DOI: 10.38146/BSZ-AJIA.2026.v74.i4.pp1081-1097

The Use of Surveillance Cameras, Legal Framework and Practical Differences: Scientific Research

Attila Steiner
doctoral student
Óbuda University
Doctoral School of Security Sciences
steinerattila70@gmail.com

Abstract

Aim: The aims of this study is to provide a comprehensive analysis of the legal and practical environments surrounding CCTV cameras, examing their domestic and international application alongside their impact on public safety and crime prevention. The research pays particular attention to exploring the specific features of Hungarian regulations and practices, benchmarking them against solutions in other countries (the United Kingdom, Germany, the United States).
Methodology: Drawing on practical experience, the author analyzes the role of surveillance systems within the operations of the police, local authorities and the private sector.
Findings: The crime prevention effects of camera systems are mixed; while in some cases they reduce the number of crimes, while in others they tend to cause a geographical desplacement of criminal activity. At the same time, they are clearly effective in crime detection, evidence gathering and strengthening the subjective sense of security. As in other countries, Hungary faces the challenge of legal regulations lagging behind technological developments, particularly with regard to biometric data and facial recognition.
Value: The research highlights that surveillance cameras can serve not only law enforcement but also urban planning and community functions. Adapting international experiences and introducing legally and ethically balanced regulations can help increase social acceptance and enhance public safety.

The manuscript was submitted in English. Received: 15 July 2025. Revised: 20 Aug 2025 Accepted: 16 Dec 2025.

Keywords: CCTV, surveillance, crime prevention, legal environment, international comparison

Introduction to public space surveillance camera systems

Concept and typology of CCTV systems

A closed-circuit television (CCTV) system, also known as video surveillance, consists of cameras that transmit signals to a specific location and to a limited number of monitors. It differs from traditional television broadcasting insofar as the signal is not transmitted openly. Complex, multi-camera systems allow images to be viewed and recorded simultaneously. Camera positions can be fixed or remotely controlled. Modern systems utilize digital video recorders (DVRs) and IP cameras, which are often supplemented with artificial intelligence functions (e.g., facial recognition, predictive analytics) (Baumgartner et al., 2024; Cabrera, 2024). This evolution demonstrates that the 'surveillance camera' is no longer just a physical device but an integrated, networked and increasingly intelligent system.

Historical development and technological progress

The first concepts of surveillance technologies were developed by Russian inventor Léon Theremin in the second half of the 1920s, utilizing radio waves. The first documented use of CCTV can be traced back to the German army (Som, 2017).

In the 1950s, American entrepreneurs began to adapt CCTV for commercial purposes, while in Hamburg, traffic monitoring became the main area of application from 1956 onwards (Tóth, 2022). In 1960, the British Metropolitan Police installed temporary CCTV cameras to monitor mass events.

From 1968, in Olean, New York, pan-and-tilt cameras were installed with the aim of reducing crime, and the images were transmitting images directly to the Olean police station. By the 1980s, CCTV had become widespread in shopping centres and city centres. The 1990s saw the transition from analogue to digital systems, followed by the emergence of IP cameras and high-definition technology in 1996, which represented the main direction of development.

Current trends include the integration of AI and facial recognition, real-time identification, cloud-based storage, access from mobile devices, advanced nighttime surveillance and the use of drones. Artificial intelligence is now capable

of object recognition, license plate recognition and predictive analytics (Ujhegyi et al., 2025; Cabanillas Carbonell et al., 2025; Salgado et al., 2024; Laufs & Borrion, 2022).

The historical overview clearly illustrates the development from primitive analogue systems to AI-supported networks. This rapid innovation – characterized by a new generation every 4–5 years in the case of CCTV – consistently outpaces legislation, which by its nature reacts more slowly, resulting in regulatory lag. This delay raises data protection risks and ethical issues, particularly in relation to profiling and predictive surveillance (Kalluri et al., 2023).

The legal framework for surveillance cameras

The General Data Protection Regulation (GDPR) and its application in Hungary

The GDPR is the European Union's primary data protection framework. It stipulates that the processing of personal data must be lawful, fair and transparent. Video recordings of identifiable individuals are considered personal data under the GDPR.

