NATIONAL SECURITY
НАЦИОНАЛНА СИГУРНОСТ

AI-ENABLED SURVEILLANCE SYSTEMS IN THE CONTEXT OF NATIONAL SECURITY AND CRITICAL INFRASTRUCTURE PROTECTION

Bastian Nagel
University of Library Studies and Information Technologies
https://doi.org/10.70300/CSJX1373

Abstract: *The article examines whether and to what extent AI-based motion and behavior pattern recognition can enhance both safety and security at train stations. To answer this research question, secondary research was conducted through a comprehensive literature review. The findings indicate that AI-supported video surveillance is essential for effective safety and security management, as it overcomes the human limitations of conventional monitoring systems. These technologies can identify and track individuals and objects, interpret behavior, and distinguish between relevant and irrelevant activities – although their performance is heavily dependent on the quality of the training data used. The systems learn typical behavior patterns and can automatically trigger alerts in case of deviations. This enables the detection of crowd dynamics, group behavior, and potentially dangerous situations, as well as the timely response to security-related incidents such as pickpocketing, unauthorized access to tracks, acts of vandalism, or even terrorism and sabotage. As a result, security personnel can be used more efficiently, and the public's sense of safety and security can be strengthened. Despite concerns regarding data protection, initial legal frameworks demonstrate that clear regulatory conditions can be established to legitimize the use of such technologies.*
Keywords: *Artificial Intelligence; CCTV; Threat Prevention; Public Safety; Risk Mitigation*

INTRODUCTION

The use of video technology at railway stations in Germany has almost doubled since 2012. By the end of 2024, a total of 11,000 cameras were in use at 750 stations, inevitably forming a central component of the security architecture of the Federal Republic of Germany (Bundesministerium des Innern 2024). In addition to the expansion of conventional video surveillance, the focus in recent years has shifted from simply recording and visualising sequences using video cameras to processing and analysing the data obtained using intelligent systems. Is the person in the video waving to his wife, who is just leaving on the train, or is he about to punch a man on the platform? The video surveillance of the future should provide an answer in a fraction of a second. These video surveillance systems, which use intelligent software to perform automated data analysis and provide users with pre-processed information, are referred to as 'smart video surveillance systems'(Schreiber 2009, 2). The prerequisite for such classification is that the software used can independently recognise patterns in the processed images using an algorithm. Possible application scenarios include biometric facial recognition, tracking people and objects, and analysing behaviour patterns (Held 2014, 21). Although it is difficult for a person being filmed to assess the extent of surveillance even in the context of conventional video surveillance, it can be assumed that the use of artificial intelligence will further restrict the personal rights of a large part of the population. Particularly when used by government agencies, this requires specific government regulation. In this context, the European Union enacted the EU Artificial Intelligence Act in 2024, which includes a risk classification for AI systems and is intended to regulate intelligent video surveillance, among other things. A comprehensive description of all usage scenarios would exceed the scope of this paper. For this reason, the focus is on motion and behaviour pattern recognition, as the author sees the greatest potential for application in this area. The aim of this article is to answer the question of whether and to what extent AI-supported movement and behaviour pattern recognition can improve safety and security at railway stations.

RESEARCH METHODOLOGY

The research methodology used for this paper includes a review and analysis of the existing literature. As part of this literature analysis research, the existing literature is not only reviewed, but also summarized, evaluated and interpreted in the context of the scientific question. This involves consulting academic literature and evaluation studies, as well as the legal situation and, in isolated cases, media reports. The evaluation of specialist literature is expected to provide information on the state of the art, legal conditions and developments in particular. By analysing the evaluation studies, information can be obtained on how the initial trials of intelligent video surveillance have progressed and what actual benefits motion and behaviour pattern recognition could have for security and safety at a railway station.

