Law. Human. Environment

Journal homepage: https://environmentalscience.com.ua/en
Law. Human. Environment, 16(2), 118-134

UDC 351.74:004.8
DOI: 10.31548/law/2.2025.118

Balancing public safety and civil rights: Successes and challenges of AI-based video surveillance systems

Surya Sagar Vaddiparti
Master of Science, Information Security Officer
City of Portland, Maine
04101, 389 Congress Str., Portland, United States of America
https://orcid.org/0009-0008-9258-9460
Fuad Babaiev*
Master of Science, IT Project Manager II
City of Portland, Maine
04101, 389 Congress Str., Portland, United States of America
https://orcid.org/0009-0004-0572-3643

Article's History:

Received: 02.02.2025
Revised: 28.04.2025
Accepted: 22.05.2025

Abstract

In contemporary society, security has acquired exceptional importance, prompting increasing interest in intelligent video surveillance. The aim of this study was to conduct a systematic analysis of current approaches to AI-powered video analytics, encompassing technological algorithms, legal constraints, and the social implications of their application. The methodology employed an interdisciplinary approach combining systems analysis, legal and comparative methods, analytical review, and case study analysis. The research examined the functional capabilities of intelligent video systems based on machine learning and deep learning. It revealed that although modern AI video analytics systems are highly effective in enhancing security (e.g., threat detection and behavioural analysis), they also generate significant ethical and legal risks – particularly with respect to privacy violations and algorithmic discrimination. A comparative legal analysis highlighted marked

Suggested Citation:
Vaddiparti, S.S., & Babaiev, F. (2025). Balancing public safety and civil rights: Successes and challenges of AI-based video surveillance systems. *Law. Human. Environment*, 16(2), 118-134. doi: 10.31548/law/2.2025.118.

*Corresponding author

differences in regulatory models across jurisdictions: European systems emphasise privacy protection, while the Chinese approach prioritises threat prevention. AI-powered video analytics has had a profound impact on the right to privacy, particularly due to the mass collection of biometric data and automated profiling, sparking debate over compliance with international standards such as the General Data Protection Regulation and the Convention for the Protection of Human Rights. The comparative analysis demonstrated divergent approaches: in the EU, privacy protection is paramount (e.g., the ban on facial recognition in France), whereas China and the United States focus more on security – often at the expense of civil liberties. Regulatory challenges include the misalignment of national laws with international norms, especially regarding data retention and algorithmic bias. To strike a balance, the study proposed clear legal frameworks, limitations on data storage periods, independent oversight, and "ethical passports" for algorithms – measures that would combine technological efficacy with the safeguarding of human rights. The study recommends harmonising standards that take into account both technical capacities and ethical-legal norms. The practical value lies in the potential use of the findings to design balanced AI video analytics systems

Keywords: surveillance; legal frameworks; algorithmic bias; privacy policy; crime prevention; public safety

Introduction

In modern world, security has become one of society's fundamental values, driving the rapid development and deployment of cutting-edge video surveillance technologies. The emergence of intelligent systems capable of analysing video streams in real time has not only transformed the monitoring of public spaces but also ushered in a new paradigm in the field of security. The application of artificial intelligence (AI) in video analytics has gained particular relevance, especially in areas such as threat detection, anomaly identification, and the monitoring of suspicious behaviour. In light of global challenges – such as terrorism, mass unrest, and disasters at large-scale events – intelligent video surveillance is increasingly viewed not merely as a monitoring tool but as an active component of public safety infrastructure. At the same time, the rapid advancement of AI demands continuous revision of existing analytical methods, the integration of new algorithms, the improvement of hardware, and the resolution of ethical and legal dilemmas. The relevance of this study lies in the contradictory effects of AI video surveillance on public safety and human rights. On the one hand, technologies for facial recognition, behavioural analysis, and predictive analytics greatly enhance crime prevention capabilities. On the other, the mass collection of biometric data, total surveillance of public spaces, and risks of algorithmic discrimination present significant threats to: Privacy (e.g., unauthorised profiling of individuals); Freedom of movement (e.g., the "chilling effect" of constant surveillance); Civil liberties (e.g., suppression of protest activity); Equality (e.g., biased algorithms affecting specific social groups). International institutions such as the United Nations and the European Union call for legal safeguards – ranging from Data Protection Impact Assessments (DPIAs) to algorithmic transparency – making the investigation of the balance between security and human rights critically important to the development of responsible AI. In the 2020s, numerous researchers examined the potential of AI in the context of video surveillance.

Notably, the work by E. Şengönül *et al.* (2023) reviewed modern machine and deep learning methods for anomaly detection in video streams. The study by A. Rashid and A. Kausik (2024) analysed over 200 sources on AI surveillance, identifying a central tension between enhancing public safety and the risks posed to privacy rights. The authors compared various regulatory models – from the strict General Data Protection Regulation (2016) to more liberal frameworks – emphasising the necessity of transparent algorithms and safeguards against discrimination. Their conclusions underscore the need for balanced legal frameworks that reconcile technological progress with the protection of democratic values. In another study, D. Almeida *et al.* (2022) examined the ethical and legal challenges of facial recognition technologies used by law enforcement in the United States, the United Kingdom, and the EU. The authors advocated for mandatory human rights and data impact assessments, alongside standardised transparency requirements.

M. Smith and S. Miller (2022) focused on the potential of facial recognition in combating crime, while simultaneously highlighting privacy risks and the need for legal frameworks to preserve democratic values. M. Anderljung *et al.* (2023) addressed regulatory challenges surrounding advanced AI models, which pose significant risks to public safety. They proposed a governance model combining industry self-regulation with state oversight through standardisation, registration, and control mechanisms. In a separate contribution, A. Mantelero (2022) developed a human rights-oriented AI risk assessment methodology, integrating ethical and social values into legal regulation and addressing shortcomings in traditional data protection approaches. The research by L. Ricciardi Celsi (2023) introduced an innovative method for assessing AI projects using a "risk-adjusted actual value" metric. It demonstrated that higher risk can diminish potential social benefit, thereby informing sound decision-making in technology development. A. Habbal *et al.* (2024) explored the AI TRiSM framework as a means of fostering trust in AI through risk management, security, and compliance. The authors stressed the importance of flexible responses to dynamic threats and cross-sectoral cooperation. Thus, the literature shows widespread interest in issues of transparency, legal oversight, ethical standards, and risk governance in the context of AI. However, insufficient attention has been paid to the influence of cultural and social contexts on the perception and legitimacy of AI surveillance, as well as the role of public participation in shaping related policies.

