi, Chris (2025): »Situational Awareness. Sensing Insecurity and Coming Catastrophes«, in: Critical Studies on Security 13 (1), S. 1–5.

Hermann, Dieter (2012): Kriminalitätsfurcht, Kriminalität und Lebensqualität. Eine Audit-Studie zur urbanen Sicherheit in Mannheim, Institut für Kriminologie, Universität Heidelberg, https://buergerinfo.mannheim.de/buergerinfo/getfile.asp?id=8034317 (zuletzt abgerufen 09.04.2025).

Hermann, Dieter (2017): Mannheimer Sicherheitsaudit 2017, Institut für Kriminologie, Universität Heidelberg, https://buergerinfo.mannheim.de/buergerinfo/getfile.asp?id=8084470 (zuletzt abgerufen 09.04.2025).

Hermann, Dieter (2021): Mannheimer Sicherheitsaudit 2020, Institut für Kriminologie, Universität Heidelberg, https://buergerinfo.mannheim.de/buergerinfo/getfile.asp?id=8154975 (zuletzt abgerufen 09.04.2025).

Hermann, Dieter (2023): Mannheimer Sicherheitsaudit 2022/2023, Institut für Kriminologie, Universität Heidelberg, https://www.mannheim.de/sites/default/files/2023-04/Gutachten-MA-2023_final.pdf (zuletzt abgerufen 09.04.2025).

HSOG (Hessisches Gesetz über die öffentliche Sicherheit und Ordnung): Fassung vom 13.12.2024, gültig ab 02.02.2025, www.rv.hessenrecht.hessen.de/bshe/document/jlr-SOGHEV30P14 (zuletzt abgerufen 09.04.2025).

IM BW (Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg) (2018): Pressemitteilung »Startschuss für die algorithmenbasierte Videoüberwachung beim Polizeipräsidium Mannheim«, 03.12.2018, https://im.baden-wuerttemberg.de/de/service/presse-und-oeffentlichkeitsarbeit/pressemitteilung/pid/startschuss-fuer-die-algorithmenbasierte-videoueberwachung-beim-polizeipraesidium-mannheim (zuletzt abgerufen 14.04.2025).

IM BW (Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg) (2023a): Pressemitteilung »Aktionsplan ›Mehr Sicherheit für Mannheim‹«, 04.12.2023, https://im.baden-wuerttemberg.de/de/service/presse-und-oeffentlichkeitsarbeit/pressemitteilung/pid/aktionsplan-mehr-sicherheit-fuer-mannheim (zuletzt abgerufen 09.04.2025).

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access -

IM BW (Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg) (2023b): Drucksache 17/5816, Antwort auf Antrag »Projekt ›Intelligente Videoüberwachung‹ in Mannheim kurz vor dem Abschluss – wie geht es weiter?«, 19.12.2023, https://www.landtag-bw.de/resource/blob/264574/e713ff79155c12a2536c0300ab0d82f7/17_5816_D.pdf (zuletzt abgerufen 24.04.2025).

IM BW (Ministerium des Inneren, für Digitalisierung und Kommunen Baden-Württemberg) (2024): Drucksache 17/6392, Nr. 5, »Beschlussempfehlung« zur Drucksache 17/5816, 31.01.2024, S. 11–12, https://www.landtag-bw.de/resource/blob/265612/180a805f9d5eecc1d89d522f60b39f50/17_6392_D.pdf (zuletzt abgerufen 03.04.2025).

Jasanoff, Sheila/Kim, Sang-Hyun (Hg.) (2015): Dreamscapes of Modernity: Sociotechnical Imaginaries and the Fabrication of Power, Chicago: University of Chicago Press.

Kaufmann, Mareile/Egbert, Simon/Leese, Matthias (2019): »Predictive Policing and the Politics of Pattern«, in: The British Journal of Criminology 59 (3), S. 674–692.

Kaufmann, Stefan/Wichum, Ricky (2016): »Risk and Security: Diagnosis of the Present in the Context of (Post-)Modern Insecurities«, in: Historical Social Research 41 (1), S. 48–69.

Klute, Amira (2025): »Hallenbad mit KI-Assistenz. Die digitale Badeaufsicht«, TAZ, 17.03.2025, https://taz.de/Hallenbad-mit-KI-Assistenz/!6066129 (zuletzt abgerufen 9.4.2025).

Koch, Lars/Nanz, Tobias/ Pause, Johannes (2016): »Imaginationen der Störung. Ein Konzept«, in: Behemoth 9 (1), S. 6–23.

