

Unterrichtung

Hannover, den 18.06.2020

Die Präsidentin des Niedersächsischen Landtages
- Landtagsverwaltung -

Können ein Mehr an Sicherheit und Datenschutz mit einer videobasierten Situations- und Gegenstandserkennung gleichermaßen verwirklicht werden?

Antrag der Fraktion der SPD und der Fraktion der CDU - Drs. 18/3415

Beschluss des Landtages vom 14.05.2019 - Drs. 18/3744 - nachfolgend abgedruckt:

Können ein Mehr an Sicherheit und Datenschutz mit einer videobasierten Situations- und Gegenstandserkennung gleichermaßen verwirklicht werden?

Der Landtag stellt zur Diskussion um den sicherheitspolitischen Nutzen intelligenter Videoauswertung fest, dass die Grenzen zwischen Freiheit und Sicherheit angesichts des digitalen Fortschritts, insbesondere auch im Bereich der Künstlichen Intelligenz (KI), stets neu sorgsam ausbalanciert werden müssen.

Für Niedersachsen werden die Regelungen über die Videoüberwachung zur Erkennung von Gefahrensituationen und von gefährlichen Gegenständen an Kriminalitätsschwerpunkten im neuen Polizeigesetz konkretisiert und an die zwischenzeitlich ergangene Rechtsprechung angepasst. Herkömmliche Videoüberwachungsmaßnahmen, insbesondere zur Verhinderung von Straftaten oder zur Vorbeugung vor Gefahrensituationen, haben eine bisweilen präventive Wirkung. Eine automatisierte Auswertung von Videobildern zur Erkennung und Meldung gefahrenträchtiger Situationen und Gegenstände, wie beispielsweise eine am Boden liegende Person, gewalttätige Auseinandersetzungen von Personen oder herrenlose Koffer, könnte diese präventive Wirkung von Videoüberwachung noch steigern. Hierzu liegen aber bislang erst wenige Erfahrungen vor, und auch die mit solchen Maßnahmen verbundenen Rechtsfragen sind noch nicht umfassend geprüft.

In einem breiten Diskurs sollen daher Einsatzmöglichkeiten und Anforderungen der Sicherheitsbehörden sowie technische Lösungen und rechtliche Rahmenbedingungen entsprechender Videoauswertetechnik erörtert werden. Auf dieser Grundlage kann bewertet werden, ob und gegebenenfalls inwieweit eine automatisierte, auf das Erkennen gefahrenträchtiger Szenarien bzw. Gegenstände gerichtete Auswertung von Videoaufnahmen dazu beitragen kann, die präventive Wirkung der Videoüberwachung zu erhöhen. Dabei muss es gleichzeitig darauf ankommen, die Tiefe des Eingriffs in das Recht auf informationelle Selbstbestimmung soweit wie möglich zu reduzieren.

Der Landtag bittet daher die Landesregierung,

1. die praktischen Anwendungsmöglichkeiten einer „intelligenten“ videobasierten Situations- bzw. Gegenstandserkennung durch die Landespolizei - einschließlich des rechtlichen Rahmens - zu untersuchen und hierzu einen Bericht zu entwickeln, der folgende Punkte umfasst:
 - a) Darstellung und Auswertung der bestehenden bundes- und landesgesetzlichen Regelungen und Projekte,
 - b) Darstellung sicherheitspolitisch sinnvoller Einsatzbereiche in Niedersachsen,
 - c) datenschutzrechtliche Bewertung der jeweiligen Fallkonstellationen,
 - d) fachliche und wirtschaftliche Bewertung bereits verfügbarer Technologien,
 - e) sicherheitspolitische Priorisierung von Projekten oder Vorhaben, die für einen Einsatz der Videoauswertetechnik infrage kommen,
2. in einem pluralistischen Verfahren die Landesbeauftragte für den Datenschutz in einen öffentlichen Diskurs zur Einführung einer Videotechnik mit automatischer Situations- oder Gegen-

- standserkennung ebenso einzubeziehen wie Bürgerinnen und Bürger, Unternehmen, Gewerkschaften und Verbände,
3. bis zum Frühjahr 2020 dem Landtag einen entsprechenden Bericht vorzulegen,
 4. auf Basis der Erkenntnisse und einer konsensualen positiven Beurteilung eine rechtliche Grundlage für einen möglichen Einsatz intelligenter Videotechnik zu entwickeln.

Antwort der Landesregierung vom 17.06.2020

Sicherheit ist ein elementares Grundbedürfnis des Menschen, das dessen Denk- und Gefühlswelt wie auch Schutzvorkehrungen umfasst.¹ Dabei beinhaltet sie verschiedene Bereiche, wie z. B. Wirtschaft, Soziales als auch innere und äußere Sicherheit. Aus dem Gemeinsinn der Verfassung ergibt sich für den Staat u. a. die Verpflichtung zum Schutz ihrer Bürgerinnen und Bürger vor Bedrohungen, Gewalt und Kriminalität. Damit diese Innere Sicherheit gewährleistet werden kann, haben die für das Staatswesen verantwortlichen Akteure die entsprechenden Rahmenbedingungen zu schaffen. Dabei ist es vor dem Hintergrund der sich aus der anhaltend hohen abstrakten Gefährdungslage erwachsenden Herausforderungen für die öffentliche Sicherheit umso wichtiger, die Strukturen und Prozesse zukunftsfähig zu gestalten.

Die niedersächsischen Regierungsparteien streben für die Wahlperiode 2017 bis 2022 die gezielte Videoüberwachung an Kriminalitätsschwerpunkten an. Vor einer Entscheidung sollen jedoch die Ergebnisse des Modellversuches in Berlin bewertet und geprüft werden.²

Durch die Polizei des Landes Niedersachsen erfolgt zurzeit ausschließlich eine konventionelle Videobeobachtung öffentlich zugänglicher Räume im Rahmen der gesetzlichen Vorgaben zum Erkennen und der Abwehr von Gefahren und zur Verhütung und Verfolgung von Straftaten. Die Einsatzmöglichkeiten erstrecken sich dabei hauptsächlich auf die Überwachung besonderer kriminalgeografischer Räume und die Beobachtung des öffentlichen Verkehrsflusses zur Gewährleistung der Sicherheit und Leichtigkeit des Straßenverkehrs. Dabei ist die dauerhafte Aufzeichnungsfunktion aus Gründen der Verhältnismäßigkeit nur teilweise aktiviert. Bei der polizeilichen Begleitung von Großveranstaltungen im Sport- und Kulturbereich und Versammlungen erfolgt eine Aufzeichnung nur zeitweise, respektive infolge besonderer Einsatzlagen sowie bei der Verfolgung und Beweissicherung von Straftaten.

Eine automatisierte Liveauswertung von Videobilddateien nach bestimmten intelligenten Kriterien mit Abgleich vorhandener Datenbestände in Echtzeit erfolgt in Niedersachsen polizeilicherseits bislang nicht. Die Nutzung einer automatisierten, auf Algorithmen basierenden Analysesoftware könnte ein geeignetes Mittel zur Gefahrenabwehr und auch zur Aufklärung von bereits erfolgten Straftaten sein. Ein alternativ durchzuführendes und durchgehendes Monitoring durch Personal widerspricht einem ressourcenschonenden Personaleinsatz und ist auch vor dem Hintergrund bestehender Einschränkungen der menschlichen Wahrnehmungsfähigkeit im Rahmen einer pausenlosen Monitorüberwachung nicht zielführend. Beim Landeskriminalamt Niedersachsen (LKA NI) wird zurzeit die Entwicklung einer intelligenten Software zur Anomalie-Erkennung auf Basis des Maschinenlernens im Rahmen des Projektes „Weiterentwicklung der polizeilichen Analyse“ vorangetrieben. Durch die Erarbeitung einer ganzheitlichen Analyseinfrastruktur für die Auswertung von Masendaten aller Art werden im LKA NI neuronale Netze für spezifische Anwendungsfälle trainiert. Diese neuronalen Netze sind Computerprogramme, die in der Lage sind, retrograde Analysen durchzuführen und somit eigenständig Muster in bereits erhobenen und gespeicherten Daten zu erkennen und diese zu bewerten. Es ist darauf hinzuweisen, dass in einem konkreten Strafverfahren ein entsprechender Abgleich durchgeführt worden ist und darüber hinaus Daten im Rahmen von Testanwendungen automatisiert analysiert werden, die zu Zwecken der Strafverfolgung verarbeitet werden können. Seit Anfang des Jahres wird in Niedersachsen als erstem Bundesland in einem landesweiten Modellprojekt zur Bekämpfung von Kinderpornografie ein eigens entwickeltes neuronales Netz von den Ermittlern in den Polizeiinspektionen zur Priorisierung sichergestellter Da-

¹ vgl. Max-Planck-Gesellschaft, Forschungsbericht 2012, Studien zur Sicherheit in Deutschland.