The aim of this study was to identify the optimal conditions for the application of AI-based video surveillance that ensure a balance between enhancing public safety and upholding human rights. The research objectives included: examining the impact of technical parameters of AI video analytics (such as algorithm accuracy and error rates) on privacy guarantees; conducting a comparative analysis of legal approaches to video surveillance regulation in the EU, the USA, and Asia; and formulating recommendations for the integrated use of security technologies and the protection of citisens' rights.

Materials and Methods

The methodological foundation of this research was an interdisciplinary approach that combined legal, socio-technical, comparative, analytical and systems analysis methods. The systems analysis method was employed to examine AI-based video surveillance systems as comprehensive cyber-physical entities comprising technical, informational, organisational, and legal components. This method facilitated the structuring of the analysis of system functionalities (e.g., event detection, intelligent video analytics, facial recognition), and the assessment of their effectiveness

in urban safety environments. The central research method was normative legal analysis, which enabled the identification of regulatory frameworks governing surveillance systems in different jurisdictions. This method was applied to the examination of key legal instruments, including the Convention for the Protection of Human Rights and Fundamental Freedoms (1950), the Personal Information Protection Law (2021), the Privacy Act (1974), and the CLOUD Act Resources (2019). These sources were scrutinised in terms of their regulation of biometric data processing, requirements for video surveillance, the rights of individuals, and oversight of public and private entities processing personal data. The comparative legal method was used to contrast national approaches to the regulation of AI-based surveillance systems. Comparisons were based on the following criteria: the presence or absence of core legislation or a regulatory code; the extent of privacy protection; conditions for data collection, processing, and storage; data subject rights safeguards; oversight and monitoring mechanisms; specific regulations on video surveillance; and examples of practical implementation. The case study method was applied to analyse concrete examples of AI-enhanced video surveillance implementation in the USA, China, and the UK. The study examined three specific cases of AI surveillance for public safety: facial recognition in Los Angeles (Team DigitalDefynd, 2025), optimisation of the 911 emergency response system in New York City, and the Flock Safety vehicle tracking system (Valentino, 2025). These cases were analysed using comparative methods to identify shared trends, quantitative evaluation of effectiveness statistics, and qualitative analysis of regulatory documents. Functional analysis was used to explore the operational aspects of AI surveillance systems (facial recognition, behavioural analysis, predictive analytics) and the interaction of these functionalities with legal norms. The study assessed whether national legislation provides adequate control over these capabilities and whether human rights compliance mechanisms are embedded in the technology (data protection impact assessments, data retention limits, algorithmic explainability requirements, etc.).

Results

Deployment of intelligent video surveillance systems: Assessing opportunities for public safety. In the context of rapid technological advancement, AI is transforming approaches to public safety. One of the most important tools in this process is the deployment of AI-based video surveillance systems. These systems combine artificial intelligence, computer vision, automated event detection, and intelligent video analytics, forming complex monitoring infrastructures capable of real-time data analysis and immediate threat identification. AI video surveillance systems involve the use of machine learning algorithms to process video data for the purpose of detecting and classifying objects, events, or anomalies without the need for direct human intervention (Sung & Park, 2021). Computer vision is a core component of these systems, enabling machines to recognise patterns, analyse video streams, and identify objects such as faces, vehicles, or behavioural patterns. Advances in computer vision have significantly enhanced the ability of surveillance systems to perform accurate facial and biometric recognition, improving the efficacy of preventive measures. Automated event detection allows AI systems to identify unusual or hazardous situations, such as unattended objects in public spaces, crowd congestion, aggressive behaviour, or unauthorised access (Ameen & Stone, 2023). This enables prompt responses to potential threats, eliminating delays associated with human operators. Intelligent video analytics further extend the functionality of these systems by providing risk prediction, crowd behaviour analysis, suspicious

activity detection, and the integration of data from various sources to form a comprehensive security picture (El-Alfy *et al.*, 2023).

These technologies are being actively implemented to enhance public safety. According to a study by M.E. Antunes (2019), 84% of cities (54 cities) implementing Smart City strategies utilise video surveillance systems with facial and biometric recognition capabilities. This significantly increases the effectiveness of criminal suspect tracking, locating missing persons, and securing access to critical infrastructure. Moreover, 46% of cities use drones and aerial surveillance systems for wide-area monitoring and rapid incident response, while 39% of municipalities employ gunshot detection sensors and mobile applications that allow citisens to report suspicious activities or threats.

The application of AI in public safety systems in the USA, China, and European countries demonstrates notable progress in the integration of AI solutions into municipal structures such as police forces, transport networks, educational institutions, and public spaces. In the USA, the Department of Homeland Security, under the leadership of Secretary Alejandro N. Mayorkas, actively deploys AI to combat illicit fentanyl trafficking, safeguard critical infrastructure, and prevent child exploitation. The DHS has introduced an updated AI solutions registry that exceeds the federal OMB M-24-10 standards (Hysen, 2024), exemplifying a transparent and accountable approach. In London, the police employ AI-driven VR simulations to train officers, enhancing their preparedness for high-stress scenarios, although these systems require oversight due to risks of psychological strain and algorithmic bias (Team DigitalDefynd, 2025). These examples illustrate the delicate balance between innovation and ethics in applying AI to public safety. In China, the development of "smart cities" entails the widespread use of video surveillance, facial recognition, and behavioural analysis in public areas. Comprehensive AI solutions are integrated into transport infrastructure, municipal services, and educational institutions, forming real-time safety networks. The Chinese model is characterised by the large-scale collection of data and extensive use of biometric technologies for monitoring both criminal and administrative violations.

One of the key indicators of the effectiveness of AI technologies is a significant reduction in crime rates. According to analytical data from 2019, the implementation of video surveillance systems with automatic event detection and intelligent video analytics can reduce crime by 30-40% (Antunes, 2019). Another important outcome of AI implementation in the security sector is the accelerated response time of emergency services. Data indicate that AI technologies can shorten the response time of rescue, police, and medical services by 20-35%. Through the use of automated video footage analysis and sensor data, AI systems enable rapid incident detection and precise localisation, significantly optimising resource coordination and facilitating timely responses to emergencies.