Data processing is only lawful if at least one of the six specified legal bases applies. 'Legitimate interest' or 'public interest/exercise of official authority' are the most relevant legal bases, which necessitate a specific risk situation and the documentation of a balancing test between the interests of the data controller and the rights of the data subject. Consent must be explicit, specific, informed, unambiguous, voluntary and easily revocable. In an employer-employee relationship, consent cannot generally be considered freely given.

Data subjects must be informed of the monitoring, including the identity and contact details of the data controller, the purpose, the legal basis, the storage period and the rights of the data subjects. This information must be provided via clearly visible signs at the earliest possible stage.

The data collected must be adequate, relevant and limited to what is necessary for the specified purpose. The purposes must be precisely defined for each camera. The data may not be used for purposes other than those specified.

A Data Protection Impact Assessment (DPIA) must be carried out for data processing operations likely to result in a high risk to the rights and freedoms of natural persons. This includes large-scale systematic monitoring of publicly accessible areas or the processing of special categories of data (e.g. biometric data through facial recognition).

Recordings must be stored securely and access must be restricted to authorised persons. Storage periods must be determined in accordance with the purpose and reviewed regularly.

NAIH decisions often refer to violations of purpose limitation and data minimisation. This requires a continuous, in-depth assessment of the reason for collecting the data and the necessity of data collection, shifting the burden of proof to the data controller. This contrasts with a more permissive, 'security for security's sake' approach.

Consent as a legal basis also presents practical challenges. Although consent is one of the legal bases under the GDPR, several sources clearly state that it is often 'not a practical or viable legal basis' for video surveillance, particularly in public places or in employer-employee relationships. This is due to the difficulty of obtaining 'freely given' consent from unknown persons or persons in a hierarchical relationship. The practical difficulty of obtaining consent often leads data controllers to rely on the legal basis of 'legitimate interest'.

Key Hungarian legislation relevant to CCTV cameras: Infotv., Rtv., Kftv., Szvmt., Tht. and other relevant Pötv. laws

Infotv. (Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information): This Act provides the general framework for data processing in conjunction with the GDPR. It defines 'data processing for law enforcement purposes', which falls under the scope of the Infotv. if the purpose is law enforcement and the data controller is a law enforcement agency.

Rtv. (Act XXXIV of 1994 on the Police): This Act originally enabled the police to install cameras in public areas and to make recordings. The police decide on the designation of the public areas to be monitored after obtaining the prior opinion of the competent local government and subsequently publish the data on the camera locations. The Rtv. also covers image and sound recordings captured during police operations.

Kftv. (Act LXIII of 1999 on public space surveillance): This legislation comprehensively regulates the recording of images for crime prevention purposes. The Public Space Surveillance Authority manages the data directly and also operates and maintains the system. Transparency and visibility are paramount, as is the use of conspicuous signage. Professional supervision is conducted by the police.

Szvmt. (Act CXXXIII of 2005 on the rules governing personal and property protection and private investigation activities): This Act regulates electronic surveillance systems for private security purposes, such as the protection of human life and personal freedom, the safeguarding of hazardous materials, and

the protection of trade secrets and property. The Szvmt. requires individuals to be informed about the use of electronic surveillance.

Mt. (Act I of 2012 on the Labour Code): The Labour Code allows employers to monitor the conduct of employees in relation to their employment, including the use of technical devices, provided there is prior written notification. Employees' personal rights may only be restricted if is absolutely necessary and proportionate to the employment relationship.

Tht. Condominium Act (Act CXXXIII of 2003 on Condominiums): In the case of condominiums, the installation and operation of a camera system are decided by the general meeting with at least a two-thirds majority of all ownership shares. The data processing rules must be included in the organisational and operational regulations (SZMSZ). Cameras may not be directed at the entrances or other openings of privately owned apartments, nor at public spaces (unless the viewing angle is restricted by masking), and placement in areas that violate human dignity, such as toilets, is prohibited.

Pötv. The Civil Guard Act (Act CLXV of 2011 on the Civil Guard and the Rules of Civil Guard Activities): Among its additional tasks, the act states that it may participate in the monitoring of recordings made by image recording units. Professional supervision is provided by the police, similar to law enforcement agencies. Members of the country's largest civil organization perform their duties without remuneration, in their free time. Their activities are regulated and stuctured, though they are not authorized to process data relating to image recordings, thus providing assistance exclusively as human resources when required.