² vgl. Koalitionsvereinbarung zwischen der SPD und der CDU für die 18. Wahlperiode des Niedersächsischen Landtages 2017-2022, Rz. 852-856.

teien getestet. Während es jedoch bei der automatisierten Videobeobachtung öffentlicher Räume um eine anlassunabhängige bzw. anlassbezogene Dauerbeobachtung geht, steht bei diesem Modellversuch der effiziente Umgang mit riesigen Datenmengen an sichergestellten vermeintlich inkriminierten Lichtbild- und Videomassendaten im Vordergrund. Ziel ist hierbei, die Ermittlerinnen und Ermittler technisch zu unterstützen und langfristig die Bearbeitungsdauer durch die Reduzierung der hohen Anzahl an zu sichtenden Dateien deutlich zu beschleunigen.

Während sich die althergebrachte präventive Videobeobachtung in den gesetzlichen Vorschriften von Bund und Ländern über Jahre etabliert hat, besteht in den Auffassungen zur intelligenten Videoüberwachung im Lichte von Rechtswissenschaft und Praxis eine ausgeprägte Diversität. Befürworter argumentieren, dass sich intelligente Maßnahmen auf die gesetzlichen Vorschriften zur konventionellen Videoüberwachung stützen ließen. Dabei beziehen sie sich auf ein Urteil des Bundesverfassungsgerichts (BVerfG) aus 2005, das in Bezug auf die „Technikoffenheit“ entschied, dass grundsätzlich gewisse kriminaltechnische Neuerungen in den Anwendungsbereich bestehender Regelungen einbezogen werden können.³ Anders Teile der juristischen und wissenschaftlichen Verbände: Sie argumentieren, dass die automatisierte Bildauswertung gegenüber deren Erhebung eine zusätzliche und ganz erhebliche grundrechtsrelevante Einschränkung in das Recht auf informationelle Selbstbestimmung darstelle, für die eine eigene Rechtsgrundlage erforderlich sei.⁴ Dies folgt auch der Rechtsprechung des BVerfG zur automatisierten Kennzeichenerkennung.⁵

Auf dem Europäischen Polizeikongress in Berlin im Februar 2020 stand der Einsatz von Künstlicher Intelligenz (KI) im Blickpunkt der öffentlichen Sicherheitsdiskussion zwischen Wirtschaft, Politik und Sicherheitsbehörden. Nach Ansicht der verschiedensten Experten gibt es zurzeit noch keine verlässliche Technik. Ein exakter vollautomatisierter Abgleich der Daten kann aktuell nicht erreicht werden. Die tatsächliche Entscheidung über einen Treffer beruht vielmehr auf zuvor eingestellte Parameter, die einen Toleranzbereich bilden, in dem die Bildpunkte vom System als „gleich“ erkannt werden. Die Merkmale werden nicht auf Gleichheit, sondern nur auf „hinreichende Ähnlichkeit“ getestet. Dies hat zur Folge, dass algorithmenbezogene Systeme die detektierte Szene nur mit einer systemtypischen Wahrscheinlichkeit bestimmen können und eine menschliche Verifizierung auch weiterhin notwendig macht.

Bei der korrekten Einführung einer intelligenten Videoüberwachung geht es nicht nur um das „Wie“, sondern auch um das „Ob“. Die Möglichkeit, Personen - so sie bereits polizeilich gespeichert sind - anhand ihrer verhaltensbezogenen Merkmale automatisiert identifizieren zu können, wäre damit verbunden, dass sich betroffene Personen nicht mehr im bisherigen Umfang anonym in der Öffentlichkeit bewegen könnten. Daneben besteht das Risiko, dass gesellschaftliche Gruppen aufgrund sozialer oder kultureller Vorurteile automatisiert sozial sortiert und überwacht werden. Insofern ist auch die Diskussion vor dem Hintergrund des Artikels 1 Abs. 1 GG - der Menschenwürde - auf eine breite Beteiligung der Öffentlichkeit zugeschnitten. Hierzu hat die EU-Kommission bereits im April 2019 Ethikleitlinien für eine „vertrauenswürdige Künstliche Intelligenz“ vorgestellt. In sieben Voraussetzungen werden die Kernanforderungen beschrieben. Dazu gehören neben Beachtung der geltenden Gesetze und des gesellschaftlichen Wohlergehens insbesondere auch die „Robustheit und Sicherheit“. „Eine vertrauenswürdige künstliche Intelligenz setzt Algorithmen voraus, die sicher, verlässlich und robust genug sind, um Fehler oder Unstimmigkeiten in allen Phasen des Lebenszyklus des Systems künstlicher Intelligenz zu bewältigen.“⁶ Neben der Definierung der ethischen Grenzen erweiterte die EU-Kommission ihren Regulierungsrahmen am 19.02.2020 um ein Weißbuch zur KI.⁷ Demzufolge erachtet die EU-Kommission die algorithmenbasierte Erkennung zum Zwecke einer biometrischen Fernidentifikation als eine für die Privatsphäre besonders risikoträchtige Technologie, an die besondere, noch zu spezifizierende Anforderungen gerichtet werden müs-

³ vgl. BVerfGE v. 12.04.2005 – 2 BvR 581/01, Rn. 51.

⁴ vgl. Stellungnahme des Deutschen Anwaltvereins zur sog. intelligenten Videoüberwachung, Nr. 47/2017, S. 5; ebenso die Wissenschaftlichen Dienste des Deutschen Bundestages, Sachstand WD 3 – 3000 – 202/16, S. 3.

⁵ vgl. BVerfGE v. 18.12.2018 - 1 BvR 142/15.

⁶ https://ec.europa.eu/commission/news/artificial-intelligence-2019-apr-08_de (Stand: 31.01.2020).

⁷ https://ec.europa.eu/info/files/white-paper-artificial-intelligence-european-approach-excellence-and-trust_de (Stand: 25.02.2020).

sen. Generell empfiehlt die EU-Kommission: „In Fällen mit hohem Risiko, z. B. in den Bereichen (...) Polizei oder Verkehr, sollten KI-Systeme transparent und rückverfolgbar sein. Die Aufsicht durch den Menschen muss stets gewährleistet sein. Behörden sollten die von Algorithmen genutzten Daten ebenso prüfen und zertifizieren können (...).“⁸ Das BMI hat zunächst von dem Vorhaben, die biometriebasierte forensische Personenerkennung an 134 Bahnhöfen und 14 Flughäfen in Deutschland einführen zu wollen, Abstand genommen.

Dies vorausgeschickt, wird zu den Nummern 1 a bis e, 2 und 4 der Landtagsentschließung Folgendes ausgeführt:

Zu 1 a:

Durch das Ministerium für Inneres und Sport (MI) wurde im November 2019 eine Bund-Länder-Umfrage zur videobasierten Situations- und Gegenstandserkennung durchgeführt. Im Ergebnis gibt es bundesweit nur wenige Vorhaben und spezifische gesetzliche Regelungen zum Einsatz einer algorithmenbasierenden Videobeobachtung.

Projekte

Auf Grundlage einer bestehenden Ordnungspartnerschaft (public private partnership) betreiben die Bundespolizei (BPOL) und die Securityorganisation der Deutschen Bahn AG (DB) ein Projekt zur Untersuchung einer intelligenten Videoanalyse am Bahnhof Berlin Südkreuz. In diesem Vorhaben soll eristet werden, inwieweit intelligente Videosysteme einen Mehrwert für die hoheitliche Aufgabenwahrnehmung der BPOL und der unternehmerischen Sicherheitsvorsorge der DB darstellen können. Im Juni 2019 begann die Erprobung für die Behandlung und Auswertung verschiedener Gefahrenszenarien. Hierzu zählen das

- Erkennen liegender Personen (z. B. hilfsbedürftige Person), die zuvor stehend oder aus der Bewegung plötzlich am Boden liegen,
- Erkennen beim Betreten definierter Bereiche z. B. Baustellen, Parkhäuser, Treppenhäuser, Zugänge für Lieferanten,
- Erkennen schneller Bewegungen / Fluchtverhalten (z. B. plötzliches Auseinanderlaufen oder schnelles Verlassen von Gruppen durch eine Tür),
- Erkennen von Personenströmen am Bahnhof zur Optimierung der Bebauung,
- Zählen von Personen, die sich in einem definierten Bereich aufhalten,
- Erkennen abgestellter Gegenstände, welche sich über einen längeren Zeitraum am gleichen Ort befinden,
- Erkennen abgestellter Gegenstände und Zugehörigkeit eines Gegenstandes zu einer Person (um z. B. Sperrungen von Bahnhöfen zu vermeiden),
- Nachvollziehen der Positionen von Personen im Bahnhof (um z. B. Besitzer der Gegenstände aufzufinden),
- Auswertung aufgezeichneter Videodaten anhand programmierbarer Parameter.