AI-powered video surveillance is used not only for detecting crimes but also for threat prediction through the analysis of criminogenic data (Kosinski, 2021). In road traffic, such systems automatically detect violations and alert emergency services, while in fire safety they ensure early smoke detection (Team DigitalDefynd, 2025). Facial recognition and classification technologies (FR/FC), which constitute half of all systems, require rigorous testing to ensure compliance with human rights standards (Hysen, 2024). In Chicago, the Strategic Subject List (SSL) predictive patrol system analyses social media and sensor data to reduce crime in key areas. These examples illustrate the balance between the efficiency of AI and the protection of civil liberties. The role of AI-powered surveillance systems in enhancing safety

within public institutions is becoming increasingly significant in today's context. The application of AI-based video surveillance across various domains is summarised in Table 1.

Table 1. The role of AI video surveillance systems in different areas

Area of application	Role and functional capabilities of AI-based video surveillance systems	Additional benefits and application features
Schools and educational institutions	Preventive monitoring to avert acts of violence, vandalism, and bullying. Detection of dangerous objects (weapons, prohibited items), identification of suspicious behaviour among students and visitors. Integration with records of past violations for developing preventive measures	Enhanced safety for students and staff. Creation of a secure educational environment. Reduction in critical incidents through early risk detection
Airports	Monitoring passenger behaviour, detecting unattended items, facial recognition of individuals posing potential threats. Integration with security systems for automated alerts and action coordination	Optimisation of evacuation procedures and passenger flow management. Enhanced transportation security without slowing down passenger movement
Public parks and open spaces	Prevention of theft, vandalism, and attacks on visitors. Real-time detection of suspicious behaviour. Monitoring compliance with environmental regulations (e.g., illegal waste disposal, damage to greenery)	Improved safety in large open areas with minimal physical patrolling. Promotion of environmental cleanliness in public spaces
Homeless shelters and crisis centres	Protection of residents from violence and disorder. Detection of emergencies (e.g., suicide attempts, aggressive behaviour) with integration into rapid response systems	Increased protection for vulnerable population groups. Timely incident response and provision of necessary assistance
Libraries, municipal offices, sports facilities, cultural centres	Prevention of property theft, monitoring public order during mass events, access control to premises. Customisation of system algorithms to local institutional conditions	Improved efficiency of security measures without excessive intrusion into visitors' privacy. Flexibility and personalisation of system settings according to the facility's specifics

Source: compiled by the authors based on N. Sugianto (2021), V. Karishma and T. Vigneswaran (2023), M. Sujkowski *et al*. (2023)

The advancement of AI technologies in video surveillance systems has led to a qualitative leap in ensuring the safety of public spaces (Sugianto *et al.*, 2024). Surveillance has evolved from passive event recording to active analytical response, allowing not only the detection of violations but also the early prediction of potential threats. The implementation of such systems facilitates more efficient allocation of security resources, reduces social tension in crisis situations, and enhances public trust in safety infrastructure.

Legal and ethical challenges of AI-powered video surveillance. The legal and ethical challenges posed by AI-powered video surveillance remain among the most pressing issues at the intersection of digital technology, human rights, and security. On the one hand, AI-based systems have proven highly effective in detecting, preventing, and investigating offences, thereby stimulating increased interest from both governments and the private sector in their widespread deployment. On the other hand, such technologies significantly affect the exercise of fundamental rights and freedoms, particularly with respect to privacy, personal autonomy, the protection of personal data, and the right to non-discrimination. In many countries, current legislation has proved ill-equipped to deal with the new realities shaped by AI and mass surveillance. Legal frameworks often fail to keep pace with technological development, leaving significant regulatory gaps that could potentially lead to violations of fundamental human rights.

In the United States, despite the foundational status of the right to privacy enshrined in the Fourth Amendment to the Constitution of the United States (1787), legislation in the field of video surveillance remains fragmented. The absence of a single federal law regulating the processing of biometric and other personal data allows private companies to collect, store, and use video and audio information without clearly defined limits or obligations. Furthermore, the "right to be forgotten" – actively protected in EU countries – has no legal basis in the US, depriving citisens of meaningful control over their digital footprint. These conditions create potential risks of abuse, discrimination, and arbitrary surveillance. The principle of legal certainty – one of the cornerstones of the rule of law – is undermined, as individuals are unable to predict how, by whom, and for what purposes their data will be processed.

China represents the opposite regulatory model. While the Personal Information Protection Law (2021) is formally aimed at limiting the collection and use of personal data, in practice it does not provide effective mechanisms for the protection of citisens' rights. In a centralised political system where state security takes precedence over individual rights, AI-enhanced video surveillance technologies are used for comprehensive population monitoring. Government authorities have near-unlimited access to surveillance cameras, and systems such as "Skynet" (Baek, 2024) track individuals' movements in real time, employ facial recognition, and process massive volumes of data without any requirement for informing or obtaining consent from citisens. As such, the Chinese regulatory framework does not function as a safeguard but instead legitimises expanded state powers in the domain of digital surveillance.

The European Union offers an alternative model, grounded in the primacy of human rights as a foundational principle of digital transformation. The General Data Protection Regulation (2016) sets high standards of transparency, accountability, and proportionality in the use of personal data. Under the GDPR, organisations are obliged to conduct a Data Protection Impact Assessment (DPIA) prior to implementing surveillance systems that may pose a high risk to privacy (Andrew & Baker, 2021). The primary aim of the DPIA is to identify, prevent, or mitigate violations of citisens' rights. Within the framework of Council of Europe law, the protection of private life has also been significantly reinforced, particularly through the case law of the European Court of Human Rights interpreting Article 8 of the Convention for the Protection of Human Rights and Fundamental Freedoms (1950). This jurisprudence establishes the obligation of states not only to avoid unlawful interference but also to ensure effective oversight of data processing by third parties, including private companies. Nonetheless, even within the EU, new challenges have emerged in connection with automated decision-making, algorithmic opacity, and the complexity of technical evaluation by judicial authorities. In response, the draft European AI Act proposes a classification of AI systems by risk level. High-risk technologies – such as AI-based video surveillance – must meet strict technical, ethical, and legal standards, including requirements for transparency, data quality, anti-discrimination safeguards, and human involvement in decision-making processes.