Landtag von Baden-Württemberg (2020): Drucksache 16/8128 »Zwischenergebnisse des Pilotprojekts zur ›intelligenten Videoüberwachung‹ in Mannheim«, Antwort auf Kleine Anfrage (SPD), 15.05.2020, https://www.landtag-bw.de/files/live/sites/LTBW/files/dokumente/WP16/Drucksachen/8000/16_8128_D.pdf (zuletzt abgerufen 18.04.2025).

Low, Setha/Maguire, Mark (Hg.) (2019): Spaces of Security: Ethnographies of Securityscapes, Surveillance and Control, New York: New York University Press.

Lulamae, Josephin (2023): »In Mannheim, an Automated System Reports Hugs to the Police«, 18.07.2023, Algorithm Watch, https://algorithmwatch.org/en/mannheim-system-reports-hugs-police/ (zuletzt abgerufen 09.04.2025).

Marres, Noortje/Stark, David (2020): »Put to the Test: For a New Sociology of Testing«, in: The British Journal of Sociology 71 (3), S. 423–443.

Marti, Urs/Kahle, Hans-Gert/Aksoy, Ahmet/Deniz, Rasim (1991): GPS-Projekt Marmara. Dokumentation der ersten Messkampagne September 90, IGP-Bericht Nr. 179, Zürich: ETH Zürich, https://ethz.ch/content/dam/ethz/spe

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access -

cial-interest/baug/igp/igp-dam/documents/Reports/179.pdf (zuletzt abgerufen 18.04.2025).

Martin, Manuel (2023): 3D Human Body Pose-Based Activity Recognition for Driver Monitoring Systems, Dissertation, Karlsruhe: KIT.

Meyer, Roland (2014): »Augmented Crowds. Identitätsmanagement, Gesichtserkennung und Crowd Monitoring«, in: Inge Baxmann/Timon Beyes/Claus Pias (Hg.), Soziale Medien – Neue Massen, Zürich: Diaphanes, S. 103–118.

Meyer, Roland (2019): Operative Porträts. Eine Bildgeschichte der Identifizierbarkeit von Lavater bis Facebook, Konstanz: Konstanz University Press.

Monari, Eduardo/Fischer, Yvonne/Anneken, Mathias (2015): »NEST-CrowdControl. Advanced Video-based Crowd Monitoring for Large Public Events«, in: Future Security 2015. Berlin, September 15–17, S. 49–56, https://publica-rest.fraunhofer.de/server/api/core/bitstreams/ce8f1feb-5a07-47c7-a08e-835061f0d519/content (zuletzt aufgerufen 18.04.2025).

Monari, Eduardo/Fischer, Yvonne (2017): »NEST CrowdControl – Videobasiertes Assistenzsystem für die Sicherheit von Grossveranstaltungen«, in: VisIT 18 (3), S. 12–13, https://publica.fraunhofer.de/bitstreams/c2daa307-0a2c-413c-ad26-b6dd7377b2d1/download (zuletzt abgerufen 09.04.2025).

Morozov, Evgeny (2013): To Save Everything, Click Here: The Folly of Technological Solutionism, New York: PublicAffairs.

Moser, Jeannie/Vagt, Christina (2018) (Hg.): »Verhaltensdesign. Technologische und ästhetische Programme der 1960er und 1970er Jahre«, in: dies. (Hg.), Verhaltensdesign. Technologische und ästhetische Programme der 1960er und 1970er Jahre, Bielefeld: transcript, S. 7–24.

Nishiyama, Hidefumi (2018): »Crowd Surveillance: The (In)Securitization of the Urban Body«, in: Security Dialogue 49 (3), S. 200–216.

OpenPetition (2018): »Offener Brief zum Ausbau der Videoüberwachung in Mannheim – Wir sagen NEIN!«, Petition von Humanistische Union, Grüne Jugend Mannheim, Selbstbestimmt Digital e. V., Bündnis90/Die Grünen Mannheim, 27.09.2018, https://www.openpetition.de/petition/online/offener-brief-zum-ausbau-der-videoueberwachung-in-mannheim-wir-sagen-nein (zuletzt abgerufen 09.04.2025).

Pantenburg, Volker (2017): »Working Images. Harun Farocki and the Operational Image«, in: Jens Eder/Charlotte Klonk (Hg.), Image Operations. Visual Media and Political Conflict, Manchester: Manchester University Press, S. 49–62.

Parikka, Jussi (2023): Operational Images: From the Visual to the Invisual, Minneapolis/London: University of Minnesota Press.