Ziele des Tests waren

- Die Feststellung einer Marktverfügbarkeit von Videofunktionalitäten (Software) zum mittelfristigen Einsatz in den Lagezentren unter Einbeziehung dreier Anbieter.
- Die Software soll dabei die Mitarbeiter der DB / Beamten der BPOL bei der passiven Live-Videoüberwachung unterstützen.
- Die Tests der Analysesoftware müssen anhand der planmäßigen Videoausstattung des Sicherheitsbahnhofs durch die DB und BPOL erfolgen.

⁸ https://ec.europa.eu/germany/news/20200219digitale-zukunft-europas-eu-kommission-stellt-strategien-fuer-daten-und-kuenstliche-intelligenz_de (Stand: 26.02.2020).

Zum derzeitigen Zeitpunkt wertet die beteiligte Universität die erlangten Fallzahlen aus. Mit einem Abschlussbericht ist in der zweiten Jahreshälfte 2020 zu rechnen. Seitens der BPOL gibt es derzeit bereits erste Überlegungen, zusammen mit der DB ein weiteres, darauf aufbauendes Forschungsprojekt zu initiieren, um die gewonnenen Erkenntnisse noch konkreter auf die polizeilichen Bedürfnisse anpassen zu können. Dies wird jedoch nicht vor dem Abschlussbericht und dem Vorliegen von validen Zahlen erfolgen.

Baden-Württemberg

In Mannheim testet die Stadtverwaltung mit dem örtlichen Polizeipräsidium an vier Kriminalitätsbrennpunkten mit insgesamt 76 installierten Kameras in der Innenstadt das automatisierte Erkennen von bestimmten, strafrechtlich relevanten Verhaltensmustern. Das im Dezember 2018 begonnene Projekt „Mannheimer Weg 2.0“ stellt eine Erweiterung der bereits bestehenden konventionellen Videoüberwachung dar. Der „Mannheimer Weg“ zeichnet sich im Grundsatz dadurch aus, dass der Fokus nicht auf der reinen Aufzeichnung von Daten und im Bedarfsfall deren retrograden Auswertung liegt. Vielmehr wird das aktuelle Geschehen durch Polizeibeamtinnen und Polizeibeamte in der Leitstelle live beobachtet. Bei entsprechenden Feststellungen lösen diese Operator unmittelbar eine Intervention oder Hilfeleistung aus. In der Version „2.0“ wird nunmehr der innovative Ansatz der algorithmenbasierten Bildauswertung zur Anwendung kommen. Damit soll auch in einem großen Kameranetzwerk gewährleistet werden, dass die Operator auf polizeilich relevante Sachverhalte hingewiesen werden, um unverzüglich die notwendigen Maßnahmen einleiten zu können.

Insgesamt investieren die Stadt Mannheim und das Land Baden-Württemberg ca. 1,6 Millionen Euro. Die Pilotierung ist auf eine Laufzeit von fünf Jahren angelegt und wird technisch durch das Fraunhofer Institut für Optronik, Systemauswertung und Bildtechnik begleitet. Grundlage der eingesetzten Technologie bietet eine bereits bestehende Software, die bislang nur unter Laborbedingungen angewandt und nun mit relevanten Echtdateien trainingsbasiert und durch selbstständiges Maschinelernen weiterentwickelt wird.

Die Projektziele sind

- das Erkennen von Personen und Objekten,
- das Erkennen grobmotorischer Angriffe. Darunter werden aktuell die vier möglichen Szenarien Treten, Schlagen, Würgen und Kollabieren erfasst.

Im aktuellen Entwicklungsstand werden Personen zuverlässig erkannt und getrackt sowie zusätzlich deren Haltung eingeschätzt. Die Qualität ist dabei vergleichbar mit den frei verfügbaren Open-Source-Lösungen, wie sie im Projekt „Weiterentwicklung der polizeilichen Analyse“ des LKA NI in der Entwicklung verwendet werden. Entgegen der Planung aus August 2019, auch feinmotorische Bewegungsmuster wie beispielsweise Taschendiebstahl erkennen zu können, werden solche Szenen nicht mehr weiter berücksichtigt. Angriffe können aktuell nicht mit hinreichender Genauigkeit erkannt werden.

Gesetzliche Regelungen

Aktuell gibt es bundesweit nur wenige spezifische Rechtsgrundlagen für den Einsatz technischer Mittel zur algorithmenbasierten Situations- und Objekterkennung mittels Videoüberwachung im öffentlichen Raum für Gefahrenabwehrzwecke. Beispiele hierfür sind Bayern, das eine Rechtsgrundlage für die algorithmenbasierte Objekterkennung vorsieht, und Baden-Württemberg, das eine Rechtsgrundlage für algorithmenbasierte Verhaltensmustererkennung enthält, die Objekterkennung aber unabhängig von einer spezifischen Rechtsgrundlage für zulässig erachtet.

Nahezu alle Bundesländer haben jedoch zurückgemeldet, dass sie eine spezifische Rechtsgrundlage im Gesetz zumindest für die algorithmenbasierte Verhaltenskontrolle aus rechtlichen Erwägungen für erforderlich erachten würden, wenn eine solche Maßnahme auf Landesebene umgesetzt werden sollte.

Hiervon abzugrenzen sind die Regelungen zur Automatischen Kennzeichenlesekontrolle, die zwar das Kfz-Kennzeichen als besonderes Objekt erkennen und die dort enthaltenen Daten auswerten, dies ist aber nicht Gegenstand dieses Entschließungsantrages und bleibt daher unberücksichtigt. Ebenso bleiben die Regelungen aus Rheinland-Pfalz (§ 37 Abs. 3 POG RP) oder Sachsen

(§ 59 SächsPVDG) unberücksichtigt, die einen automatisierten Abgleich von erhobenen Bildaufzeichnungsdaten mit Fahndungsdateien von Personen ermöglichen.

Einen umfassenden Überblick über den Wortlaut der derzeit vorhandenen spezifischen gesetzlichen Regelungen zur algorithmenbasierten Verhaltens- und Objekterkennung vermittelt die **Anlage**.

Bund

Das Bundesministerium des Innern, für Bau und Heimat (BMI) vertritt die Auffassung, dass die Ermächtigung zur Objekt- und Verhaltensmustererkennung in der Grundnorm zu deren Norm zur Videoüberwachung enthalten ist. Im Rahmen des Einsatzes der selbsttätigen Bildaufnahme- und Bildaufzeichnungsgeräte zum Zwecke des Objektschutzes führt das BMI weiter aus, dass die algorithmenbasierte Auswertung, sofern sie nicht auf die Verarbeitung biometrischer Daten beruhe, im § 27 S. 1 BPolG enthalten sei.

Für die freiwilligen Testpersonen gab es als ergänzende Rechtsgrundlage die §§ 4, 4 a Bundesdatenschutzgesetz (BDSG). Für den Test wurde ein Datenschutzkonzept erarbeitet, das umfassende Hinweise auf den Test, leichte Ausweichmöglichkeiten für übrige Bahnreisende und weitreichende Löschpflichten für die aufgezeichneten Daten beinhaltet.

Baden-Württemberg

Als Rechtsgrundlage für die algorithmenbasierte Verhaltensmustererkennung bietet seit Dezember 2017 der § 21 Abs. 4 PolG BW dem Polizeivollzugsdienst die Möglichkeit einer automatisierten Bildauswertung. Gesetzliche Voraussetzung für den Abgleich ist lediglich, dass nur solche Verhaltensmuster abgeglichen werden, die auf die Begehung einer Straftat hindeuten. Systematisch setzt die Norm auf der Videobilddatenerhebung auf und rechtfertigt den nachgelagerten, algorithmenbasierten Datenabgleich mit hinterlegten Verhaltensmustern. Grundvoraussetzung ist eine gefahrenabwehrrechtliche Videodatenerhebung, die sich auf Kriminalitätsschwerpunkte bezieht sowie Orte bzw. Veranstaltungen mit Gefährdungsrisiko.

Bayern

Im Polizeiaufgabengesetz (PAG) wird der bayerischen Polizei in Artikel 33 Abs. 5 die Verwendung von Systemen zur automatischen Erkennung und Auswertung von Mustern bezogen auf Gegenstände einschließlich der automatischen Systemsteuerung erlaubt. Wie auch in Baden-Württemberg ist die Norm systematisch als eine der Videobilddatenerhebung nachgelagerte Norm für den Bereich der Datennutzung ausgestaltet. Materiell-rechtlich enthält die Norm lediglich die Einschränkung, dass der Abgleich vor dem Hintergrund der jeweiligen Gefahrenlage aufgrund entsprechender Erkenntnisse erforderlich sein muss.

Konkrete Vorhaben oder Projekte, die sich auf diese Ermächtigung beziehen, wurden der Landespolizei Niedersachsen im Rahmen der durchgeführten Bund-Länder-Umfrage jedoch nicht berichtet.