In numerous jurisdictions, inconsistencies exist between legal provisions on privacy, surveillance, cybersecurity, and AI usage. This can result in situations where the use of a particular technology – such as AI-powered surveillance – complies with one legal act but contradicts another. For example, within the EU, despite the harmonised framework provided by the GDPR, national approaches to implementing its provisions vary (Atkinson *et al.*, 2021). In France, the Commission Nationale Informatique & Libertés has prohibited the use of real-time facial recognition in

public spaces, whereas other EU countries maintain less stringent restrictions (Poirson, 2021). In Germany, even the use of experimental video surveillance systems by the police remains limited (Tóth, 2023). These disparities illustrate the need for further harmonisation within the European legal space. A comparative analysis of legal frameworks in the area of video surveillance reveals two global models: the European model, prioritising human rights, stability, and control over technological development; and the Asian-American model, characterised by corporate freedom in the US and state control in China. The choice of model has a direct impact on the legal architecture of society, the level of privacy protection, and the transparency of digital surveillance tools.

In Los Angeles, an extensive network of cameras equipped with facial recognition and behaviour analysis technologies has been implemented to detect suspicious activity in real time. The system automatically alerts law enforcement to potential threats, such as unattended items or the presence of individuals with criminal records. Despite improved response efficiency, the use of such technologies has raised serious public concern regarding the risks of mass surveillance and racial bias in the processes of recognition and categorisation (Team DigitalDefynd, 2025). The practice of automated profiling and the real possibility of recognition errors may result in unlawful intrusions into citisens' private lives and discriminatory outcomes.

A particularly illustrative case occurred on February 19 involving the Flock Safety system, which uses AI to detect stolen vehicles. The system identified a stolen Jeep, prompting a police patrol to initiate a pursuit and apprehend the suspect. This incident demonstrated the high efficiency of AI in combating crime; however, it simultaneously intensified public debate regarding the right to privacy. Human rights organisations have emphasised that the mass capture of license plates of all vehicles – regardless of whether they are connected to any offenses – constitutes a serious intrusion into citisens' private lives. In the city of Oakland alone, 289 such cameras have already been installed, with the number expected to rise to 400 by the summer. Representatives of the American Civil Liberties Union (ACLU) have regarded such measures as steps toward total surveillance, arguing that the systems track the movements of ordinary citisens without their consent (Valentino, 2025). Despite police assurances that the collected data is retained for only 30 days and used exclusively for crime prevention, experts warn of potential abuses, particularly the use of such data to create citisen profiles or for purposes beyond those originally declared.

The fragmented nature of legal regulation in the United States lies in the absence of a unified, nationwide act that would standardise the protection of personal data. Instead, various laws adopted at the state level apply, resulting in an uneven legal landscape where citisens' rights depend on their place of residence or even the location where the data was collected. For example, the California Consumer Privacy Act (2018) grants state residents the right to know what data is collected about them and to request its deletion (Kaminski *et al.*, 2021). In contrast, states such as Texas and Georgia either lack such legislation or offer significantly lower levels of protection. This creates a situation where the same company operating across multiple states must comply with different standards depending on the jurisdiction, and citisens effectively have unequal levels of rights and privacy guarantees.

This fragmentation also poses serious challenges to the implementation of the principle of legal certainty. Companies may intentionally locate their servers or data processing centres in jurisdictions with less stringent privacy requirements to avoid stricter regulations, such as those in California or Illinois (where the Biometric Information Privacy Act applies). In the field of video

surveillance, this results in the practical possibility of using facial recognition systems in public spaces without informing citisens or obtaining their consent – actions that may be legal in some states but illegal in others. This complicates judicial practice, undermines the principle of equality before the law, and opens the door to potential abuses. In such an environment, both users and public authorities often struggle to define clear legal boundaries or protection mechanisms, which significantly weakens the effectiveness of law enforcement and erodes trust in digital technologies at the national level.

The principle of legal certainty requires clarity and stability of legal norms to ensure predictable law enforcement. In the context of video surveillance, a notable example of legal uncertainty is the ambiguous application of the so-called "right to be forgotten" across jurisdictions. While this right is enshrined in Article 17 of the EU's GDPR (2016), there is no equivalent legal mechanism in the United States. As a result, American citisens are deprived of the opportunity to seek the deletion of information that may harm their reputation or privacy – an especially critical issue amid the proliferation of automated surveillance systems.

In countries undergoing legal transformation – such as Ukraine and several post-Soviet states – there is a noticeable discrepancy between the provisions of national legislation and the obligations assumed under international law. Ukraine is a party to the Convention for the Protection of Human Rights and Fundamental Freedoms (1950) and recognises the jurisdiction of the European Court of Human Rights (ECtHR), whose case law is binding. This is particularly relevant to compliance with Article 8 of the Convention, which guarantees the right to respect for private and family life, home, and correspondence. The ECtHR has repeatedly emphasised that state interference in private life is permissible only when it is lawful, necessary, and proportionate.

Nevertheless, Ukrainian national legislation regarding the implementation of video surveillance technologies – particularly those involving AI and facial recognition – does not contain explicit requirements for prior human rights impact assessments. This approach is inconsistent with the GDPR (2016), which mandates the use of Data Protection Impact Assessments (DPIAs) when technologies are likely to pose a high risk to fundamental rights and freedoms (Andrew & Baker, 2021). The absence of such procedures in Ukrainian law indicates a lack of alignment with European data protection standards and potentially violates Article 8 of the Convention, which, according to ECtHR jurisprudence, also applies to digital surveillance. Furthermore, the lack of regulation – or excessive generality – in provisions governing the use of surveillance systems creates conditions for their disproportionate and non-transparent application. For instance, deploying facial recognition cameras in public spaces without adequate legal justification and effective oversight mechanisms may constitute excessive intrusion into private life. Such practices contradict European standards, which require that any surveillance technology be grounded in law, have clearly defined boundaries of use, and be subject to independent oversight. As a result, a conflict arises between a state's declared international obligations and the actual state of their implementation in the national legal system.

Given the findings regarding public attitudes toward AI-based surveillance systems and the identified need for legal clarity, trust, and transparency, a set of scientifically grounded recommendations is warranted at both legislative and practical levels. First and foremost, it is necessary to adopt a unified national act regulating the use of AI systems in the field of security, in light of current technological challenges. Unlike the EU, the United States lacks a comprehensive federal data protection law equivalent to the General Data Protection

Regulation (2016). Currently, only regional acts exist, most notably the California Consumer Privacy Act (2018), which, while providing basic rights, does not fully regulate the use of biometric data.