Pietsch, Klaus/Hauck, Nils (2021): »Algorithmenbasierte Bildauswertung – innovativer Baustein der Sicherheitsarchitektur im urbanen Raum«, in: Hans-Jürgen Lange/Christian Kromberg/Anna Rau (Hg.), Urbane Sicherheit. Migration und der Wandel kommunaler Sicherheit, Wiesbaden: Springer VS, S. 85–115.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY

PolG BW (Polizeigesetz Baden-Württemberg) (2017), Fassung vom 28.11.2017, gültig ab 08.12.2017, https://www.landesrecht-bw.de/bsbw/document/jlr-PolGBW1992V15P21 (zuletzt abgerufen 22.4.2025).

PolG BW (Polizeigesetz Baden-Württemberg) (2021), Fassung vom 06.10.2020, gültig ab 17.01.2021, https://www.landesrecht-bw.de/bsbw/document/jlr-PolGBW2021pP44 (zuletzt abgerufen 09.04.2025).

Polizeipräsidium Mannheim (2018): Datenschutzkonzept der Polizei Mannheim, »Projektgruppe Videoüberwachung Mannheim 2017«, 14.12.2018, https://fragdenstaat.de/anfrage/informationen-zum-thema-videobeouberwachung-142/707444/anhang/datenschutzkonzeptvideoberwachunggeschwrzt.pdf (zuletzt abgerufen 09.04.2025).

Polizeipräsidium Mannheim (2019a): »Polizeiliche Kriminalitätsstatistik 2018«, 27.03.2019, https://www.presseportal.de/blaulicht/pm/14915/4229213 (zuletzt abgerufen 01.10.2021).

Polizeipräsidium Mannheim (2019b): »Polizeiliche Videoüberwachung im Bereich Mannheim, ›Breite Straße‹ – Errichtungsanordnung«, 17.06.2019, https://fragdenstaat.de/anfrage/informationen-zum-thema-videobeouberwachung-142/615937/anhang/anlagen1und4bis7_geschwaerzt.pdf (zuletzt abgerufen 09.04.2025).

Rau, Franziska (2023): »Intelligente Videoüberwachung. Polizei Hamburg will ab Juli Verhalten automatisch erkennen«, 19.06.2023, netzpolitik.org, https://netzpolitik.org/2023/intelligente-videoueberwachung-polizei-hamburg-will-ab-juli-verhalten-automatisch-scannen/ (zuletzt abgerufen 09.04.2025).

Rauert, Louis (2019): »Umarmungen in Dauerschleife: Tanz-Demo gegen Kameras«, in: Mannheimer Morgen, 06.05.2019, https://www.mannheimer-morgen.de/orte/mannheim_artikel,-mannheim-umarmungen-in-dauerschleife-tanz-demo-gegen-kameras-_arid,1447000.html (zuletzt abgerufen 09.04.2025).

Reichenbecher, Franziska (2025): »Door Work. Türsteher, Türhänger und die Medien des Gatekeeping«, in: dies./Gabriele Schabacher (Hg.), Medien des Gatekeeping. Akteure, Architekturen, Prozesse, Bielefeld: transcript, S. 67–102.

Reichenbecher, Franziska/Gabriele Schabacher (2025): »Medien des Gatekeeping. Einleitung«, in: dies. (Hg.), Medien des Gatekeeping. Akteure, Architekturen, Prozesse, Bielefeld: transcript, S. 7–44.

Reuter, Markus (2024): »Panoptischer Rewe-Supermarkt. Einkaufen mit Skelettkontrolle«, 13.01.2024, netzpolitik.org, https://netzpolitik.org/2024/panoptischer-rewe-supermarkt-einkauf-mit-skelettkontrolle/ (zuletzt abgerufen 09.04.2025).

Runkel, Simon (2019): »Eine Kulturgeschichte des Crowd Management in gebauten Versammlungsstätten. Soziomechanische, affektive, technokratische und

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY

mediale Sicherheits- und Kontrollregimes«, in: Christoph Groneberg (Hg.), Veranstaltungskommunikation, Wiesbaden: Springer VS, S. 129–167.

Schabacher, Gabriele (2021): »Infrastrukturen und Verfahren der Humandifferenzierung. Medienkulturwissenschaftliche Perspektiven«, in: Dilek Dizdar/Stefan Hirschauer/Johannes Paulmann/Gabriele Schabacher (Hg.), Humandifferenzierung. Disziplinäre Perspektiven und empirische Sondierungen, Weilerswist: Velbrück, S. 287–313.