Zu 1 b:

Im Kontext der Vielzahl von sicherheitspolitischen und kriminalistischen Herausforderungen kann die gezielte polizeiliche Videobeobachtung ein wirksames, unterstützendes Mittel zur Steigerung der objektiven und subjektiven Sicherheit der Bevölkerung sein. Eine softwarebasierte Liveauswertung könnte in diesem Zusammenhang die Effizienz der Videobeobachtung steigern. Insofern erscheint es folgerichtig, die sicherheitspolitischen Aspekte und Potenziale der KI im Sinne einer gesamtstaatlichen Sicherheitsvorsorge zu diskutieren. Diese muss jedoch auch immer unter Abwägung von Grundrechtseingriffen erfolgen.

Zum sicherheitspolitischen Ziel einer automatisierten polizeilichen Videobeobachtung im sozialen Raum gehört es, das Sicherheitsgefühl in der Bevölkerung auf öffentlichen Straßen oder Plätzen oder an anderen öffentlich zugänglichen Orten zu erhöhen und Straftaten zu verhindern bzw. deren Aufklärung zu erleichtern. Durch eine automatisierte Videoanalyse wird die Polizei schneller als mit herkömmlichen Mitteln auf bestimmte Bewegungs- und Situationsmuster, die auf besondere Kriminalitätsformen und herausgehobene Gefährdungssituationen hindeuten, hingewiesen. Eine tech-

nisch gestützte Liveauswertung der auf den Monitoren angezeigten Videodaten bietet den Vorteil, dass nach automatisierter Detektion eines sicherheitsrelevanten Ereignisses polizeiliche Kräfte sofort alarmiert werden und gezielt reagieren können, sodass am Einsatzort Täter schneller aufgegriffen und ermittelt sowie Opfer geschützt und hilfsbedürftige Personen unterstützt werden. Dadurch verkürzt sich grundsätzlich die Interventionszeit. Gleichzeitig erhöht sich die Eigensicherung der eingesetzten Kräfte, da der Operator durch die Beobachtung eine sich verändernde Lage unmittelbar erkennt und aktuelle Informationen weitergeben kann.

Der Einsatz einer polizeilichen Videoüberwachung kann eine generalpräventive Wirkung entfalten, wobei entscheidend ist, dass sie offen ausgeführt wird und Fahndungserfolge sowie Tataufklärungen ins Bewusstsein der Bevölkerung gelangen. Besondere Einsatzlagen, abgewehrte Gefahren, Festnahmen und in deren Folge Tataufklärungen können durch eine begleitende Öffentlichkeitsarbeit für ein gesteigertes Bewusstsein sorgen sowie zu einer erhöhten Akzeptanz in der Bevölkerung beitragen. Mithilfe einer frühzeitigen intelligenten Erkennung von potenziell strafbaren Verhaltensmustern sollen Tatgelegenheiten reduziert und das Entdeckungsrisiko für den Täter erhöht werden. In der Folge können aufgrund der Stärkung des individuellen Sicherheitsgefühls auch Angstorte wieder stärker frequentiert werden.

Als Ergebnis der Beteiligung aller niedersächsischen Polizeibehörden erscheinen aus polizeifachlicher Sicht verschiedene Anwendungsfälle für eine im Livemonitoring betriebene automatisierte optisch-elektronische Beobachtung auf öffentlichen Straßen und Plätzen sowie an anderen öffentlich zugänglichen Orten denk- und perspektivisch auch umsetzbar zu sein. Vorzugsweise orientiert sich die polizeiliche Videobeobachtung an Kriminalitätsbrennpunkten, an (potenziell) gefährdeten Orten sowie bei Veranstaltungslagen und im öffentlichen Personennahverkehr. Als denkbare Fallkonstellationen kommen insbesondere folgende Situations- und Gegenstandsmuster in Betracht:

Sich entwickelnde Gewalthandlungen:

- Schlagen,
- Treten,
- Würgen,
- Entreißen.

Veränderungen im Aktionsmuster:

- Stürzen,
- Kollabieren,
- länger liegende Personen,
- Rennen / Flüchten,
- zügiges Auseinanderströmen.

Unerwünschte Objekte:

- Waffen (Messer, Schusswaffen),
- abgestellte Taschen (Koffer, Rucksack),
- sich bewegende Fahrzeuge in einem definierten Umfeld,
- atypisch schnellfahrende Fahrzeuge in einem definierten Umfeld.

Zu 1 c:

Verfassungsrechtlicher Rahmen

Im Unterschied zur konventionellen Art der Videobeobachtung, die sich in der Erhebung der digitalisierten Videobilddaten und anschließend manuellen Auswertung erschöpft, erfolgt die Auswertung der Daten bei der algorithmenbasierten Videodatenverarbeitung durch einen schematisch festge-

legten Rechenvorgang. Insofern mit der Maßnahme der algorithmenbasierten Videodatenauswertung ein Personenbezug herstellbar ist, liegt nach § 24 Nr. 1 und 2 Niedersächsisches Datenschutzgesetz (NDSG) eine Erhebung personenbezogener Daten und damit ein Eingriff in das informationelle Selbstbestimmungsrecht nach Artikel 2 Abs. 1 in Verbindung mit Artikel 1 Abs. 1 GG vor.

Mit der algorithmenbasierten Videodatenauswertung werden die erhobenen Informationen mit bereits bekannten Mustern oder hinterlegten bzw. errechneten Durchschnittsmustern abgeglichen. Diese Automatisierung erlaubt eine höhere Intensität der Datenauswertung, sowohl hinsichtlich des möglichen Umfangs des Datenbestands als auch hinsichtlich des zeitlichen Horizonts der Verfügbarkeit des Auswertungsergebnisses. Auch die technische Auswertungsqualität kann durch Verknüpfungsmöglichkeiten und digitale Abgleichmöglichkeiten gesteigert werden. Das Bundesverfassungsgericht sieht in einer automatisierten Datenverarbeitung daher eine eigenständig zu beurteilende Erhöhung der Eingriffsintensität.⁹ Wegen der damit verbundenen zusätzlichen Einschüchterungseffekte und der hohen Streubreite der Maßnahme, ist es gerechtfertigt, auch unabhängig von dem Auswertungsergebnis eine zusätzliche Eingriffsqualität allein durch den Umstand der Automatisierung der Auswertung zu bejahen.¹⁰ Zwar dient die Maßnahme in Form der Verhaltensmustererkennung der Zielrichtung nach dazu, Daten von rechtstreuen Dritten herauszufiltern, gleichzeitig ist die Verarbeitung der Verhaltensdaten aber ein denkbare Zwischenschritt für den erforderlichen Abgleich mit Mustern. Auch hieran besteht für diesen Schritt der Auswertung und das verfolgte Ziel einer Alarmierung der Einsatzkräfte daher ein behördliches Interesse, was eingriffsauslösend wirkt.¹¹

Durch die Automatisierung können technisch auch viel leichter und schneller Muster miteinander abgeglichen werden, die den menschlichen Augen so nicht erkennbar wären. Insofern können zusätzliche Informationen generiert werden und der Überwachungsdruck wird erhöht. Auch dies spricht für eine zusätzliche Eingriffsqualität und ein zusätzliches Eingriffsgewicht. Darüber hinaus gibt es ein Risiko, dass Muster rechnerisch fehlinterpretiert werden, was nachteilige Anschlussmaßnahmen der Polizei nach sich ziehen kann. Auch insofern erhöht sich daher die Eingriffsqualität einer solchen Maßnahme.

Demgegenüber steht die Aufgabe des Staats, Gefahren der öffentlichen Sicherheit sowie Straftaten zu verhindern. Auch dieser Aufgabe kommt eine hohe verfassungsrechtliche Bedeutung zu,¹² so dass der Einsatz einer algorithmenbasierten Videodatenauswertung trotz des hohen Gewichts einer flächendeckenden Auswertung von Videobilddaten nicht generell ausgeschlossen ist. Maßnahmenanlass und Maßnahmenziel müssen im Verhältnis zum Eingriffsgewicht aber in einem verhältnismäßigen Ausgleich stehen.

Objekterkennung

Die Objekterkennung, die lediglich das Erkennen von Objekten betrifft, ohne personenbezogene Maßnahmen hieran anzuknüpfen, weist in dieser schlichten Zielrichtung gerade keinen Personenbezug auf. Erkennt der Algorithmus einen gefährlichen Gegenstand und schlägt Alarm, so ist im Anschluss zwar regelmäßig auch eine Identifizierung der Besitzerin oder des Besitzers möglich, sofern die Videoaufnahmen gemäß § 32 Abs. 3 NPOG auch rechtmäßig aufgezeichnet wurden. Dies ist aber nicht Teil des Abgleichs im Rahmen der Objekterkennung. Bei der Identifizierung im Anschluss an die Objekterkennung handelt es sich jedoch um einen weiteren Eingriff auf der Grundlage von §§ 38, 39 NPOG i. V. m. § 32 Abs. 1 bis 3 NPOG.

⁹ BVerfGE 120, 378, 406.