In the Hungarian legal environment, there is an observable interaction and potential conflict between different pieces of legislation. Hungary utilizes both general data protection laws and specific statutes. Although the GDPR is the supreme source of law, national laws use 'opening clauses' to establish more detailed rules. However, this can lead to situations where specific laws may be outdated or interpreted in a manner contrary to the principles of the GDPR, as demonstrated by the repeal of conflicting provisions in 2019. This complex legal stratification requires constant vigilance and updates to ensure consistency and compliance, highlighting the challenge of maintaining a uniform data protection standard across different sectors.

Decisions and interpretations of the National Authority for Data Protection and Freedom of Information (NAIH)

The role of the National Authority for Data Protection and Freedom of Information (NAIH) is continually evolving as the body responsible for interpreting

and enforcing legislation. Its decisions often clarify ambiguities and impose fines for non-compliance. NAIH's active enforcement and detailed decisions are key to shaping the practical application of surveillance laws in Hungary, bridging the gap between abstract legal texts and real-world implementation, and encouraging data controllers to adhere more strictly to the principles of the GDPR. At the same time, these regulations may also act as an obstacle to the wider use of cameras, including the inclusion of private, condominium and industrial cameras into public surveillance systems.

The NAIH has addressed the processing of biometric data and facial recognition in public surveillance systems (e.g. the Siófok system). Attila Péterfalvi, President of the NAIH, expressed concern about the lack of clear regulations on the use of facial recognition software in public space systems and the central storage of public space camera recordings.

NAIH decisions consistently emphasize that camera surveillance in the workplace must be based on an appropriate legal basis, as consent in a hierarchical relationship can rarely be considered truly voluntary due to the imbalance of power (NAIH, 2020). Cameras may not be placed in areas that violate human dignity. Surveillance must be proportionate and limited to specific, justified purposes (e.g. property protection). Employers must provide adequate, transparent and prior written information about the use of cameras.

The use of cameras by private individuals is only exempt from the GDPR if it is for private purposes only. If it extends to public areas, other private property or commercial purposes, the GDPR applies. The NAIH has issued specific decisions on camera systems in apartment buildings, often focusing on transparency, legal bases and adequate information.

If a system uses facial recognition, the recorded images become biometric data, which is considered a 'special category' of personal data under the GDPR and requires stricter data processing conditions. The NAIH has repeatedly emphasized that facial recognition is a particularly sensitive area in the case of public space camera surveillance, as it can affect large numbers of people and is capable of covert profiling. Recent amendments in Hungary, which allow the police to use facial recognition in all misdemeanor proceedings, have been criticised for violating the EU AI Act (European Parliament and Council, 2016). The AI Act prohibits real-time remote biometric identification in public places for law enforcement purposes, except in narrowly defined cases of serious crime.

The conflict between national security needs and EU data protection and AI regulations is a direct consequence of rapid technological development and differing national priorities, leading to potential legal challenges.

International legal and regulatory environment

United Kingdom: Data Protection Act 2018 and Information Commissioner's Office (ICO) guidelines

The UK Data Protection Act 2018 incorporates the principles of the GDPR into UK law. Any CCTV recording that captures an identifiable person is considered personal data and falls under the scope of this legislation.

Key requirements:

- Operators must have a legitimate reason (e.g. crime prevention) and clearly indicate that surveillance is taking place.
- Clearly visible signs must be displayed informing individuals about the system, its purpose and the contact details for requesting further information. This ensures transparency.
- Recordings must be appropriate, relevant and limited to what is necessary for the purpose. Excessive surveillance of areas that do not pose a security risk may give rise to data protection concerns.
- Recordings must be stored securely and be only accessible to authorised persons, with password protection and encryption.
- Recordings should not be stored longer than necessary, typically 30 days is the standard retention period, unless there is a valid reason (e.g., an ongoing investigation).
- Individuals have the right to request recordings made about them within one month, with masking applied if necessary to protect the privacy of other individuals.
- During the Data Protection Impact Assessment process, the data controller assesses and manages the risks arising from the data processing operation in advance if they are likely to pose a high risk to the rights of natural persons. This is mandatory for operations likely to present a high risk, especially in the case of systems with biometric capabilities.

CCTV used for personal, domestic purposes (e.g. home security) is generally exempt from the full scope of the DPA and GDPR. However, if cameras record images beyond the property boundary (e.g. neighbours' gardens, public pavements), the rules of the DPA apply, requiring notification of neighbours and clearly visible signage.