It would be advisable to expand the provisions of the California Consumer Privacy Act (2018) – particularly in the section on the collection and processing of personal information (§1798.100-1798.115) – by introducing a clause requiring mandatory notification of individuals when AI-based identification is conducted in public spaces. Such notifications should include the authority conducting the surveillance and the purposes of data collection. It would also be appropriate to amend §1798.105 of the CCPA concerning the right to data deletion, by introducing a specific subcategory: "biometric images obtained through automated video surveillance," which must be destroyed after a clearly defined period (e.g., 30 days), unless there is a lawful basis for retention. Additionally, it is crucial to introduce a provision establishing the right to algorithmic appeal, similar to Article 22 of the GDPR (2016), which prohibits decisions based solely on automated processing when such decisions may have significant legal effects. This provision should be implemented either as a new paragraph within the California Consumer Privacy Act or as a separate clause in a forthcoming national act.

In terms of practical implementation, it is particularly important to strengthen the institutional oversight mechanisms for AI systems. An effective example is the AI Ethics Board initiative in New York, which holds advisory powers concerning the deployment of new video analytics systems. Such an approach enhances transparency and fosters social dialogue. It is recommended to extend a similar model at the federal level, with expanded authority. Attention should also be paid to the EU's experience, particularly the AI Act project, in which biometric surveillance systems were for the first time classified as high-risk and permitted only in exceptional cases. Based on this, it is recommended that AI-powered video surveillance be designated as a "high risk" to human rights, requiring additional legal review prior to the launch of each specific system. This provision should be made mandatory in national legislation. To ensure transparency and accountability, the following measures are recommended: the introduction of a unified online registry of AI video surveillance systems indicating their location, owning authority, data collection purposes, and data retention policy; and the requirement for system providers to develop and publish "ethical passports" of algorithms – a concise description of decision-making logic, associated risks, and safeguards. To ensure the social legitimisation of AI systems, it is proposed that educational curricula include dedicated modules on digital ethics and user rights, aimed at fostering critical awareness among citisens regarding AI technologies.

Discussion

The present study, devoted to modern approaches to ensuring public safety in smart cities through AI-based video surveillance systems, demonstrates both technical advancements in this field and the need for ethical reflection on their implementation. In comparison to other contemporary scholarly works, the findings of this study allow the identification of key commonalities and differences in the emphases, approaches, and challenges associated with integrating intelligent surveillance systems into urban environments. The results obtained should be considered within the context of the current academic discourse on surveillance systems in smart cities, where three major vectors dominate: technological efficiency, socio-humanitarian implications, and the pursuit of ethical balance. In this context, it is pertinent to compare the present article with the works of other researchers, which reveals similarities and distinctions in approaches to balancing public

safety and civil rights under AI-driven surveillance. The study by M. Cabanillas-Carbonell *et al.* (2025) outlined the boundaries of effective AI use in the security domain, with particular emphasis on human rights protection. The authors highlighted the importance of legal support, the implementation of Data Protection Impact Assessments (DPIAs), reduced data retention periods, and algorithmic transparency. Both approaches recognised the need to balance technological potential with ethical standards. However, M. Cabanillas-Carbonell *et al.* (2025) adopted a strategic orientation towards global sustainable development goals, while the present study shifted the emphasis toward regional contexts (EU, USA, China) and practical regulatory solutions (e.g., the AI Act model).

The comparison of research findings enables a deeper evaluation of each study's unique contribution to the discourse on AI in surveillance. The study by W. Ullah *et al.* (2022) underscored the effectiveness of AI technologies in post-conflict stabilisation, focusing on responsiveness, analytical accuracy, and the ability of AI to ensure basic security. In contrast, the current study developed a vision of the necessity for democratic oversight accompanying technological advancement. The emphasis was placed on trust-building mechanisms – independent oversight, digital ethics, and algorithmic accountability – thus extending author's narrowly utilitarian approach towards legal and ethical considerations.

The research by C. Fontes *et al.* (2022) produced a three-component analytical model for assessing AI's societal impact – functional, legal, and social. The authors demonstrated that public perception of AI systems is largely shaped by a sense of state control and fear of privacy intrusion. Comparatively, the current study concluded on the need for regulatory institutionalisation of trust. The proposal for "ethical passports" for technologies emerged as an attempt to develop regulatory tools capable of transforming technical transparency into measurable legal and social responsibility. Thus, while C. Fontes *et al*. (2022) results were analytical in nature, the current study takes a normative and applied approach. In the study by M. Kashef *et al.* (2021), the findings were conceptualised as a transition from centralised, technically closed surveillance systems to open, socio-technical ecosystems. The authors highlighted the importance of decentralisation, public engagement, and open-source code as foundations for increasing public trust. In contrast, the present study resulted in a specific architectural-analytical approach implemented through flexible systems embedded with control mechanisms, legal adaptation, and accountability monitoring. While M. Kashef *et al.* (2021) focused on politico-social models of transformation, this analysis takes an applied, design-oriented approach prioritising human rights compliance in high-tech surveillance contexts.

The work by B.R. Ardabili *et al.* (2022) centred on ensuring user privacy in smart surveillance systems. This study proposed a unique approach to mitigating the risk of personal data exposure via pose-oriented algorithms. This approach fundamentally differed from the methods examined in the present article, which predominantly involved traditional deep learning techniques aimed at enhancing recognition accuracy and behaviour analysis. In contrast, B.R. Ardabili *et al.* (2022) demonstrated a trade-off between privacy protection and analytical efficiency: anomaly detection accuracy significantly declined due to the avoidance of pixel-based image analysis. Hence, the publication highlighted the ambivalence of technological choices – high accuracy does not always align with ethical priorities regarding confidentiality. Meanwhile, the present study proposed a combination of recognition accuracy with a conceptual analysis of legal and ethical boundaries, preserving the balance between

technological efficiency and social responsibility. A comparison with the study by I. Ahmed and G. Jeon (2021) demonstrated that their research was primarily focused on improving real-time tracking and segmentation algorithms, particularly in densely populated environments. The proposed system, based on the SiamMask algorithm, achieved high accuracy even under challenging surveillance conditions, which is especially relevant to urban settings. In contrast to this technocratic approach, the present study placed emphasis on integrating infrastructural solutions with the needs of civil society, including a risk assessment of human rights implications. While the technical advantages reported by I. Ahmed and G. Jeon (2021) – such as 95% accuracy and high adaptability – were of considerable practical value, they remained within the engineering paradigm. Conversely, the analysed article emphasised that in the context of post-crisis urban recovery, priority should be given not only to efficiency but also to the social legitimacy of deploying such technologies, thus offering a more holistic perspective.