¹⁰ Vgl. auch Held, Intelligente Videoüberwachung, S. 111. Dies wird zusätzlich untermauert durch die Rechtsprechung des Bundesverfassungsgerichts zum automatisierten Kennzeichenabgleich, wonach selbst bei Nichttrefferfällen bei automatisierter Datenverarbeitung einen Eingriff bejaht wurde (BVerfGE 150, 244ff.).

¹¹ BVerfGE 115, 320, 342: „Auch dann, wenn die Erfassung eines größeren Datenbestandes letztlich nur Mittel zum Zweck für eine weitere Verkleinerung der Treffermenge bildet, kann in der Datenerhebung bereits ein Eingriff liegen [...]. Maßgeblich ist, ob sich bei einer Gesamtbetrachtung mit Blick auf den durch den Überwachungs- und Verwendungszweck bestimmten Zusammenhang das behördliche Interesse an den betroffenen Daten bereits derart verdichtet, dass ein Betroffensein in einer einen Grundrechtseingriff auslösenden Qualität zu bejahen ist.“ Vgl. auch Held, Intelligente Videoüberwachung, S. 112.

¹² BVerfGE 100, 313, 387f..

Bei der Erfassung von Bildpunkten von Objekten und deren Abgleich mit Objektmustern handelt es sich gerade nicht um eine Verarbeitung personenbezogener Daten. Ein Grundrechtseingriff liegt danach nicht vor, sodass die Schaffung einer Rechtsgrundlage zum Zwecke dieser allein auf die Objekterkennung zielenden Videoauswertung nicht erforderlich ist. Zu diesem Ergebnis ist auch der Gesetzgeber des Landes Baden-Württemberg gekommen. Wie oben dargestellt sieht die baden-württembergische Regelung zur automatisierten Videodatenauswertung in § 21 Abs. 4 PolG keine spezifische Rechtsgrundlage für die Objekterkennung vor, obschon ausweislich der Gesetzesbegründung davon ausgegangen wird, dass zumindest ortsfeste Objekte ebenfalls in die algorithmenbasierte Videodatenauswertung einbezogen werden sollten.¹³

Auch wenn eine gesetzliche Regelung nach dem Vorstehenden nicht erforderlich ist, erscheint es aus Gründen der Normenklarheit jedoch allgemein empfehlenswert, für die Objekterkennung ohne Personenbezug wie in Bayern (Artikel 33 Abs. 5 PAG) eine klarstellende Norm in das Gesetz aufzunehmen, ohne hierfür besondere verfahrensrechtliche oder materiellrechtliche Schwellen vorzusehen.

Situations- und Verhaltensmustererkennung

Die automatisierte algorithmenbasierte Erkennung gefährlicher Situationen und Verhaltensweisen knüpft im Unterschied zur Objekterkennung unmittelbar an menschliche Verhaltensweisen an und zielt darauf ab, diese menschlichen Verhaltensweisen auszuwerten. Selbst wenn die Verhaltensmustererkennung in diesem Fall lediglich die Bildpunkte selbst verarbeitet, haben diese jedoch ihre Ursache unmittelbar in menschlichem Verhalten und sollen auch mit dem Ziel einer späteren Personenbeziehbarkeit ausgewertet werden. Darüber hinaus ist der Personenbezug der Bildpunkte ohne weiteren Zwischenschritt unmittelbar herzustellen. Es ist daher von einer Verarbeitung personenbezogener Daten auszugehen.

Die automatisierte Auswertung der Daten stellt einen gewichtigen Eingriff in das Recht auf informationelle Selbstbestimmung dar, der nicht allein auf die allgemeine Rechtsgrundlage der Videobeobachtung/Videoaufzeichnung und Auswertung nach § 32 Abs. 1 bis 3 NPOG und §§ 38, 39 NPOG gestützt werden kann. Grund hierfür ist, dass die Erkennung von Aktionsmustern wie etwa Schlagen oder Treten dazu geeignet ist, einen zusätzlichen Anpassungsdruck der menschlichen Verhaltensweisen zu erzeugen. Insofern wäre in Niedersachsen eine spezifische Rechtsgrundlage für die Verhaltensmustererkennung erforderlich. Eine spezifische Vorschrift zur automatisierten Erkennung von Verhaltensweisen ist bisher - wie oben dargestellt - ausschließlich in Baden-Württemberg mit § 21 Abs. 4 PolG BW eingeführt worden.

In der Rechtsgrundlage zur Situations- und Verhaltensmustererkennung müssten Anlass, Zweck und Grenzen des Eingriffs bei der automatisierten Bildauswertung zur Verhaltensmustererkennung hinreichend bereichsspezifisch geregelt sein, damit sich die betroffenen Bürgerinnen und Bürger auf die möglichen belastenden Maßnahmen einstellen können. Insbesondere das Maßnahmeziel, das auch den Grundrechtseingriff rechtfertigt, muss in der Rechtsgrundlage festgelegt werden. Die Verhütung von Straftaten ist ein legitimes Ziel, das ähnlich wie in der baden-württembergischen Regelung, in der Rechtsnorm verankert werden könnte. Zur Klarstellung sollte darüber hinaus die automatisierte Auswertung anhand biometrischer Merkmale explizit ausgeschlossen werden.

Weitere datenschutzrechtliche Rahmenbedingungen

Da das technologische Verfahren zur Verhaltensmustererkennung zumindest im Ausgangspunkt Videobilddaten von Personen zum Gegenstand hat und damit auf personenbeziehbare Daten aufsetzt, ist vom Verfahren her zu berücksichtigen, dass diesbezüglich eine Datenschutzfolgeabschätzung nach § 39 NDSG vorzunehmen ist, und eine Anhörung der Landesbeauftragten für den Datenschutz (LfD) nach § 40 NDSG vorher abzuschließen ist. Wegen der zur Implementierung der algorithmenbasierten Videodatenauswertung erforderlichen neuen Technologien hat es mit der LfD bereits erste konkrete Gespräche gegeben. Auch bedarf die Konfiguration der Algorithmen, die die Datenverarbeitung bestimmen, und deren Fortentwicklung durch das beabsichtigte Maschinenlernen ebenso wie die Übertragungswege, die Speicherparameter sowie die begleitende polizeiliche

¹³ vgl. LT-Drucksache BW 16/2741, S. 28.

Handlungskonzeption einer transparenten Dokumentation, um eine externe Kontrolle zu ermöglichen.

Zu 1 d:

Die in den Polizeidirektionen eingesetzten Videoüberwachungssysteme sind quantitativ und qualitativ aktualisiert erhoben. In den regionalen Polizeibehörden befinden sich im Rahmen vorhandener gesetzlicher Ermächtigungen an 59 Standorten insgesamt 181 polizeilich genutzte konventionelle Kamerasysteme im Einsatz, wovon das Gros in der Landeshauptstadt Hannover verortet ist. Weitere 23 Einheiten werden in der Zentralen Polizeidirektion Niedersachsen (ZPD NI) als Servicekomponenten für die Flächendienststellen vorgehalten. Über 60 % (126) dieser Bildbeobachtungseinheiten dienen der Begleitung von Veranstaltungslagen, davon vorrangig im Zusammenhang mit Fußballspielen.¹⁴

Die technischen Standards unterscheiden sich landesweit im Hinblick auf die Leistungsmerkmale der Kameras, der Übertragungswege als auch der Speicherung und Auswertung der Rohdaten. Zudem sind sie vielfach veraltet. Auf Basis der vorliegenden Berichte erscheint die vorhandene Technik für das Vorhaben nicht geeignet zu sein. Vor dem Hintergrund, dass Systeme in dieser Kombination in Niedersachsen bislang nicht im unmittelbaren Fokus standen, bedarf es zunächst der Erarbeitung eines Fachkonzepts zur Ermittlung der konkreten fachlichen Anforderungen sowie der technischen und monetären Aspekte im Rahmen einer überbehördlichen Befassung. Nach Bewertung der ZPD NI wird dieses mindestens zwölf Monate in Anspruch nehmen. Erst dann können auch valide Aussagen zu den erforderlichen Haushaltsmitteln getroffen werden. Bei den zu erwartenden hohen Kosten ist nach dem Prinzip „Sicherheit durch Kooperation“ grundsätzlich auch immer eine Beteiligung der originär zuständigen Gefahrenabwehrbehörden zu prüfen.

Zu 1 e:

Die polizeiliche Videoüberwachung des öffentlichen Raums ist ein geeignetes Mittel zur frühzeitigen Erkennung von Gefahren und zur Aufklärung von Straftaten. Dabei soll die Technik die Polizeibeamtinnen und Polizeibeamten bei ihrer Tätigkeit unterstützen, nicht ersetzen. Gleichwohl lässt sich bei näherer Betrachtung auch hier ein Spannungsfeld zwischen Freiheit und Sicherheit erkennen. Einerseits gilt, dass eine flächendeckende Überwachung durch eine Vielzahl von Kameras nicht erforderlich ist, sondern eine sorgfältige, am geltenden Recht und der aktuellen Lage orientierte Auswahl der Kamerastandorte zu erfolgen hat. Andererseits müsste jedoch aus objektiv und subjektiv sicherheitsrelevanten Aspekten gerade an solchen (Angst-)Orten eine intelligente Echtzeitbeobachtung installiert sein, die aufgrund taktischer und personeller Gegebenheiten grundsätzlich nachrangig betrachtet werden.