Schabacher, Gabriele (2023): »AI and the Work of Patterns. Recognition Technologies, Classification, and Security«, in: Andreas Sudmann/Anna Echterhölter/Markus Ramsauer/Fabian Retkowski/Jens Schröter/Alexander Waibel (Hg), Beyond Quantity. Research with Subsymbolic AI, Bielefeld: transcript, S. 123–154.

Schabacher, Gabriele/Spallinger, Sophie (2023): »Tests als Medien der Gewöhnung. Pilotversuche am Bahnhof«, in: Zeitschrift für Medienwissenschaft 29, S. 35–50.

Scheiwe, Hannah (2023): »KI-Kameras: Umstrittene Helfer der Polizei«, RedaktionsNetzwerk Deutschland, 15.06.2023, https://www.rnd.de/panorama/ki-kameras-umstrittener-freund-und-helfer-der-polizei-Z62ORVRR7VJTZF4MAIQQSXL4RI.html (zuletzt abgerufen 09.04.2025).

Seiler, Eberhard (1983): Grundbegriffe des Meß- und Eichwesens, Wiesbaden: Vieweg und Teuber.

Sprenger, Florian (2021): »Autonome Automobilität. Eine medien- und kulturwissenschaftliche Einführung«, in: ders. (Hg.), Autonome Autos. Medien- und kulturwissenschaftliche Perspektiven auf die Zukunft der Mobilität, Bielefeld: transcript, S. 9–81.

Stadt Mannheim (2012): Informationsvorlage V537/2012 »Sicherheitsbefragung«, 04.10.2012, https://buergerinfo.mannheim.de/buergerinfo/getfile.asp?id=8034316 (zuletzt abgerufen 09.04.2025).

Stadt Mannheim (2017a): Informationsvorlage V450/2017 »Ausbau der Videoüberwachung«, 02.10.2017, https://buergerinfo.mannheim.de/buergerinfo/getfile.asp?id=8082792 (zuletzt abgerufen 09.04.2025).

Stadt Mannheim (2017b): Informationsvorlage V450/2017 »Ausbau der Videoüberwachung«, Anlage, 02.10.2017, https://buergerinfo.mannheim.de/buergerinfo/getfile.asp?id=8082800 (zuletzt abgerufen 09.04.2025).

Stadt Mannheim (2017c): Informationsvorlage V562/2017 »Ergebnisse der Sicherheitsbefragung 2016«, 13.11.2017, https://buergerinfo.mannheim.de/buergerinfo/getfile.asp?id=8084469 (zuletzt abgerufen 09.04.2025).

Stadt Mannheim (2018a): Präsentationsfolien der Informationsveranstaltung »Videoüberwachung in Mannheim«, 27.06.2018, https://media.frag-den-staat.de/files/foi/98124/VideoberwachungBezirksbeirteInfoVfinaleFassung.pdf (zuletzt abgerufen 09.04.2025), inaktiv.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access -

Stadt Mannheim (2018b): Pressemitteilung »Startschuss für intelligente Videoüberwachung«, 03.12.2018, www.mannheim.de/de/nachrichten/startschuss-fuer-intelligente-videoueberwachung (zuletzt abgerufen 15.08.2021), inaktiv.

Stadt Mannheim (2021a): Informationsvorlage V222/2021 »Ergebnisse der Sicherheitsbefragung 2020«, 20.04.2021, https://buergerinfo.mannheim.de/buergerinfo/getfile.asp?id=8155204 (zuletzt abgerufen 09.04.2025).

Stadt Mannheim (2021b): Informationsvorlage V564/2021 »Videoüberwachung in Mannheim«, 08.10.2021, https://buergerinfo.mannheim.de/buergerinfo/getfile.asp?id=8167178 (zuletzt abgerufen 09.04.2025).

Stadt Mannheim (2023): Informationsvorlage V245/2023 »Ergebnisse der Mannheimer Sicherheitsbefragung 2022/2023«, 19.04.2023, https://buergerinfo.mannheim.de/buergerinfo/getfile.asp?id=8187882 (zuletzt abgerufen 09.04.2025).

Stadt Mannheim (2024): Informationsvorlage V042/2024 »Aktueller Sachstand intelligenter Videoschutz«, 19.01.2024, https://buergerinfo.mannheim.de/buergerinfo/getfile.asp?id=8201325 (zuletzt abgerufen 18.04.2025).