The work of D. Çelikkaya (2024) focused on ethical challenges arising from the integration of AI into criminal justice systems within the EU. Convergence with the present research was found in the shared focus on human rights protection, algorithmic accountability, and the need to maintain human oversight over AI-based decision-making. D. Çelikkaya's (2024) study adopted a normative-ethical approach, seeking to develop universal principles for AI in justice systems, without placing particular emphasis on public perception. The concept of "trustworthy AI", as presented by N. Díaz-Rodríguez *et al.* (2023), showed considerable alignment with the conclusions of the primary analysis. Both studies stressed the importance of transparency, fairness, accountability, and data protection, while calling for robust oversight mechanisms. A distinctive feature of author's approach was the systematic structuring of ethical requirements through the triadic lens of legality, ethicality, and technical robustness, which complemented the practical focus of the present study on instruments such as "ethical passports" and regulatory frameworks like the AI Act. As such, both approaches reinforced the necessity for regulated and transparent AI development that addresses a broad range of ethical concerns.

The study by S. Doboș and V. Bagrin (2024) also addressed the dilemma between privacy and security; however, their analysis adopted a more journalistic and discursive tone, concentrating on the societal and legal implications of mass surveillance. A commonality with the present research lay in recognising the dangers of authoritarian misuse of surveillance technologies. However, unlike the systemic approach that proposed concrete legal and technological mechanisms for transparent video surveillance systems, S. Doboș and V. Bagrin's (2024) work largely remained at the level of identifying risks and advocating for further discussion on the limits of oversight, without offering operational models for balancing competing interests. The analysis by K. Nishat (2024) strongly resonated with the present study's findings, particularly in the critique of mass data collection, the opacity of algorithmic processes, and the threat to fundamental rights. Both studies shared a commitment to formulating rights-based policies, prioritising privacy protection and openness. Yet, while K. Nishat (2024) focused on the limitations of existing legal frameworks – such as the General Data Protection Regulation and the International Covenant on Civil and Political Rights – in addressing new digital realities, the present study was enhanced by empirical survey data that reflected actual public sentiment regarding video surveillance, thereby increasing the empirical validity of its conclusions. All of the studies under comparison recognised that the effective deployment of AI in the security domain

must strictly observe human rights, algorithmic transparency, and democratic oversight. Nonetheless, they varied in analytical focus – from legal analysis to socio-political consequences – and in methodology, ranging from conceptual models and ethical theorising to empirical surveys.

The present work proposed a unique combination of interdisciplinary analysis (legal and technical) and practical recommendations, enabling the clear delineation of conditions under which AI-based surveillance systems may be deemed legitimate and socially acceptable. In summary, the comparative analysis revealed substantial interdisciplinary convergence in acknowledging the ethical boundaries and legal requirements for safe AI surveillance development. However, only the present study incorporated direct examination of societal reactions to these processes, representing a key methodological and practical advantage.

Conclusions

The findings of the study demonstrate that AI-based video analytics systems are fundamentally reshaping the relationships between the state, the private sector, and citisens, particularly in relation to the right to privacy, freedom of movement, and the protection of personal data. The most significant threat lies in the mass and often disproportionate collection of biometric information, automated facial recognition in public spaces, and behavioural profiling, which frequently occur without individuals' informed awareness or consent. Such practices violate the principle of voluntariness in the processing of personal data, as enshrined in both international law and national legislation – for example, Article 8 of the European Convention on Human Rights and the provisions on consent in the General Data Protection Regulation. Particular concern arises from the fact that the deployment of AI video analytics is occurring in the absence of an adequate regulatory framework or within highly fragmented legal environments. In many countries, including the United States and a number of post-Soviet states, legal norms remain scattered, inconsistent, or technologically outdated, preventing effective safeguards against abuse. The research identified cases of prolonged storage of video data, its secondary use without proper legal justification, and the risks of selective surveillance targeting vulnerable population groups. These developments pose risks of algorithmic discrimination, distortion of justice, increased inequality, and erosion of public trust in the institutions deploying such technologies. The analysis revealed several critical challenges: lack of algorithmic transparency, insufficient independent oversight, and inconsistent or vague regulatory mechanisms.

To reconcile security needs with privacy rights, a number of practical solutions are proposed. First, biometric systems should be classified as "high-risk," subject to enhanced scrutiny prior to deployment. Second, mechanisms for algorithmic appeals against AI decisions should be developed, in line with Article 22 of the GDPR. The experience of systems like Flock Safety (which has reportedly reduced car theft by 40%) illustrates their effectiveness but also underscores the need for clear limitations on data retention. Equally important is the creation of unified registers of AI systems, indicating their locations, purposes, and data retention policies. Special attention should be given to public education initiatives, as only 19% of citisens are sufficiently informed about the operational principles of such systems. The future of AI-powered video surveillance should be based on four key pillars: technical transparency, legal regulation, institutional oversight, and public dialogue. Evidence shows that technological progress without adequate human rights safeguards leads to distrust and social tension. At the same time, excessive restrictions may reduce the effectiveness of law enforcement. Resolving this dilemma requires sustained dialogue among developers, regulators, human rights advocates, and the public,

as well as flexible regulation capable of adapting to the rapid pace of technological development. Only such a comprehensive approach can unlock the potential of AI video surveillance while preserving democratic values and fundamental rights.

Access to data on the actual effectiveness of AI-based surveillance is limited due to commercial confidentiality and the classified nature of law enforcement operations, which may affect the objectivity of the analysis. Additionally, the sociological surveys were conducted primarily among residents of California, meaning that the findings may not fully reflect the situation in other regions with differing legal and cultural contexts. A promising direction lies in interdisciplinary research that combines technical analysis of AI algorithms with in-depth study of the social consequences of their deployment across various cultural environments. The implementation of pilot projects in "electronic democracy," where citisens participate in shaping surveillance policies via digital platforms, may represent a new phase in the pursuit of a balance between security and freedom.

Acknowledgements

None.

Funding

The study was not funded.

Conflict of Interest

None.

References

[1] Ahmed, I., & Jeon, G. (2021). A real-time person tracking system based on SiamMask network for intelligent video surveillance. *Journal of Real-Time Image Processing*, 18(5), 1803-1814. doi: 10.1007/s11554-021-01144-5.