Ein Einsatz von Videotechnik mit automatisierter Situations- und Gegenstandserkennung an derartigen Kriminalitätsbrennpunkten ermöglicht die Freisetzung personeller und zeitlicher Ressourcen. So kann der häufige Einsatz von u. a. Polizeibeamtinnen und Polizeibeamten des Streifendienstes, oftmals sowohl mit Einbindung der Kontaktbereichsbeamtinnen und Kontaktbereichsbeamten als auch der Bereitschaftspolizei, reduziert und die frei werdenden Ressourcen für eine anderweitige höhere Polizeipräsenz und Präventionseinsätze genutzt werden. Eine positive Wirkung, auch im Rahmen einer Kosten-Nutzen-Analyse, kann nur mit einer ausgereiften Technik erzielt werden. Wiederholt fehlerhafte Alarmierungen können dabei zu einer verringerten Akzeptanz sowie einer erhöhten Einsatzbelastung führen. Darüber hinaus ist bei der Zusammenschaltung der genutzten Videotechnik, beispielsweise in den Leitstellen, Personal für eine Beobachtung der Übertragungsbilder, spätestens aber bei einer entsprechenden Detektion zur Alarmierung von Einsatzkräften und Übermittlung wesentlicher Informationen, notwendig. Die intelligente Technik sorgt aber dafür, dass nicht ständig eine Vielzahl von Monitoren betrachtet werden müssen, sondern nur nach einer Detektion durch eine Polizeibeamtin oder einen Polizeibeamten das Ergebnis verifiziert werden muss, um dann die notwendigen Maßnahmen einzuleiten.

Angesichts der noch zu leistenden technischen Entwicklungsarbeit, der hohen zu erwartenden Investitions- und Unterhaltungskosten, der fehlenden Rechtsgrundlage für die Verhaltensmustererkennung sowie der gesellschaftspolitischen Bedeutung könnte die objektive Wirkung einer

¹⁴ Stand: 05.11.2019.

KI-basierten Videobeobachtung zunächst im Rahmen einer genau abgestimmten Projektierung ermittelt werden. Um die verschiedenen Dimensionen der Wirkung polizeilicher Videoüberwachung sach- und fachgerecht abbilden zu können, sollte ein Untersuchungszeitraum von mindestens zwei Jahren veranschlagt werden. Bei der Auswahl möglicher Projekte gilt es eine Reihe von Erwägungen zu berücksichtigen. Hierzu gehören neben den wirtschaftlichen Aspekten und rechtlichen Voraussetzungen auch die Schwierigkeit der Implementierung, Erfolgswahrscheinlichkeit und nicht minder wichtig zu treffende Vereinbarungen mit Stakeholdern bzw. Kooperationspartnern.

Für die Generierung von automatisierten Mustererkennungsverfahren sind verschiedene strafrechtlich relevante Verhaltensweisen vorstellbar. Hierzu zählen vorrangig Eigentumsvergehen, Gewalt- und Straßekriminalität, aber auch beispielsweise sexuell motivierte Delikte im Zusammenhang mit Veranstaltungen bzw. dem Auftreten von Menschenmassen. Daneben kommen auch potenziell nicht strafbare Verhaltensmuster wie das Erkennen von hilfsbedürftigen Menschen, z. B. Kinder ohne Begleitpersonen, Verunfallte oder Betrunkene, sowie abgestellte Gegenstände als Testszenarien in Betracht.

Ein etwaiges Projektvorhaben wäre an einem Standort durchzuführen, der sowohl über eine herausgehobene Kriminalitätsbelastung verfügt als auch eine erforderliche Raumstruktur aufweist.

Unter Berücksichtigung aller Charakteristika zeichnet sich die Bekämpfung der Straßekriminalität als primär geeignetes Einsatzgebiet zur Erprobung der Leistungsfähigkeit einer auf Algorithmen basierenden automatischen Videobeobachtung ab.

Zu 2:

Die Landesregierung betreibt bereits seit Jahren für die offene, präventive Videoüberwachung öffentlicher Räume zur Stärkung der Bürgerrechte und Transparenz ein öffentlich einsehbares „Anlagenkataster“. Hierauf gab es in der Vergangenheit vonseiten der Öffentlichkeit kaum Nachfragen für den polizeilichen Fachbereich. Dieses dürfte sich jedoch perspektivisch ändern, da das Vorhaben aufgrund der Eingriffsintensität in der Gesellschaft nicht unumstritten ist und eine unmittelbare Auswirkung auf das individuelle Lebensumfeld und den öffentlichen Alltag nach sich zieht.

Die Akzeptanz der Öffentlichkeit wird wesentlich von der Transparenz abhängig sein, was eine intelligente Videobeobachtung überhaupt zu leisten imstande ist, wofür sie eingesetzt werden soll, und wie sich der Umgang mit den erhobenen persönlichen Daten gestaltet. Um den hohen unterschiedlichen Ansprüchen von Bürgerinnen und Bürgern, Gewerbetreibenden sowie den Interessenvertretern von Verbänden, den Kommunen und dem Land gerecht zu werden, bedarf es einer intensiven und behutsamen Planung als auch der Bereitstellung ausreichender zeitlicher, personeller und finanzieller Ressourcen.

Angesichts der fehlenden rechtlichen Grundlage für die Verhaltensmustererkennung und der noch vielen offenen Fragen, insbesondere zu den technisch sicherzustellenden Anonymisierungsprozessen, den Übertragungswegen, Speicherparametern und den vielfältigen praktischen Anwendungsmöglichkeiten, erscheint eine so frühzeitige breite öffentliche Thematisierung nicht zielführend zu sein. Diese Ansicht wird von Vertretern der LfD geteilt. Zu einem späteren Zeitpunkt ist ein partizipatives Beteiligungsverfahren auf einer gesellschaftspolitischen Ebene für den Demokratieprozess allerdings unabdingbar. Dadurch bleibt zudem gewährleistet, dass die beabsichtigten Maßnahmen rechtzeitig überprüft und neue praxisnahe Vorschläge berücksichtigt werden können. Zur Steigerung der Akzeptanz für die politische Entscheidung sollte ein dialogorientiertes Beteiligungsformat Anwendung finden, das sich durch eine neutrale Moderation auszeichnet und Möglichkeiten zum aktiven Mitreden und Mitgestalten bietet. Vorstellbar wäre eine Mischung aus Präsenzveranstaltung mit Online-Beteiligung. Eine umfassende Öffentlichkeitsarbeit unter Nutzung alter und neuer Medien hat dabei den Vorteil, regelmäßig und aktuell zur Bekanntheit des Programms und Mitwirkung bei der öffentlichen Meinungsbildung beizutragen. Außerdem kann eine begleitende Medienberichterstattung von den Bürgerinnen und Bürgern als auch den Gewerbetreibenden als Indiz aufgefasst werden, dass deren Interessen von staatlicher Seite ernst genommen werden. Parallel zu einem niedersächsischen Pilotprojekt empfiehlt sich eine begleitende wissenschaftliche Forschungsstudie, die insbesondere Aussagen zur Akzeptanz, zur individuellen subjektiven Sicherheit sowie einer möglichen Verhaltensanpassung im Wissen um eine Videobeobachtung herleiten lässt.

Gesamtbetrachtend bleibt festzustellen, dass die Nutzung neuronaler Netze mit Mustererkennung aus polizeilicher Sicht grundsätzlich eine gewinnbringende Sicherheitstechnologie sein kann, um die kriminalpräventiven Potenziale der Videobildanalyse zu erhöhen. Auf der anderen Seite kann Technik aber auch keine Lösung für soziale Probleme sein, zumal die intelligente Videoüberwachung nicht bei den Ursachen ansetzt, sondern erst vermeintlich delinquentes Verhalten erkennt. Auch aus einem pragmatischen und ethischen Sinn heraus ist die anlassfreie Massendatenerhebung mit automatisierter Bewertung in Bezug auf unsere soziale Werteordnung fragwürdig. Als richtungsweisend für die Bildung ethischer Grenzen und verbindlicher einheitlicher Standards gilt das Weißbuch zur Künstlichen Intelligenz der EU-Kommission, das sich zurzeit noch in der öffentlichen Konsultation befindet.