This creates a 'grey area' where an apparently private activity can easily become a regulated activity without explicit intent. It highlights the practical

difficulty of regulating surveillance, leading to the need for clear guidelines on camera positioning and masking.

Employers must use CCTV responsibly for specific purposes (security, theft prevention), inform their employees, and ensure that recordings are stored securely and access is restricted.

The Information Commissioner's Office (ICO) regulates and enforces data protection law, provides guidance and handles complaints. The Protection of Freedoms Act 2012 contains the Code of Practice on Surveillance Cameras.

Germany: Bundesdatenschutzgesetz (BDSG, 2018) 'German Federal Data Protection Act' and State Laws (Provincial Police Laws Polizeigesetze-POG/PoIG)

In Germany, police law is a matter for the federal states, which is why video surveillance in public spaces is regulated by separate state laws. (NRW hotspot video: PolG NRW; Bavaria: PAG; Baden-Württemberg: PolG BW; Berlin: ASOG Bln; Rhineland-Palatinate: 'POG' – Polizei- und Ordnungsbehördengesetz). Germany's Federal Data Protection Act (Bundesdatenschutzgesetz, 2018) is in line with the GDPR and supplements it, using so-called 'opening clauses' (Öffnungsklauseln) to clarify or restrict data processing requirements.

Video surveillance of publicly accessible areas is permitted if it is necessary for the performance of tasks, the determination of access rights or the protection of legitimate interests, provided that there are no reasons that override the legitimate interests of the data subjects. The protection of life, health and freedom is considered a paramount interest (BDSG, 2018).

Video surveillance of public areas is regulated in part by the BDSG and in part by police laws, which allow the police to use or require the use of video technology in 'crime hotspots'. Surveillance and the data controller's details must be made clear at the earliest possible point in time, typically by means of clearly visible information boards. The data collected must be deleted immediately if it is no longer necessary for the original purposes or if individuals have a legitimate interest in having the data deleted.

German law places great emphasis on proportionality, ensuring that surveillance is appropriate and necessary, taking into account less invasive means. The courts have ruled that video surveillance is generally illegal at announced gatherings (demonstrations, rallies) and must be deactivated for a certain period of time before and after the gathering in order to protect the fundamental right to freedom of assembly.

Data protection supervision in Germany is decentralised, with each of the sixteen federal states (Länder) having its own authorities. Although the BDSG

provides a federal framework, state police laws also regulate surveillance. This decentralised structure, while allowing for regional approaches, can also lead to inconsistencies in interpretation and enforcement within Germany, making compliance more difficult for national or international entities operating in multiple states.

United States: federal and state data protection laws

The United States does not have a comprehensive, uniform GDPR-like law as in the European Union, but instead employs a patchwork system. Surveillance laws consist of a combination of federal legislation (e.g. Wiretap Act 1968, ECPA 1986, HIPAA 1996, COPPA 1998) and state-level regulations (e.g. CCPA in California, CDPA in Virginia). The application of the two is often fragmented and inconsistent, making compliance difficult for businesses and individuals operating across state lines, leading to greater legal uncertainty and potentially uneven data protection across the country.

Federal laws:

Wiretap Act (Omnibus Crime Control and Safe Streets Act III) 1986: Regulates the interception of oral, wire and electronic communications. A court order is generally required for government interception, and unauthorised interception may be a federal crime.

Electronic Communications Privacy Act (ECPA) 1986: Extended wiretap protections to new forms of digital communication (e-mail, online chat, stored voicemail). Businesses that store surveillance videos or have access to recorded communications may be subject to the ECPA.

Video Voyeurism Prevention Act 2004: Made it a federal crime to record individuals in situations where they have a 'reasonable expectation of privacy.'

Reasonable expectation of privacy is a constitutional principle in the United States established by the Supreme Court (Katz v. United States, 1967). It is generally lawful to record video in public places where there is no reasonable expectation of privacy (e.g., streets, parks). However, it is illegal to record without consent in places where there is a legitimate expectation of privacy (e.g., private bedrooms, bathrooms, changing rooms). However, this concept is subject to judicial interpretation, leading to a reactive legal approach, especially in the case of new technologies, which are evaluated after installation, often through litigation.

In the US, so-called 'wiretapping laws' determine whether the consent of one party or the consent of all participants is sufficient. In 'one-party consent' states, only one person in a conversation needs to consent to the recording (e.g. New

York, Texas). In states with 'two-party' or 'all-party' consent, all participants must be aware of and consent to the recording (e.g. California).