RESULTS

Necessity of using intelligent video surveillance at railway stations

The use of intelligent video technology is an option in places where conventional video surveillance is already in place. In addition to public events and gatherings, conventional video surveillance focuses in particular on public places prone to danger and particularly vulnerable objects (Desoi 2018, 268). According to the German Minister of the Interior, rail transport is a critical infrastructure that is particularly worthy of protection (Deutscher Bundestag 2007, 5). In addition to airports, railway stations are also considered particularly vulnerable, with the added factor that the open system of the railway does not provide for any security checks on persons or fencing around the infrastructure, as is customary at airports. In particular, the open system and the transport of large numbers of people make both railway stations and trains potential terrorist targets (Bergfink 2016, 16). In addition to the specific threat of terrorist attacks, there are other reasons for installing conventional video surveillance. These include deterring potential perpetrators and enabling identification in cases of offences commonly committed at railway stations, such as damage to property, bodily harm or theft, from a police perspective, and ensuring smooth operations on the part of transport companies (Bergfink 2016, 4). However, operating companies have also recognized that the safer passengers feel, the more frequently they use rail transport. Preventing crimes against passengers and protecting operating facilities from vandalism is therefore just as important as increasing rail users' subjective sense of safety (Harter 2023, 46). Since artificial intelligence has now become suitable for mass use and can be utilized on widely available standard devices (Kämpfer und Voss-de Haan 2019, 1).Security authorities and public service companies cannot ignore this technology either. This is particularly true when it can be assumed that the use of such technology will prevent or immediately stop both terrorist acts and everyday crimes through early detection of the perpetrators. Especially since manual evaluation would require a much larger workforce, particularly when dealing with large amounts of data, e.g. in the context of major events. But the accuracy of humans searching for matches can also be called into question (Wübbelt 2020, 44). In this context, Desoi refers to a decline in performance in relation to the viewing time of the video images (monitor blindness) and long response times between the reporting of a relevant event and the deployment of security personnel. For these reasons as well, effective security and safety measures within the framework of conventional video surveillance can only be achieved through a high personnel effort. (Desoi 2018, 18).

CCTV vs. intelligent video surveillance

The basic principle of conventional video surveillance is simple. A video camera films an area and the images are transmitted one-to-one to a monitor, where they can be viewed by a control person. Intelligent video surveillance uses software for this purpose, which filters the video material for predefined anomalies. If the software detects an anomaly, an operator is notified, who then has the opportunity to view the detail filtered out by the software and take appropriate action (Held 2014, 18 ff.). This means that intelligent video surveillance goes beyond the motion detection already available in conventional video surveillance. Instead, the software can recognise, categorise, track, locate and interpret the behavior of relevant objects. These can be both people and objects that can change a situation (Fraunhofer IOSB 2017, 10). A prerequisite for the evaluation of dig-

itized data by algorithms is that the software also has access to as much training data as possible with known patterns or statistical average patterns with which a comparison can be made (Held 2014, 50).

Technical fundamentals of intelligent video surveillance

Due to the complexity and varying designs offered by different manufacturers, only a rough overview can be provided here. Intelligent video surveillance systems usually consist of several interconnected 'intelligent' video cameras. The number depends on the user's requirements and is only limited by the performance capabilities of the existing hardware. Multiple networked cameras have the particular advantage that the probability of comprehensive motion detection within a video-recorded area increases with the number of cameras used (Desoi 2018, 27). The oldest analysis method, which can be considered the basis for further steps in the vast majority of existing video surveillance systems, is 'motion detection', which is particularly suitable for static events, such as leaving a suitcase behind, because it is already possible to recognize simple behavior patterns and trigger an alarm based on such a detection (Anstädt et al. 2010, 5). The system thus recognizes that something is moving in an image. In many cases, this is followed by 'tracking', which aims to map the actual movement of the detected object (Desoi 2018, 28). Object tracking continuously determines the position of an object in the camera image during recording. In the subsequent activity detection, the algorithms learn to recognize typical behavior in the monitored area. If an unusual or predefined deviating movement is detected, the system triggers an alarm (Lang 2023, 124).

Operational applications of motion and behaviour pattern recognition

Security research therefore focuses in particular on analysis software that can be used in the field of hazard prevention and hazard control. Examples of areas of application include behavioral analysis for the prevention of security-related incidents and the analysis of people flows at large events with the aim of identifying and avoiding potential accident situations at an early stage (Desoi 2018, 3). In 2018, Horn et al. investigated the capabilities of computer vision in relation to the sociological analysis of group emotions and escalation processes within a group. According to their findings, image-based evaluations can be used to perform systematic and large-scale analyses of group behavior. This enables the detection of relevant events and provides new research approaches for further phenomena of group behaviour (Horn et al. 2018, 146). Since technology allows behavior to be declared irregular, it is also possible to monitor high-crime areas with regard to specific offences. In the case of railway stations, these offences include pickpocketing, damage to property and drug dealing. By detecting loitering, pre-delinquent behavior can be identified at an early stage and crimes can thus be prevented before they occur (Lang 2023, 126). Railway companies also do not want groups of people or individuals to linger for long periods without the intention of travelling by train. Loitering can therefore also be detected when the usual length of stay in an area is exceeded. Risks to people associated with rail transport can also be minimized. For example, if someone enters a defined alarm zone, such as the track area, video analysis can detect unauthorized access and immediately alert security personnel (Harter 2023, 47). Subsequently, track closure could be initiated immediately or security personnel could be dispatched. Depending on the susceptibility to error, fully automated track closure due to a person entering the track would also be conceivable. For several years now, Berlin Südkreuz station has been used for research purposes by Deutsche Bahn (Germany´s national railway company) and the Federal Police with the aim of improving security and responsiveness at a busy station through modern video surveillance and intelligent analysis systems. The focus here is on preventing dangers and providing automated support for security personnel. Following the completion of a project on facial recognition at railway stations (Bundespolizeipräsidium Potsdam 2018) video technology has been expanded since 2019 and research is being conducted in the field of behaviour recognition. Here, too, AI-supported software is used to generate automatic alerts to a control centre. The research project aims to identify certain scenarios, such as people in need of assistance, abandoned luggage, crowds and people entering restricted areas, and to derive appropriate measures. Tests are carried out with actors to demonstrate the scenarios and optimize the software by simulating real-life hazardous situations (Deutsche Bahn 2024a). The focus here is on the aforementioned alarm