Staller, Mario/Koerner, Swen (Hg.) (2021): Handbuch polizeiliches Einsatztraining. Professionelles Konfliktmanagement – Theorie, Trainingskonzepte und Praxiserfahrungen, Wiesbaden: Springer.

Stanley, Jay (2019): »The Dawn of Robot Surveillance: AI, Video Analytics, and Privacy«, New York: American Civil Liberties Union, 13.06.2019, https://www.aclu.org/publications/dawn-robot-surveillance (zuletzt abgerufen 24.04.2025).

Teepe, Torben/Gilg, Johannes/Herzog, Fabian/Hörmann, Stefan/Rigoll, Gerhard (2022): »Towards a Deeper Understanding of Skeleton-based Gait Recognition«, in: 2022 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), New Orleans, LA, USA, S. 1568–1576.

Trüper, Thomas (2017): Meinungsbericht des Stadtrats DIE LINKE, »Wiedereinführung der Videoüberwachung in Mannheimer City«, 18.10.2017, https://kommunalinfo-mannheim.de/2017/10/18/wiedereinfuehrung-der-videoueberwachung-in-der-mannheimer-city/ (zuletzt abgerufen 09.04.2025).

Ullrich, Peter/Tullney, Marco (2012): »Die Konstruktion ›gefährlicher Orte‹. Eine Problematisierung mit Beispielen aus Berlin und Leipzig«, in: sozialraum.de (4) Ausgabe 2/2012, https://www.sozialraum.de/die-konstruktion-gefaehrlicher-orte.php (zuletzt abgerufen 18.04.2025).

Virilio, Paul (1989): Die Sehmaschine, Berlin: Merve.

Voth, Sascha (2019): »NEST: Intelligente Videoüberwachung«, in: VisIT 20 (1), S. 6–7, https://services.iosb.fraunhofer.de/visIT/intelligentesicherheitstechnik/ (zuletzt abgerufen 09.04.2025).

Wietschorke, Jens (2025): »Theorie des Türhüters. Eine Skizze zur Kulturanalyse intermediärer Figuren«, in: Franziska Reichenbecher/Gabriele Schabacher

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY

(Hg.), Medien des Gatekeeping. Akteure, Architekturen, Prozesse, Bielefeld: transcript, S. 47–66.

Zurawski, Nils (2014): »Kartografien des Risikos. Das Unbekannte und die imaginären Geografien der Sicherheit«, in: Kritische Berichte 42 (3), S. 67–76.

Onlinequellen

BündnisHansaplatz, Homepage, https://buendnis-hansaplatz.de/ (inaktiv).

Fraunhofer IOSB (Institut für Optronik, Systemtechnik und Bildauswertung) (2025a): »Abteilung Videoauswertesystem (VID) und Abteilungsgruppe Videobasierte Sicherheits- und Assistenzsysteme«, Homepage, https://www.iosb.fraunhofer.de/de/kompetenzen/bildauswertung/video-exploitation-systems/forschungsthemen.html (zuletzt abgerufen 09.04.2025).

Fraunhofer IOSB (Institut für Optronik, Systemtechnik und Bildauswertung) (2025b): »Network Enabled Surveillance and Tracking (NEST)«, Homepage des Forschungsprojekts, https://www.iosb.fraunhofer.de/de/projekte-produkte/nest.html (zuletzt abgerufen 09.04.2025).

Fraunhofer IOSB (Institut für Optronik, Systemtechnik und Bildauswertung) (2025c): »NurseEye«, Homepage des Forschungsprojekts, https://www.iosb.fraunhofer.de/de/projekte-produkte/nurse-eye.html (zuletzt abgerufen 09.04.2025).

Fraunhofer IOSB (Institut für Optronik, Systemtechnik und Bildauswertung) (2025d): »S²UCRE. Sicherheit in städtischen Umgebungen: Crowd-Monitoring, Prädiktion und Entscheidungsunterstützung«, Homepage des Forschungsprojekts, https://www.iosb.fraunhofer.de/de/projekte-produkte/s2ucre.html (zuletzt abgerufen 09.04.2025).

KIT (Karlsruher Institut für Technologie) (o. J.): »KITcube – Integrated Atmospheric Observation System«, https://www.kitcube.kit.edu/61.php (zuletzt abgerufen 18.04.2025).

Marx.wtf [Matthias Marx] (2024): »Hansaplatz-Versuch war kein Erfolg«, 24.12.2024, https://marx.wtf/2024/12/24/der-hansaplatz-versuch-war-kein-Erfolg/ (zuletzt abgerufen 09.04.2025).