Only about 15 states have specific security camera laws, but counties and cities may also have their own rules. States differ in their regulations on hidden cameras and private property.

Surveillance in the workplace is generally permitted for legitimate business purposes (security, theft prevention), but not in private areas. Some states require employee notification or consent, especially for audio recording.

Signs are often used as a deterrent or for informational purposes, but are not always required at the federal level. However, many jurisdictions mandate clearly visible signage.

Comparative analysis of legal approaches and enforcement

All jurisdictions emphasize the need for lawful purpose, data minimization, secure storage and transparency (conspicuous signage). Data subject rights, such as the right to access one's own recordings, are also widely recognized.

There is a notable difference in the philosophy of legal regulation: a rights-based versus an expectations-based approach. The European legal frameworks (GDPR, Infotv., DPA 2018) are predicated on the assumption that the processing of personal data is prohibited unless specific legal grounds and principles are met. American law, while protecting data privacy, often operates on a 'privacy by design' model. This philosophical divergence leads to different approaches to regulation: Europe tends towards proactive, comprehensive frameworks and strict supervision, while the United States relies more on reactive, case-by-case interpretations and specific prohibitions, resulting in different levels of protection and legal certainty.

The EU imposes stricter regulations under Article 9 of the GDPR and the AI Act, classifying biometric data as 'special category' data and prohibiting real-time remote biometric identification in public places for law enforcement purposes, except in narrow circumstances. In the United States, there is no comprehensive federal law, and state laws vary considerably.

The phenomenon of 'function creep' also poses a challenge in all jurisdictions. Practical applications of CCTV extend beyond their original security purposes to include traffic management, urban planning, retail analytics, and even marketing. This expansion poses recurring ethical and legal challenges. The growing capabilities of video analytics and AI directly incentivize the expansion of application areas. This creates constant tension with the legal principle of purpose limitation, requiring constant reviews of proportionality and transparency, and often leading to legal violations if not handled properly.

Regulatory bodies such as NAIH (Hungary) and ICO (United Kingdom) are actively issuing decisions and imposing fines for non-compliance. The United States relies more on civil lawsuits and specific federal/state enforcement actions.

Table 1

Comparative overview of key legal provisions on CCTV (Hungary, United Kingdom, Germany, USA)

Legal Aspect	Hungary	United Kingdom	Germany	United States
Primary Legal Framework(s)	GDPR; Info Act; Police Act; Private Security and Private Investigation Act; Labour Code; Condominium Act	DPA 2018 (GDPR principles), Protection of Freedoms Act	BDSG (GDPR supplement), State Police Acts (POG)	Federal (Wiretap, ECPA, Video Voyeurism Prevention Act) and State Laws
Legal Basis for Public/Commercial Surveillance	Legitimate interest, Public interest task	Legitimate interest, Public task	Legitimate interest (no overriding interest), Performance of a task, Protection of life/health	Expectation of Privacy, Public Interest, Legitimate Interest, Consent
Consent Requirements (General/Voice)	Practically inapplicable in public/workplace environments.	Practically difficult in public places.	Practically difficult in public places.	One-party /All parties consent for audio (varies by state).
Transparency/ Information	Mandatory, clearly visible signs, detailed information.	Mandatory, clearly visible signs, purpose and contact details.	Mandatory, clearly visible signs about surveillance and data controller.	Signs are often used, but not always mandatory at federal level; varies by state.
Data minimisation/ Proportionality	Strict necessity, purpose limitation, respect for human dignity.	Adequate, relevant, limited to what is necessary.	Consideration of necessary and proportionate, less invasive means.	Must be proportionate to security needs, not overly intrusive.
DPIA Requirement	Mandatory in cases of high risk (e.g. biometrics, large-scale surveillance).	Mandatory in high-risk situations (e.g. biometrics).	Mandatory in high-risk situations (e.g. large-scale public surveillance, biometrics).	No general federal requirement, but recommended in high-risk situations.
Data storage (Typical/Guideline)	Purpose-specific, regular deletion (e.g. until the end of proceedings in the case of criminal offences).	Purpose-specific (typically 30 days, except for investigations).	Purpose-specific, immediate deletion when no longer necessary.	Purpose-bound, secure storage, no longer than necessary.
Biometric/Facial Recognition Specifics	Special category data, stricter conditions, EU AI Act conflict.	Special category data (GDPR Article 9), additional conditions under DPA 2018.	Special category data, stricter conditions, protection of assembly rights.	No comprehensive federal law, regulations vary from state to state.
Supervisory/ Enforcement Body	NAIH (National Authority for Data Protection and Freedom of Information).	ICO (Information Commissioner's Office).	Provincial data protection authorities (Länder).	Federal/state courts and agencies (e.g. FTC).