system that is triggered when certain areas are entered. The software detects people or objects that remain in sensitive areas, such as the platform edge or directly on the tracks, for a prolonged period of time and automatically triggers warnings to the control center. A final report is not yet available (Deutsche Bahn 2024b). From a police perspective, there are also further test phases. For example, the police in Mannheim have been testing an AI-supported system since 2018 that automatically detects potentially criminal behavior and alerts the police control center. The system was initially installed at Mannheim railway station and in other areas of the city center. Encrypted data is transmitted to the police control center, where it is evaluated by the algorithm and then assessed by police officers. The focus here is on determining the extent to which certain algorithms can reliably detect behavior patterns relevant to policing, such as hitting or kicking (Kannenberg 2018). The project was extended by three years in December 2023 (Fraunhofer IOSB 2025). Right from the start of the project, the police were able to provide initial positive feedback. When a critical movement pattern was detected, e.g. a fight breaking out, the police were able to arrive at the scene with police officers after an average of two and a half minutes (Wübbelt 2020, 44). In the immediate vicinity of the station, alarm messages can be used even more immediately by addressing perpetrators or endangered persons via loudspeaker announcements and demanding that they take or refrain from taking certain actions. Behavior pattern recognition can also be useful outside enclosed railway facilities, as it allows unauthorized persons in the track area to be detected, thereby preventing metal theft or acts of sabotage on the railway infrastructure (Harter 2023, 47).

Legal Challenges

Although conventional video surveillance in public spaces has been the subject of legal debate for decades due to the limited personal rights of railway station users (Desoi 2018, 4), it is undisputed that, given the greater intensity of the intrusion, the existing legal basis for conventional video surveillance is insufficient for the use of AI-based analysis software (Wübbelt 2020, 45) (Desoi 2018, 282) (Golla 2020). The European Union has recognized this problem and already enacted the EU AI Act in August 2024, which applies to all European Member States and sets out binding regulations depending on the risk that an AI system poses to society. Behavioral pattern recognition is indirectly regulated in Article 5(1)(c) and (d), Annex III(6a) and Annex III(4b). According to these provisions, it is prohibited when used for social scoring or mass surveillance and highly regulated when used in the areas of law enforcement, security or emotion recognition. These applications therefore fall under the category of 'high-risk AI' and special requirements are imposed to ensure that the use of AI in the field of behavioural pattern recognition does not violate fundamental rights and the GDPR (European Parliament 01.08.2024). The newly enacted police powers in some federal states are based on these principles and were developed at state level to meet specific requirements. In February 2025, Hamburg introduced a change in the law that allows the police to train and test AI systems under strict data protection and security requirements (§ 37a PolDVG). In December 2024, the federal state of Hesse passed the 'Law on Strengthening Internal Security'. Section 14 explicitly regulates motion and behavior pattern recognition. According to this, AI-based video analysis may be used to recognize and evaluate motion patterns that indicate a criminal offence, as well as patterns of a weapon, knife or dangerous object. If movement patterns indicating a criminal offence are detected, the police subsequently check whether a criminal offence of considerable significance is likely; in the case of a weapon pattern, the police may also automatically track the person (Landtag Hessen 13.12.2024).