[2] Almeida, D., Shmarko, K., & Lomas, E. (2022). The ethics of facial recognition technologies, surveillance, and accountability in an age of artificial intelligence: A comparative analysis of US, EU, and UK regulatory frameworks. *AI and Ethics*, 2(3), 377-387. doi: 10.1007/s43681-021-00077-w.

[3] Ameen, M., & Stone, R. (2023). Advancements in crowd-monitoring system: A comprehensive analysis of systematic approaches and automation algorithms: State-of-the-art. *arXiv*. doi: 10.48550/arXiv.2308.03907.

[4] Anderljung, M., *et al*. (2023). Frontier AI regulation: Managing emerging risks to public safety. *arXiv*. doi: 10.48550/arXiv.2307.03718.

[5] Andrew, J., & Baker, M. (2021). The general data protection regulation in the age of surveillance capitalism. *Journal of Business Ethics*, 168, 565-578. doi: 10.1007/s10551-019-04239-z.

[6] Antunes, M.E. (2019). *Surveillance and predictive policing through AI*. Retrieved from https://www.deloitte.com/an/en/Industries/government-public/perspectives/urban-future-with-a-purpose/surveillance-and-predictive-policing-through-ai.html?utm.

[7] Ardabili, B.R., Pazho, A.D., Noghre, G.A., Neff, C., Bhaskararayuni, S.D., Ravindran, A., Reid, S., & Tabkhi, H. (2023). Understanding policy and technical aspects of ai-enabled smart video surveillance to address public safety. *Computational Urban Science*, 3(1), article number 21. doi: 10.1007/s43762-023-00097-8.

[8] Atkinson, K., Collenette, J., Bench-Capon, T., & Dsehtsiarou, K. (2021). Practical tools from formal models: The ECHR as a case study. In J. Maranhão & A.Z. Wyner (Eds.), *Proceedings of the eighteenth international conference on artificial intelligence and law* (pp. 170-174). New York: Association for Computing Machinery. doi: 10.1145/3462757.3466095.

[9] Baek, D.S. (2024). *Skynet project in China – the rise of ubiquitous surveillance*. Retrieved from https://medium.com/@davidsehyeonbaek/skynet-project-in-china-the-rise-of-ubiquitous-surveillance-33fee53c350e.

[10] Cabanillas-Carbonell, M., Rivera, J.S., & Muñoz, J.S. (2025). Artificial intelligence in video surveillance systems for suspicious activity detection and incident response: A systematic literature. *Advances in Science and Technology Research Journal*, 19(3), 389-405. doi: 10.12913/22998624/196795.

[11] California Consumer Privacy Act. (2018, June). Retrieved from https://oag.ca.gov/privacy/ccpa.

[12] Çelikkaya, D. (2024). *Ethical concerns of artificial intelligence use in the criminal justice system under EU law*. Istanbul: Marmara Universitesi.

[13] CLOUD Act Resources. (2019, April). Retrieved from https://www.justice.gov/criminal/cloud-act-resources.

[14] Constitution of the United States. (1787, September). Retrieved from https://constitution.congress.gov/constitution/amendment-4/.

[15] Convention for the Protection of Human Rights and Fundamental Freedoms. (1950, November). Retrieved from https://www.echr.coe.int/european-convention-on-human-rights.

[16] Díaz-Rodríguez, N., Del Ser, J., Coeckelbergh, M., de Prado, M.L., Herrera-Viedma, E., & Herrera, F. (2023). Connecting the dots in trustworthy Artificial Intelligence: From AI principles, ethics, and key requirements to responsible AI systems and regulation. *Information Fusion*, 99, article number 101896. doi: 10.1016/j.inffus.2023.101896.

[17] Doboș, S., & Bagrin, V. (2024). The balance between privacy and safety: The ethics of public video surveillance. In *Technical-scientific conference of students, master and PhD students* (pp. 805-809). Chisinau: Tehnica-UTM.

[18] El-Alfy, E.-S., Bebis, G., & Zhou, M. (2023). *Intelligent image and video analytics*. London: CRC Press.

[19] Fontes, C., Hohma, E., Corrigan, C.C., & Lütge, C. (2022). AI-powered public surveillance systems: why we (might) need them and how we want them. *Technology in Society*, 71, article number 102137. doi: 10.1016/j.techsoc.2022.102137.

[20] General Data Protection Regulation. (2016, May). Retrieved from https://gdpr-info.eu.

[21] Habbal, A., Ali, M.K., & Abuzaraida, M.A. (2024). Artificial Intelligence trust, risk and security management (AI trism): Frameworks, applications, challenges and future research directions. *Expert Systems with Applications*, 240, article number 122442. doi: 10.1016/j.eswa.2023.122442.

[22] Hysen, E. (2024). *AI at DHS: A deep dive into our use case inventory*. Retrieved from https://www.dhs.gov/archive/news/2024/12/16/ai-dhs-deep-dive-our-use-case-inventory?utm.

[23] Kaminski, M.E., Snow, J., Wu, F.T., & Hughes, J. (2021). Symposium: The California consumer privacy act. *SSRN*. doi: 10.2139/ssrn.3763290.

[24] Karishma, V.R., & Vigneswaran, T. (2023). Artificial intelligence in video surveillance. In P. Swarnalatha (Ed.), *Handbook of research on deep learning techniques for cloud-based industrial IoT* (pp. 1-17). London: IGI Global. doi: 10.4018/978-1-6684-8098-4.ch001.

[25] Kashef, M., Visvizi, A., & Troisi, O. (2021). Smart city as a smart service system: Human-computer interaction and smart city surveillance systems. *Computers in Human Behavior*, 124, article number 106923. doi: 10.1016/j.chb.2021.106923.

[26] Kosinski, M. (2021). Facial recognition technology can expose political orientation from naturalistic facial images. *Scientific Reports*, 11(1), article number 100. doi: 10.1038/s41598-020-79310-1.

[27] Mantelero, A. (2022). *Beyond data: Human rights, ethical and social impact assessment in AI*. Berlin: Springer Nature. doi: 10.1007/978-94-6265-531-7.

[28] Nishat, K. (2024). Human rights protections in digital surveillance: Balancing security needs and privacy rights. *Mayo Communication Journal*, 1(1), 83-92.