Note. Edited by the authors.

Practical applications and implementation differences

Public sector applications: Law enforcement, urban planning, traffic management

CCTV systems are widely deployed to prevent crime and enhance public safety. In Hungary, the police are authorised to operate cameras in public areas for

the purposes of crime prevention and detection, as well as for the prosecution of offences.

Video surveillance data, especially when augmented with video content analytics, provides valuable information in areas beyond public safety. Cameras monitor traffic flow, detect incidents, and optimize traffic light control to reduce congestion. They can identify cycle paths or pedestrian routes, assisting at pedestrian crossings. Video analytics data assists in the assessment and development of urban infrastructure and even in environmental monitoring.

This creates a 'dual-use' dilemma, where systems installed for security purposes can be easily repurposed for broader urban management purposes, potentially leading to 'function creep' and raising new privacy concerns.

Cameras are capable of 'patrolling' multiple areas without the need to deploy numerous security guards or police officers, thereby reducing the need for human labour in certain surveillance tasks.

The integration of CCTV with AI, the Internet of Things (IoT) and data analytics is the cornerstone of 'smart city' initiatives. These technologies promise efficiency in traffic, waste management and public safety. This creates a strong incentive for governments to expand surveillance infrastructure, potentially prioritising efficiency over individual privacy rights if not carefully balanced.

Private sector application: Retail

CCTV became commonplace in banks in the mid-1980s and in shops in the 1990s. Modern retail utilize video analytics to improve store layout, optimise customer flow (via heat maps, dwell time, queue length), manage staff and reduce losses. AI algorithms are used to analyze and optimise marketing strategies, facilitating the rise of unmanned shops, which rely heavily on AI capabilities.

Efficiency, ethical considerations and social impact

International research shows mixed results regarding the crime prevention effects of CCTV. Some studies suggest that cameras reduce the number of certain crimes (e.g. vehicle-related offences), while in other cases they tend to cause a geographical displacement of crime (Welsh & Farrington, 2004). At the same time, the systems are undoubtedly useful as investigative tools: the recordings serve as evidence, facilitate the identification of suspects and increase the efficiency of proceedings.

From an ethical point of view, the consistent application of the principles of purpose limitation and proportionality is of paramount importance. Recordings

with an overly wide angle of view or stored for an unreasonably long period of time violate the requirement of data minimization, a point regularly emphasised in NAIH decisions (e.g. NAIH/2019/6865/2).

New technologies raise further ethical dilemmas. The proven biases of algorithms and the risk of discrimination (Wachter, Mittelstadt & Floridi, 2017) suggest that the use of these systems is only acceptable under strict safeguards. From the point of view of social trust, it is important that surveillance does not become a source of the 'Big Brother syndrome' (Bak, et al., 2023; Lyon, 2018), which can lead to self-censorship and a decline in civic participation.

According to data from a 2000 study conducted by the Ministry of the Interior, 64 per cent of citizens consider the operation of surveillance systems to be useful, with 40 per cent considering it to be very appropriate (Horváth, 2006).

Findings and recommendations

Main findings

- The development of CCTV technology consistently outpaces legislation, resulting in regulatory delays.
- In addition to the common principles of Hungarian and international legal frameworks (transparency, data minimization, proportionality), there are significant differences in the handling of biometric data and facial recognition.
- The impact of cameras on crime prevention is not uniform; their role is strongest in investigation and evidence gathering.
- The phenomenon of ‚function creep' creates new ethical risks.
- The psychological effects of pervasive surveillance (e.g., self-censorship, erosion of trust) may also affect democratic participation in the longer term.
- The cyber security vulnerabilities of these systems can have serious financial and legal consequences.
- In non-official practical use, regulatory boundaries are blurred, partly due to lack of knowledge and partly due to necessary requirements, resulting in a significant gap between practice and regulation.

Recommendations

For regulation:

- Proactive, forward-looking legislation is needed to regulate AI and biometric technologies at a harmonised EU level.