CONCLUSIONS/DISCUSSION

It is clear that police authorities, railway companies and station operators cannot resist the continuous development and expansion of intelligent video surveillance, as it is an important component of an innovative, digitally supported security architecture. Motion and behavior pattern recognition can be used not only for law enforcement purposes but is also essential from a preventive policing perspective in order to be able to prevent criminal acts at an early stage or to recognize in good time when a person poses a danger or is in a dangerous situation. AI-based video surveillance will continue to face criticism from data protectionists who are concerned about mass surveillance

and a lack of control. However, the first police intervention standards show that legislators are perfectly capable of creating clear legal regulations that can dispel some doubts. In addition to reducing the workload on staff, knowledge of intelligent video surveillance and, in particular, behavior pattern recognition, which can also prevent terrorist offences in certain circumstances, can lead to an increased sense of security among the general public and railway users. Another benefit not considered here could also be in the area of occupational safety. For example, motion detection could warn of an approaching train, or the system could detect people in the track area or people who are not wearing high-visibility vests. Such benefits could be explored further in the future.

REFERENCES

ANSTÄDT, T.; KELLER, I.; LUTZ, H., 2010. *Intelligente Videoanalyse. Handbuch für die Praxis*. 1. Auflage, neue Ausg. Weinheim: Wiley-VCH.

BERGFINK, A., 2016. *Videoüberwachung im öffentlichen Personennahverkehr*. Dissertation. Edewecht: OLWIR – Oldenburger Verlag für Wirtschaft, Informatik und Recht.

BUNDESMINISTERIUM DES INNERN, 2024. *Gemeinsam für mehr Sicherheit: 11.000 Kameras an Bahnhöfen – Zahl der durch die Bundespolizei aufgeklärten Straftaten verdreifacht*. [viewed 08 July 2025]. Available from: https://www.bmi.bund.de/SharedDocs/pressemitteilungen/DE/2024/12/bahnhof-kameras.html

BUNDESPOLIZEIPRÄSIDIUM POTSDAM, 2018. *Teilprojekt 1: Biometrische Gesichtserkennung. Abschlussbericht.* Potsdam. [viewed 13 September 2025]. Available from: https://media.frag-den-staat.de/files/foi/431222/20191023_Abschlussbericht_Stand_18.09.2018.pdf

DESEOI, M., 2018. *Intelligente Videoüberwachung: Rechtliche Bewertung und rechtsgemäße Gestaltung*. Wiesbaden: Springer Vieweg.

DEUTSCHE BAHN, 2024a. *Ausbau der Videotechnik. Deutsche Bahn und Bundespolizei bauen gemeinsam die Videotechnik an Bahnhöfen aus*. [viewed 13 September 2025]. Available from: https://sicherheitsbahnhof.bahnhof.de/suedkreuz/Videotechnik/Ausbau-der-Videotechnik-9642248#9642248

DEUTSCHE BAHN, 2024b. *Fragen und Antworten zur Videotechnik und Videoanalyse*. [viewed 13 September 2025]. Available from: https://sicherheitsbahnhof.bahnhof.de/suedkreuz/Videotechnik/Fragen-und-Antworten-zur-Videotechnik-und-Videoanalyse-9643002

DEUTSCHER BUNDESTAG, 2007. *Beschlussempfehlung und Bericht des Innenausschusses zu dem Gesetzentwurf der Bundesregierung – Drucksachen* 16/6292, 16/6570 (neu). Entwurf eines Dritten Gesetzes zur Änderung des Bundespolizeigesetzes. Berlin. [viewed 14 September 2025]. Available from: https://dserver.bundestag.de/btd/16/071/1607148.pdf

EUROPEAN PARLIAMENT, 2024. *Artificial Intelligence Act (AI Act)*. 01 August 2024. [viewed 14 September 2025]. Available from: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L_202401689

FRAUNHOFER IOSB, 2017. *Öffentliche Sicherheit – intelligente Videoauswertung. Ed. J. Beyerer. Karlsruhe: Fraunhofer Institut für Optronik, Systemtechnik und Bildauswertung*. [viewed 12 September 2025]. Available from: https://www.iosb.fraunhofer.de/content/dam/iosb/iosbtest/documents/projekte/intelligente-video%C3%BCberwachung/visIT3_2017%20Oeffentliche%20Sicherheit.pdf

FRAUNHOFER IOSB, 2025. *Intelligente Videoüberwachung für mehr Sicherheit und Datenschutz. Algorithmenbasierte Videoüberwachung im öffentlichen Raum zur Bekämpfung von Straßenkriminalität*. [viewed 13 September 2025]. Available from: https://www.iosb.fraunhofer.de/de/projekte-produkte/intelligente-videoueberwachung.html

GOLLA, S., 2020. *Lernfähige KI erfordert lernfähiges Polizeirecht. Verfassungsblog*. [viewed 13 September 2025]. Available from: https://verfassungsblog.de/lernfaehige-ki-erfordert-lernfaehiges-polizeirecht/

HARTER, M., 2023. Intelligente Videoüberwachung sichert Bahnhöfe und Bahnanlagen. *Der Nahverkehr*, no. 12, pp. 46–48.