[29] Personal Information Protection Law of the People's Republic of China. (2021, August). Retrieved from https://www.gov.cn/xinwen/2021-08/20/content_5632486.htm.

[30] Poirson, C. (2021). The legal regulation of facial recognition. In K. Miller & K. Wendt (Eds.), *The fourth industrial revolution and its impact on ethics: Solving the challenges of the agenda 2030* (pp. 283-302). Cham: Springer. doi: 10.1007/978-3-030-57020-0_21.

[31] Privacy Act. (1974, December). Retrieved from https://www.justice.gov/opcl/privacy-act-1974.

[32] Rashid, A.B., & Kausik, A.K. (2024). AI revolutionising industries worldwide: A comprehensive overview of its diverse applications. *Hybrid Advances*, 7, article number 100277. doi: 10.1016/j.hybadv.2024.100277.

[33] Ricciardi Celsi, L. (2023). The dilemma of rapid AI advancements: Striking a balance between innovation and regulation by pursuing risk-aware value creation. *Information*, 14(12), article number 645. doi: 10.3390/info14120645.

[34] Şengönül, E., Samet, R., Abu Al-Haija, Q., Alqahtani, A., Alturki, B., & Alsulami, A.A. (2023). An analysis of artificial intelligence techniques in surveillance video anomaly detection: A comprehensive survey. *Applied Sciences*, 13(8), article number 4956. doi: 10.3390/app13084956.

[35] Smith, M., & Miller, S. (2022). The ethical application of biometric facial recognition technology. *AI & Society*, 37(1), 167-175. doi: 10.1007/s00146-021-01199-9.

[36] Sugianto, N. (2021). *Responsible AI for automated analysis of integrated video surveillance in public spaces*. Gold Coast: Griffith University. doi: 10.25904/1912/4371.

[37] Sugianto, N., Tjondronegoro, D., Stockdale, R., & Yuwono, E.I. (2024). Privacy-preserving AI-enabled video surveillance for social distancing: Responsible design and deployment for public spaces. *Information Technology & People*, 37(2), 998-1022. doi: 10.1108/ITP-07-2020-0534.

[38] Sujkowski, M., Kozuba, J., Uchroński, P., Banaś, A., Pulit, P., & Gryżewska, L. (2023). Artificial intelligence systems for supporting video surveillance operators at international airport. *Transportation Research Procedia*, 74, 1284-1291. doi: 10.1016/j.trpro.2023.11.273.

[39] Sung, C.S., & Park, J.Y. (2021). Design of an intelligent video surveillance system for crime prevention: applying deep learning technology. *Multimedia Tools and Applications*, 80(26), 34297-34309. doi: 10.1007/s11042-021-10809-z.

[40] Team DigitalDefynd. (2025). *AI in public safety – 5 case studies [2025]*. Retrieved from https://digitaldefynd.com/IQ/ai-in-public-safety/.

[41] Tóth, L. (2023). The evolution of public surveillance systems in Europe. *Magyar Rendésset*, 23(1), 191-204. doi: 10.32577/mr.2023.1.12.

[42] Ullah, W., Ullah, A., Hussain, T., Muhammad, K., Heidari, A.A., Del Ser, J., Baik, S.W., & De Albuquerque, V.H. (2022). Artificial Intelligence of Things-assisted two-stream neural network for anomaly detection in surveillance Big Video Data. *Future Generation Computer Systems*, 129, 286-297. doi: 10.1016/j.future.2021.10.033.

[43] Valentino, S. (2025). *CHP uses AI surveillance to arrest Bay Area suspect on Oakland bus*. Retrieved from https://is.gd/yfvzoO.

Баланс між громадською безпекою та громадянськими правами: успіхи та виклики систем відеоспостереження на основі ШІ

Сурія Сагар Ваддіпарті
Магістр, спеціаліст з інформаційної безпеки
Портланд, Мен
04101, вул. Конгресу, 389, м. Портланд, Сполучені Штати Америки
https://orcid.org/0009-0008-9258-9460
Фуад Бабаєв
Магістр, керівник ІТ-проектів ІІ
Портланд, Мен
04101, вул. Конгресу, 389, м. Портланд, Сполучені Штати Америки
https://orcid.org/0009-0004-0572-3643

Анотація

У сучасному суспільстві безпека набула особливої цінності, що зумовило зростаючу увагу до інтелектуального відеоспостереження. Метою дослідження був системний аналіз сучасних підходів до ШІ-відеоаналітики, включаючи технологічні алгоритми, правові обмеження та соціальні наслідки їх застосування. Методологію становив міждисциплінарний підхід із поєднанням системного, правового, порівняльного, аналітичного аналізу та кейс-стаді. У ході дослідження було проаналізовано функціональні можливості інтелектуальних відеосистем, що ґрунтувалися на машинному та глибокому навчанні. Дослідження виявило, що сучасні системи ШІ-відеоаналітики, попри їхню ефективність у підвищенні безпеки (виявлення загроз, аналіз поведінки), породжували серйозні етико-правові ризики, зокрема порушення приватності та алгоритмічну дискримінацію. Порівняльний правовий аналіз засвідчив значну різницю між моделями регулювання у різних юрисдикціях: європейські системи зосереджуються на захисті приватності, натомість китайська – на превенції загроз. Відеоаналітика з використанням штучного інтелекту суттєво вплинула на право на приватність, зокрема через масовий збір біометричних даних та автоматичне профілювання, що викликало суперечки щодо відповідності міжнародним стандартам, таким як Загальний регламент про захист даних і Конвенція про захист прав людини. Порівняльний аналіз показав різні підходи: у ЄС домінує захист приватності (наприклад, заборона розпізнавання облич у Франції), тоді як у Китаї та США акцент зроблено на безпеку, часто за рахунок прав громадян. Регуляторні виклики включали неузгодженість національних законів із міжнародними нормами, зокрема щодо зберігання даних та алгоритмічної упередженості. Для досягнення балансу запропоновано чіткі юридичні рамки, обмеження строків зберігання даних, незалежний нагляд та «етичні паспорти» алгоритмів, що дозволило б поєднати ефективність технологій із гарантіями прав людини. Рекомендовано уніфікацію стандартів, що враховують як технічні можливості, так і етико-правові норми. Практична цінність полягає у можливості використання результатів для проєктування збалансованих ШІ-систем відеоаналітики

Ключові слова: контроль; правові рамки; алгоритмічна упередженість; політика конфіденційності; запобігання злочинності; суспільна безпека