Die Erfahrungen aus den Projekten „Sicherheitsbahnhof Berlin Südkreuz“ und „Mannheimer Weg 2.0“ zeigen, dass die Technik derzeit noch nicht in der Lage ist, die an sie gerichteten Anforderungen verlässlich zu erfüllen. Jedoch steht die Entwicklung algorithmenbasierender Technik erst am Anfang und ist noch nicht erschöpft. Es bleibt abzuwarten, ob mit zunehmender technischer Stabilität auch die Möglichkeiten für einen rechtskonformen Einsatz steigen und sich damit bessere Chancen für den Grundrechtsschutz ergeben. Die rechtlichen und gesellschaftlichen Auswirkungen lassen sich nicht abschätzen, und es bleibt bei einem mehrdimensionalen Spannungsfeld.

Losgelöst von einem notwendigen demokratischen Deliberationsverfahren wird angesichts der fehlenden rechtlichen Voraussetzungen und der zu erwartenden hohen Kosten für die Entwicklung und den Betrieb eines eigenen Projektvorhabens empfohlen, mit der Entscheidung über die Einführung einer intelligenten videobasierten Situations- bzw. Gegenstandserkennung noch abzuwarten und stattdessen die Entwicklung der intelligenten Systeme weiter zu beobachten, um die Möglichkeiten und Grenzen der Nutzung in polizeilicher Hinsicht, aber auch aus allgemeiner, technischer, rechtlicher und gesellschaftlicher Perspektive noch differenzierter bewerten zu können.

Zu 4:

Im Rahmen der Beratung zum Entwurf eines Reformgesetzes zur Änderung des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung und anderer Gesetze (NPOG) wurde von einer Aufnahme einer für die Einführung der intelligenten Videoüberwachung erforderliche Rechtsgrundlage abgesehen, da zunächst die Ergebnisse der bekannten Projekte abgewartet werden sollten. Die bisherigen Erkenntnisse zeigen, dass je nach technischer Ausgestaltung der algorithmenbasierten Videodatenauswertung und nach dem Umfang der Verarbeitung personenbezogener Daten jedoch bereits bei Durchführung eines Pilotprojektes zur Verhaltensmustererkennung eine rechtliche Regelung vorliegen muss, welche den technischen Einsatz der automatisierten Auswertung mit der Zielrichtung der Verhütung von Straftaten, aber auch der allgemeinen Gefahrenabwehr zum Inhalt hat. Die Verfolgung der in den Fachgremien und der Öffentlichkeit geführten Diskussionen zeigen, dass die Überwachung sozialer Räume immer noch ein viel diskutiertes, polarisierendes Thema ist. Die bekannten Projekte haben insoweit noch kein eindeutiges positives Ergebnis der Diskussionen gezeigt. Für Niedersachsen bleibt festzuhalten, dass ein Pilotprojekt voraussetzt, dass die technischen Systeme so ausgereift sind, dass möglichst wenig technische Fehlinterpretationen von Mustern zu erwarten sind. Eine breite konsensuale positive Beurteilung in der Gesellschaft setzt einen entsprechenden Diskurs über die Rahmenbedingungen einer solchen Maßnahme voraus. Dieser steht noch aus. Dieser Bericht gemeinsam mit dem nach Nummer 2 der Landtagsentschließung vorgesehenen öffentlichen Diskurs zur Einführung der Videotechnik mit den gesellschaftlichen Akteuren in Niedersachsen können die entscheidenden Rahmenbedingungen definieren, die für eine breite konsensuale Beurteilung eines solchen Pilotprojektes erforderlich sind. Eine flächendeckende, anlasslose Videoüberwachung erscheint vor dem Hintergrund der in diesem Bericht dargelegten verfassungsrechtlichen Erwägungen nicht durchführbar. Vor dem Hintergrund des Eingriffsgewichts der Verhaltensmustererkennung ist eine spezifische Rechtsgrundlage erforderlich, die die Einsatzbedingungen für die algorithmenbasierte Videodatenauswertung festlegt und entsprechend gewichtige formelle und/oder materielle Schwellen vorsieht. Relevante Faktoren für die Bestimmtheit der Norm können hierfür die Einsatzorte, die zeitliche Begrenzung der Videodatenauswertung, die Einsatzanlässe, die zu schützenden Rechtsgüter, Löschrufen und gegebenenfalls einzuhaltende Verfahrensschritte bei der Anordnung der Maßnahme sein. Auch für die Objekterkennung erscheint eine klarstellende Regelung zumindest wünschenswert, um transparent darzulegen, dass die Videodaten auch für diesen Zweck genutzt werden dürfen. Der unter Num-

mer 2. des Entschließungsantrags vorgesehene öffentliche Diskurs kann dazu dienen, einen breiten Konsens in der Beurteilung der algorithmenbasierten Videodatenauswertung insgesamt zu erzielen. Folglich ist es für die Entwicklung einer gesetzlichen Grundlage noch zu früh.

Anlage: Bundes- und landesgesetzliche Regelungen zur intelligenten Videoüberwachung

In der Anlage werden die im Bund und in den Ländern vorhandenen spezifischen Bestimmungen und sonst relevanten gesetzlichen Regelungen mit Relevanz für den Bericht zum Entschließungsantrag zur algorithmenbasierten Videodatenauswertung im öffentlichen Raum unkommentiert dargestellt.

1. Bundesgesetzliche Regelung

§ 27 BPolG - Selbsttätige Bildaufnahme- und Bildaufzeichnungsgeräte

Die Bundespolizei kann selbsttätige Bildaufnahme- und Bildaufzeichnungsgeräte einsetzen, um

1. unerlaubte Grenzübertritte oder Gefahren für die Sicherheit an der Grenze oder
- 2. Gefahren für die in § 23 Abs. 1 Nr. 4¹ bezeichneten Objekte oder für dort befindliche Personen oder Sachen**

zu erkennen.

In den Fällen des Satzes 1 Nr. 2 muss der Einsatz derartiger Geräte erkennbar sein. Werden auf diese Weise personenbezogene Daten aufgezeichnet, sind diese Aufzeichnungen in den Fällen des Satzes 1 Nr. 1 spätestens nach zwei Tagen und in den Fällen des Satzes 1 Nr. 2 spätestens nach 30 Tagen zu vernichten, soweit sie nicht zur Abwehr einer gegenwärtigen Gefahr oder zur Verfolgung einer Straftat oder Ordnungswidrigkeit benötigt werden.

2. Landesgesetzliche Regelungen

2.1. Baden-Württemberg

§ 21 PolG BW - Offener Einsatz technischer Mittel zur Bild- und Tonaufzeichnung

(1) Der Polizeivollzugsdienst kann bei oder im Zusammenhang mit öffentlichen Veranstaltungen und Ansammlungen, die ein besonderes Gefährdungsrisiko aufweisen, Bild- und

¹ § 23 Abs. 1 Nr. 4 BPolG: Die Bundespolizei kann die Identität einer Person feststellen, wenn die Person sich in einer Einrichtung der Bundespolizei (§ 1 Abs. 3), einer Anlage oder Einrichtung der Eisenbahnen des Bundes (§ 3), einer dem Luftverkehr dienenden Anlage oder Einrichtung eines Verkehrsflughafens (§ 4), dem Amtssitz eines Verfassungsorgans oder eines Bundesministeriums (§ 5) oder an einer Grenzübergangsstelle (§ 61) oder in unmittelbarer Nähe hiervon aufhält und Tatsachen die Annahme rechtfertigen, dass dort Straftaten begangen werden sollen, durch die in oder an diesen Objekten befindliche Personen oder diese Objekte selbst unmittelbar gefährdet sind, und die Feststellung der Identität auf Grund der Gefährdungslage oder auf die Person bezogener Anhaltspunkte erforderlich ist.

Tonaufzeichnungen von Personen zur Erkennung und Abwehr von Gefahren anfertigen.
Veranstaltungen und Ansammlungen weisen ein besonderes Gefährdungsrisiko auf, wenn

1. auf Grund einer aktuellen Gefährdungsanalyse anzunehmen ist, dass
Veranstaltungen und Ansammlungen vergleichbarer Art und Größe von terroristischen
Anschlägen bedroht sind oder
2. auf Grund der Art und Größe der Veranstaltungen und Ansammlungen
erfahrungsgemäß erhebliche Gefahren für die öffentliche Sicherheit entstehen können.

(2) Der Polizeivollzugsdienst kann in den in § 26 Abs. 1 Nr. 3 genannten Objekten² oder in deren unmittelbarer Nähe Bild- und Tonaufzeichnungen von Personen anfertigen, soweit Tatsachen die Annahme rechtfertigen, dass an oder in Objekten dieser Art Straftaten begangen werden sollen, durch die Personen, diese Objekte oder darin befindliche Sachen gefährdet sind.

(3) Der Polizeivollzugsdienst oder die Ortspolizeibehörden können an öffentlich zugänglichen Orten Bild- und Tonaufzeichnungen von Personen anfertigen, wenn sich die Kriminalitätsbelastung dort von der des Gemeindegebiets deutlich abhebt und Tatsachen die Annahme rechtfertigen, dass dort auch künftig mit der Begehung von Straftaten zu rechnen ist.