HELD, C., 2014. *Intelligente Videoüberwachung*. Dissertation, Universität Würzburg, 2013. Berlin: Duncker & Humblot.

HORN, D.; HOUBEN, S.; SCHÖNER, G., 2018. Erste Ansätze zur automatischen Erkennung von Gruppenverhalten mithilfe des Computersehens. In: REICHERTZ, J.; KEYSERS, V. (Eds.). *Emotion, Eskalation, Gewalt. Wie kommt es zu Gewalttätigkeiten vor, während und nach Fußballspielen?* 1. Auflage. Weinheim; Basel: Beltz Juventa, pp. 130–147.

KÄMPFER, A.; VOSS-DE HAAN, P., 2019. *Künstliche Intelligenz und ihre Bedeutung für die Polizei. Bundeskriminalamt.* [viewed 12 September 2025]. Available from: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/ForumKI/ForumKI2019/kiforum2019VossKaempferAbstract.html

KANNENBERG, A., 2018. *Mannheim testet verhaltensbasierte Videoüberwachung. In Mannheim soll ein intelligentes Kamerasystem kriminelles Verhalten erkennen und die Polizei alarmieren*. [viewed 13 September 2025]. Available from: https://www.heise.de/news/Mannheim-testet-verhaltensbasierte-Videoueberwachung-4239279.html

LANDTAG HESSEN, 2024. *Gesetz zur Stärkung der Inneren Sicherheit in Hessen*. 13 December 2024. [viewed 10 September 2025]. Available from: https://starweb.hessen.de/cache/GVBL/2024/00083.pdf

LANG, J., 2023. Intelligente Videoüberwachung. Eine Wirkungsanalyse am Beispiel der Verhaltens-/Bewegungsmustererkennung. *Kriminalistik*, no. 2, pp. 124–128.
SCHREIBER, S., 2009. *Personenverfolgung und Gestenerkennung in Videodaten*. Technische Universität München. [viewed 08 July 2025]. Available from: https://mediatum.ub.tum.de/doc/676401/676401.pdf
WÜBBELT, B., 2020. Zankapfel intelligente Videoüberwachung: Verwaltungsgericht Hamburg kassiert Löschungsanordnung. *Polizei, Verkehr und Technik*, vol. 65, no. 2, pp. 42–45.

СИСТЕМИ ЗА НАБЛЮДЕНИЕ, ПОДПОМАГАНИ ОТ ИЗКУСТВЕН ИНТЕЛЕКТ, В КОНТЕКСТА НА НАЦИОНАЛНАТА СИГУРНОСТ И ЗАЩИТАТА НА КРИТИЧНАТА ИНФРАСТРУКТУРА

Резюме: *Статията разглежда дали и до каква степен разпознаването на модели на движение и поведение, базирано на изкуствен интелект, може да подобри безопасността и сигурността на железопътните гари. За да се отговори на този изследователски въпрос, беше проведено вторично проучване чрез цялостен преглед на литературата. Констатациите показват, че видеонаблюдението, поддържано от ИИ, е от съществено значение за ефективното управление на безопасността и сигурността, тъй като преодолява човешките ограничения на конвенционалните системи за наблюдение. Тези технологии могат да идентифицират и проследяват лица и обекти, да интерпретират поведението и да правят разлика между релевантни и нерелевантни дейности, въпреки че ефективността им силно зависи от качеството на използваните данни за обучение. Системите учат типични модели на поведение и могат автоматично да задействат сигнали в случай на отклонения. Това дава възможност за откриване на динамиката на тълпата, групово поведение и потенциално опасни ситуации, както и за навременна реакция при инциденти, свързани със сигурността, като джебчийство, неразрешен достъп до релси, вандалски актове или дори тероризъм и саботаж. В резултат на това персоналът по сигурността може да се използва по-ефективно, а чувството за безопасност и сигурност на обществеността може да се засили. Въпреки опасенията, свързани със защитата на данните, първоначалните правни рамки показват, че могат да бъдат създадени ясни регулаторни условия, които да легитимират използването на такива технологии.*

Ключови думи: *изкуствен интелект; видеонаблюдение; предотвратяване на заплахи; обществена безопасност; намаляване на риска*

Бастиан Нагел, докторант
Университет по библиотекознание и информационни технологии
София, България
E-mail: bastian.nagel2@gmx.de