MPI (Max Planck-Institut) für Meteorologie (2021): »FESSTVaL: Großangelegte Messkampagne zur Erfassung kleinräumiger Wetterphänomene«, 17.05.2021, https://mpimet.mpg.de/kommunikation/detailansicht-news/fesstval-grossangelegte-messkampagne-zur-erfassung-kleinraeumiger-wetterphaenomene (zuletzt abgerufen, 18.04.2025).

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY-NC

Audioviduelle Quellen

Algorithmenbasierte Kameraüberwachung, Dokumentation, D 2022, Regie: Martin Mannweiler, 40 Min.

All Eyes on You, Dokumentation, D 2021, Regie: Michaela Kobsa-Mark, 33 Min.

Kommunalinfo Mannheim (2019): »Silent Dance – Flashmob gegen Videoüberwachung in Mannheim«, Video, 06.05.2019, YouTube, https://www.youtube.com/watch?v=NL9uQJyS17U (zuletzt abgerufen 09.04.2025).

Interviews mit Expert:innen

Interview Sophie Spallinger mit Stadträtin Bündnis90/Die Grünen Mannheim, 01.10.2021.

Interview Sophie Spallinger mit ehemaligem Bezirksbeiratssprecher Bündnis90/Die Grünen, Neckarstadt Mannheim, 04.10.2021.

Interview Sophie Spallinger mit Mitglied des Chaos Computer Club Mannheim, 06.10.2021.

Interview Sophie Spallinger mit Projektleiter Gruppe Videobasierte Sicherheits- und Assistenzsysteme, Fraunhofer IOSB, 19.10.2021.

Interview Sophie Spallinger mit projektinternem Informatiker des Fraunhofer IOSB, 09.05.2022.

Interview Sophie Spallinger mit Mitarbeitendem von Digitalcourage e. V., 07.12.2023.

Interview Sophie Spallinger mit Sprecher vom Chaos Computer Club Hamburg, 13.12.2023.

Interview Sophie Spallinger mit Projektleiter »Videoschutz«, Polizeipräsidium Mannheim, 19.06.2024.

Abbildungen

Abb. 1: Stadt Mannheim (2018a): Präsentationsfolien der Informationsveranstaltung »Videoüberwachung in Mannheim«, 27.06.2018, https://media.frag-den-staat.de/files/foi/98124/VideoberwachungBezirksbeirteInfoVfinaleFassung.pdf (zuletzt abgerufen 09.04.2025), Folie 8.

Abb. 2: Polizeipräsidium Mannheim/Stadt Mannheim (2019): Handout »Infos zum Videoschutz in Mannheim«, https://ppmannheim.polizei-bw.de/wp-content/uploads/sites/8/2019/08/VideoueberwachungMA_Info.pdf (zuletzt abgerufen 09.04.2025), S. 3.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY

Abb. 3: Golda, Thomas/Cormier, Mickael/Beyerer, Jürgen (2022): »Intelligente Bild- und Videoauswertung für die Sicherheit«, in: Dieter Wehe/Helmut Siller (Hg.), Handbuch Polizeimanagement. Polizeipolitik – Polizeiwissenschaft – Polizeipraxis, Wiesbaden: Springer, S. 1493.

Abb. 4: Eigene Fotografie, Sophie Spallinger, 04.10.2021.

Abb. 5: Vom Polizeipräsidium Mannheim/Fraunhofer IOSB im Juni 2024 zur Verfügung gestelltes Videomaterial, Aufnahme vom 06.08.2020, Screenshot.

Abb. 6: Kommunalinfo Mannheim (2019): »Silent Dance – Flashmob gegen Videoüberwachung in Mannheim«, Video, 06.05.2019, YouTube, https://www.youtube.com/watch?v=NL9uQJyS17U (zuletzt abgerufen 09.04.2025), TC: 00:01:09, Screenshot.

Abb. 7: Eigene Fotografie, Sophie Spallinger, 19.06.2024.

Abb. 8: Bürgerschaft der Freien und Hansestadt Hamburg (2024): Drucksache 22/14472, 23.02.2024, https://www.buergerschaft-hh.de/parldok/dokument/86533/22_14472_einsatz_von_kuenstlicher_intelligenz_bei_der_ueberwachung_des_hansaplatzes_vi#navpanes=0 (zuletzt abgerufen 9.4.2025), S. 2–3, Ausschnitt.

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access -

https://doi.org/10.14361/9783839458594-011 https://www.inlibra.com/de/agb - Open Access - (cc) BY-SA