(4) Der Polizeivollzugsdienst kann die nach Absatz 1 Satz 2 Nummer 1 sowie Absatz 2 und 3 angefertigten Bildaufzeichnungen auch automatisch auswerten. Die automatische Auswertung darf nur auf das Erkennen solcher Verhaltensmuster ausgerichtet sein, die auf die Begehung einer Straftat hindeuten.

(5) Der Polizeivollzugsdienst kann bei der Durchführung von Maßnahmen zur Gefahrenabwehr oder zur Verfolgung von Straftaten oder Ordnungswidrigkeiten an öffentlich zugänglichen Orten zur Abwehr einer Gefahr Daten durch Anfertigen von Bild- und Tonaufzeichnungen mittels körpernah getragener Aufnahmegeräte erheben. Die Erhebung personenbezogener Daten kann auch dann erfolgen, wenn Dritte unvermeidbar betroffen sind.

(6) Die Speicherung der nach Absatz 5 erlangten Daten für eine Dauer von mehr als 60 Sekunden ist nur zulässig, wenn Tatsachen die Annahme rechtfertigen, dass dies zum Schutz von

² Verkehrs- oder Versorgungsanlage oder -einrichtung, öffentliches Verkehrsmittel, Amtsgebäude, anderes besonders gefährdetes Objekt

Polizeibeamten oder Dritten gegen eine Gefahr für Leib oder Leben erforderlich ist. Die Datenerhebung nach Absatz 1 bis 4 und 7 bleibt unberührt.

(7) Der Polizeivollzugsdienst kann in Gewahrsam genommene Personen offen mittels Bildübertragung beobachten, soweit dies zu ihrem oder zum Schutz des zur Durchführung des Gewahrsams eingesetzten Personals oder zur Verhütung von Straftaten in polizeilich genutzten Räumen erforderlich ist.

(8) Auf die Beobachtung mittels Bildübertragung und die Bild- und Tonaufzeichnung sowie die automatisierte Auswertung ist, sofern diese nicht offenkundig ist, in geeigneter Weise hinzuweisen. Bild- und Tonaufzeichnungen sind unverzüglich, spätestens jedoch nach vier Wochen zu löschen, soweit sie im Einzelfall nicht zur Verfolgung von Straftaten oder von Ordnungswidrigkeiten von erheblicher Bedeutung, zur Geltendmachung von öffentlich-rechtlichen Ansprüchen oder nach Maßgabe des § 2 Abs. 2 zum Schutz privater Rechte, insbesondere zur Behebung einer bestehenden Beweisnot, erforderlich sind. Die weitere Verarbeitung darf auch erfolgen, wenn Dritte unvermeidbar betroffen werden. Die Bedeutung einer Ordnungswidrigkeit ist erheblich, wenn nach den Umständen des Einzelfalls ein Schaden für ein wichtiges Rechtsgut oder für andere Rechtsgüter in erheblichem Umfang droht oder wenn die betreffende Vorschrift ein sonstiges wichtiges Interesse der Allgemeinheit schützt.

(9) Für die erhobenen Daten nach Absatz 5 gilt Absatz 8 mit der Maßgabe, dass diese spätestens nach 60 Sekunden automatisch zu löschen sind und jede über das Erheben hinausgehende Verarbeitung ausgeschlossen ist, sofern nicht zuvor die Voraussetzungen des Absatzes 6 vorliegen.

2.2. Bayern

Art. 33 PAG - Offene Bild- und Tonaufnahmen

(1) Die Polizei kann bei oder im Zusammenhang mit öffentlichen Veranstaltungen oder Ansammlungen personenbezogene Daten offen

1. auch durch den Einsatz technischer Mittel zur Anfertigung von Bild- und Tonaufnahmen oder -aufzeichnungen über die für eine Gefahr Verantwortlichen erheben, wenn tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dabei Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten begangen werden, oder

2. mittels

- a) Bildaufnahmen oder Übersichtsaufnahmen oder
- b) Übersichtsaufzeichnungen

erheben, wenn dies wegen der Größe oder Unübersichtlichkeit der Örtlichkeit erforderlich ist; die gezielte Feststellung der Identität einer auf der Übersichtsaufzeichnung abgebildeten Person ist nur unter den Voraussetzungen der Nr. 1 zulässig.

(2) Die Polizei kann

1. zur Abwehr

- a) einer Gefahr oder
- b) einer drohenden Gefahr für ein bedeutendes Rechtsgut,

2. an den in Art. 13 Abs. 1 Nr. 2 genannten Orten³, wenn sie öffentlich zugänglich sind, oder

3. an Orten, bei denen tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass dort Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten begangen werden, wenn diese Orte öffentlich zugänglich sind,

offen Bild- und Tonaufnahmen oder -aufzeichnungen von Personen anfertigen.

(3) Die Polizei kann an oder in den in Art. 13 Abs. 1 Nr. 3 genannten Objekten⁴ offen Bild- und Tonaufnahmen oder -aufzeichnungen von Personen anfertigen, soweit tatsächliche Anhaltspunkte die Annahme rechtfertigen, dass an oder in Objekten dieser Art Straftaten begangen werden sollen, durch die Personen, diese Objekte oder andere darin befindliche Sachen gefährdet sind.

(4) Die Polizei kann bei Maßnahmen der Gefahrenabwehr an öffentlich zugänglichen Orten Personen offen mittels automatisierter Bild- und Tonaufzeichnung, insbesondere auch mit körpernah getragenen Aufnahmegeräten, kurzfristig technisch erfassen, wenn dies zum Schutz von Polizeibeamten oder Dritten erforderlich ist. Verarbeitungsfähige Aufzeichnungen dürfen gefertigt werden, wenn dies nach den Umständen zum Schutz von Polizeibeamten oder eines Dritten vor

³ Ort, von dem auf Grund tatsächlicher Anhaltspunkte anzunehmen ist, dass dort Personen Straftaten verabreden, vorbereiten oder verüben, sich Personen ohne erforderliche Aufenthaltserlaubnis treffen, sich Straftäter verbergen, an dem Personen der Prostitution nachgehen, der als Unterkunft oder dem sonstigen, auch vorübergehenden Aufenthalt von Asylbewerbern und unerlaubt Aufhältigen dient.

⁴ Verkehrs- oder Versorgungsanlage oder -einrichtung, öffentliches Verkehrsmittel, Amtsgebäude, anderes besonders gefährdetes Objekt

Gefahren für ein bedeutendes Rechtsgut erforderlich ist. In Wohnungen dürfen Maßnahmen nach diesem Absatz nur zur Abwehr einer dringenden Gefahr für Leben, Gesundheit oder Freiheit einer Person erfolgen, sofern damit nicht die Überwachung der Wohnung verbunden ist. In Wohnungen darf zudem keine kurzfristige technische Erfassung ohne unverzügliche Fertigung verarbeitungsfähiger Aufzeichnungen erfolgen. Es ist sicherzustellen, dass im Falle einer kurzfristigen technischen Erfassung im Sinn von Satz 1, an die sich keine unverzügliche Fertigung verarbeitungsfähiger Aufzeichnungen anschließt, die betroffenen personenbezogenen Daten unverzüglich gelöscht werden.

(5) Bei Maßnahmen nach den Abs. 1 bis 3 dürfen Systeme zur automatischen Erkennung und Auswertung von Mustern bezogen auf Gegenstände einschließlich der automatischen Systemsteuerung zu diesem Zweck verwendet werden, soweit dies die jeweilige Gefahrenlage auf Grund entsprechender Erkenntnisse erfordert.

(6) Die Polizei weist bei Maßnahmen nach den Abs. 1 bis 4 in geeigneter Weise auf die Bild- und Tonaufnahmen und -aufzeichnungen hin, soweit diese nicht offenkundig sind oder Gefahr im Verzug besteht. Auf die Verwendung von Systemen im Sinn von Abs. 5 ist dabei gesondert hinzuweisen.

(7) Maßnahmen nach den Abs. 1 bis 5 dürfen auch dann durchgeführt werden, wenn Dritte unvermeidlich betroffen werden.

(8) Bild- und Tonaufnahmen oder -aufzeichnungen und daraus gefertigte Unterlagen sind spätestens zwei Monate nach der Datenerhebung zu löschen oder zu vernichten, soweit diese nicht benötigt werden

1. zur Verfolgung von Ordnungswidrigkeiten von erheblicher Bedeutung oder Straftaten,
2. zur Überprüfung der Rechtmäßigkeit der polizeilichen Maßnahme, wenn eine solche Überprüfung zu erwarten steht, oder
3. zum Zwecke der Benachrichtigung gemäß Art. 50 Abs. 1 Satz 1 Nr. 1, wenn die Erhebung nach Abs. 5 Satz 2 erfolgt ist.

Die Löschung ist zu dokumentieren.

(9) Für Bild- und Tonaufnahmen oder -aufzeichnungen durch die Polizei bei oder im Zusammenhang mit öffentlichen Versammlungen und Aufzügen gilt Art. 9 BayVersG.