- The role of supervisory bodies such as the NAIH should be strengthened, with clear guidelines on the practical interpretation of legitimate interest and proportionality.
- Human rights impact assessments (HRIA) could be made mandatory for high-risk systems.

For practitioners:
- Integration of data protection into design and consistent application of the principle of data minimization.
- Enhanced technical and organisational cybersecurity measures (encryption, access restrictions, regular audits).
- Transparent, understandable information for data subjects to maintain trust.

For research:
- Long-term, comparative studies are needed on the actual effectiveness of CCTV in different environments.
- Developing new methods for detecting and reducing algorithmic bias is crucial.
- Social science research is needed to explore psychological and democratic effects.

Concluding thoughts

Surveillance cameras have become a fundamental infrastructure for public safety, city management and commerce. Although their effectiveness is debatable, they have proven value in investigations and in enhancing the subjective sense of safety. At the same time, the gap between technological development and legal regulation, as well as ethical dilemmas (data protection, dignity, discrimination) continue to raise new questions. One of the key questions for the future is whether society will be able to maintain a balance between security and civil liberties.

References

Bak, G., Őszi, A., & Kovács, T. (2023). The assessment of biometric identification – Part 2. *Hadmérnök*, 18(1), 5–16. http://doi.org/10.32567/hm.2023.1.1

Baumgartner, H., & Őszi, A. (2024). Artificial Intelligence in Crime Prevention and Counterterrorism. *Security Science Review,* 6(3), 115–125. https://biztonsagtudomanyi.szemle.uni-obuda.hu/index.php/home/article/view/476/381

Cabanillas Carbonell, M., Sallari Rivera, J., & Santivañez Muñoz, J. (2025). Artificial intelligence in video surveillance systems for suspicious activity detection and incident response: A systematic review. *Advances in Science and Technology Research Journal, 19*(3), 389–405. https://doi.org/10.12913/22998624/196795

Cabrera, L. L. (2024, 30 April). *Eu Ai Act Brief – pt. 2, Privacy & Surveillance*. Centre for Democracy and Technology. https://cdt.org/insights/eu-ai-act-brief-pt-2-privacy-surveillance/

David, L. (2018). The Culture of Surveillance: Watching as a Way of Life. *Poltity*.

Horváth, Zs. (2008). Police camera surveillance in Hungary – Must we choose between public safety and human rights? In Smuk, P. (Ed.), *Optimi Nostri: Award-winning Scientific Student Theses, 2007* (pp. 120–151). Universitas-Győr.

Kalluri, P. R., Agnew, W., Cheng, M., Owens, K., Soldaini, L., & Birhane, A. (2023). *The Surveillance AI Pipeline.* ArXiv. https://doi.org/10.48550/arXiv.2309.15084

Kardos, Pál. (2025). *Legal regulation* of *civil defence. Belügyi Szemle, 73*(1), 45-61. DOI: 10.38146/BSZ-AJIA.2025.v73.i1.pp45-61. belugyiszemlejournal.org+2

Laufs, J., & Borrion, H. (2021). Technological innovation in policing and crime prevention: Practitioner perspectives from London. *International Journal of Police Science & Management, 24*(2), 190-209. https://doi.org/10.1177/14613557211064053

Salgado, N., Meza, J., Vaca-Cárdenas, M., & Vaca-Cárdenas, L. (2024). Current and emerging trends in the use of AI for community surveillance. *Journal of Infrastructure, Policy and Development, 8*(8), 6135. https://doi.org/10.24294/jipd.v8i8.6135

Som, Z. (2017). CCTV systems from an interoperability and information security perspective. *Magyar rendészet, 17*(2), 159-171. https://folyoirat.ludovika.hu/index.php/magyrend/article/view/1969/1254

Tóth, L. (2022). *Opportunities for improving the efficiency of video surveillance systems in the field of public space surveillance. Doctoral thesis, Óbuda University.* https://bdi.uni-obuda.hu/wp-content/uploads/2023/06/Doktori-PhD-ertekezestervezet-Toth-Levente.pdf

Ujhegyi, P., & Őszi, A. (2025). The relationship between biometric identification and AI, and its risk assessment possibilities. *Belügyi Szemle, 73*(5), 977-999. http://doi.org/10.38146/BSZ-AJIA.2025.v73.i5.pp977-999

Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a Right to Explanation of Automated Decision-Making Does Not Exist in the General Data Protection Regulation. *International Data Privacy Law, 7*(2), 76–99. https://doi.org/10.1093/idpl/ipx005

Welsh, B. & Farrington, D. (2004). Evidence-based crime prevention: The effectiveness of CCTV. *Crime Prevention and Community Safety, 6*(2), 21-33. https://doi.org/10.1057/palgrave.cpcs.8140184

Applied administrative decisions

National Authority for Data Protection and Freedom of Information (2019). Decision No. NAIH/2019/6865/2.
National Authority for Data Protection and Freedom of Information. (2019). Decision No. NAIH 2019/5421/5.
National Authority for Data Protection and Freedom of Information. (2019). Decision No. NAIH 5896-1/2021.
National Authority for Data Protection and Freedom of Information (2020). Decision No. NAIH/2020/1163/6.
National Authority for Data Protection and Freedom of Information. (2020). Decision No. NAIH 2020/2729/15.

Applicable legislation

Act XXXIV of 1994 on the Police.
Act CXXXIII of 2005 on the Rules of Private Investigation Activities.
Act CXII of 2011 on the Right of Informational Self-Determination and Freedom of Information.
Act V of 2013 on the Civil Code.
California Consumer Privacy Act (CCPA) / *California Privacy Rights Act* (CPRA). Cal. Civ. Code §§ 1798.100–1798.199 (2018, módosítva 2020).
California Penal Code § 632.
Children's Online Privacy Protection Act (COPPA) of 1998. 15 U.S.C. §§ 6501–6506.
Deutschland (2018): *Bundesdatenschutzgesetz (BDSG)*. BGBl. I S. 2097.
Electronic Communications Privacy Act (ECPA) of 1986. Pub. L. 99–508, 100 Stat. 1848 (1986).
Freie und Hansestadt Hamburg (2019): *Gesetz über die Datenverarbeitung der Polizei (PolDVG HH)*. HmbGVBl. 2019, S. 233.
Freistaat Bayern (2018): *Polizeiaufgabengesetz (PAG)*. GVBl. 2018, S. 302.
Georgia Code O.C.G.A. § 16-11-62.
Health Insurance Portability and Accountability Act (HIPAA) of 1996. Pub. L. 104–191, 110 Stat. 1936 (1996).
Information Commissioner's Office (ICO) (2015). *CCTV Code of Practice.*
Information Commissioner's Office (ICO) (é. n.). *Data Protection Impact Assessments (DPIAs) – Guidance.*
Information Commissioner's Office (ICO) (é. n.). *Home CCTV Systems – Guidance for the Public.*
Katz v. United States, 389 United States Reports 347 (1967).
Land Baden-Württemberg (2020): *Polizeigesetz (PolG BW)*. GBl. 2020, S. 885.
Land Berlin (2021): *Allgemeines Sicherheits- und Ordnungsgesetz (ASOG Bln)*. GVBl. 2021, S. 842.

Land Nordrhein-Westfalen (2021): *Polizeigesetz (PolG NRW)*. GV. NRW. 2021, S. 990.
New York Penal Law Article 250.
Texas Penal Code § 16.02.
United Kingdom (2012*): Protection of Freedoms Act 2012*. London: The Stationery Office.
United Kingdom (2018): *Data Protection Act 2018*. London: The Stationery Office.
Video Voyeurism Prevention Act of 2004. Pub. L. 108–495, 118 Stat. 3999 (2004).
Virginia Consumer Data Protection Act (CDPA). Va. Code Ann. §§ 59.1–575–59.1–584 (2021).
Wiretap Act (Omnibus Crime Control and Safe Streets Act of 1968, Title III). Pub. L. 90–351, 82 Stat. 197 (1968).

Reference of the article according to APA regulations

Steiner, A. (2026). The Use of Surveillance Cameras, Legal Framework and Practical Differences: Scientific Research. *Belügyi Szemle*, *74*(4), 1081–1097. https://doi.org/10.38146/BSZ-AJIA.2026.v74.i4.pp1081-1097

Statements

Conflict of interest

The author has declared no conflicts of interest.

Funding

The author has received no financial support for the research, authorship, and/or publica-tion of this article.

Ethics

No dataset is associated with this article.

Corresponding author

The corresponding author of the article is Attila Steiner, who can be contacted at steinerattila70@gmail.com