

ARMED SECURITY GUARDS IN HUNGARY: HISTORICAL DEVELOPMENT, LEGAL FRAMEWORK AND OPERATIONAL CHALLENGES

Violetta Rottler¹, PhD

Vince Vári, PhD

Ludovika University of Public Service, Faculty of Law Enforcement, Hungary

ABSTRACT

Objective: The objective of this study is to present the institution of armed security guards (ASGs) in Hungary, to trace its historical development, examine the evolution of protected assets and facilities, and analyze the legal, organizational, and technological framework that defines its operation. Special attention is given to the role of ASGs in the protection of critical infrastructure, public utilities, and other facilities of strategic importance to the functioning of the state.

Approach: The paper applies a descriptive and analytical approach. It relies on Hungarian and international academic literature, statutory regulations, and professional guidelines related to law enforcement, risk-based security, and critical infrastructure protection. Technological development is examined in direct relation to the operational tasks performed by armed security guards.

Findings: The analysis shows that armed security guards constitute a unique hybrid institution within the Hungarian security system. Although they operate under civilian employment conditions, they perform public security tasks requiring the lawful use of force and advanced security technologies. Their effectiveness depends on the coordinated operation of manpower, legal regulation, and integrated technical protection systems.

Value: The study highlights the need for legislative modernization, coherent training and continuing education systems, and sustainable financing models. It also emphasizes the importance of civilian control, transparency, and accountability in maintaining legitimacy and public trust in ASG operations.

Keywords: armed security guards; public safety; critical infrastructure protection; risk-based security; resilience of critical organizations

About the authors

Violetta Rottler, PhD, pol. major, is an adjunct professor at the Ludovika University of Public Service, Faculty of Law Enforcement, Department of Private Security and Municipal Policing, Budapest, Hungary.

Vince Vári, PhD, pol. lt. col., is an associate professor at the Ludovika University of Public Service, Faculty of Law Enforcement, Department of Criminal Procedure Law, Budapest, Hungary. E-mail: vari.vince@uni-nke.hu

¹ rottler.violetta@unu-nke.hu



INTRODUCTION

Security is a social product and a fundamental necessity for both society and the individual. According to Finszter, danger is exclusively a threat that attacks socially protected values, and its origin may be natural, technological, or intentional human activity (Finszter, 2010). Absolute security does not exist; accordingly, the objective of security policy is to reduce risks to an acceptable level through legal, organizational, and technical measures.

The historical development of the Hungarian private security sector provides an important context for understanding the later emergence of armed security guards. As demonstrated by Rottler and Kovács (2022), the evolution of private security in Hungary was shaped by both facilitating and constraining regulatory factors. While statutory regulation was necessary to ensure legality and professionalism, early regulatory frameworks also revealed tensions between effective state oversight and operational viability. This historical dynamic highlights how state regulation has continuously defined the boundaries between public and private security functions, within which the institution of armed security guards later developed as a distinct, state-supervised form of security provision.

Every state has a fundamental interest in protecting state functions, public welfare, irreplaceable cultural heritage, and assets vital to national defense, national security, and law enforcement. Traditionally, these protection tasks have been carried out by the police and the armed forces. In Hungary, however, a specific solution has evolved: armed security guards perform armed protection tasks while remaining outside the system of state law enforcement bodies, thus occupying a special position within the national security architecture.

Certain sectors, such as nuclear energy and international air transport, are governed by international regulatory frameworks that prescribe minimum protection requirements. Within these sectors, national authorities retain responsibility for determining the organizational form of protection. The Hungarian armed security guard system thus represents a nationally specific and unique institutional response embedded in an international regulatory environment, rather than an isolated domestic solution.

THEORETICAL AND CONCEPTUAL FRAMEWORK

The functioning of armed security guards can be interpreted within the framework of risk-based security and critical infrastructure protection. Risk-based approaches focus on the identification of threats, the assessment of probabilities and consequences, and the proportional allocation of protective resources (Kaplan & Garrick, 1981; Aven, 2016).

Critical infrastructure protection aims at safeguarding assets whose disruption would have severe consequences for societal functioning, public safety, or national security (Rinaldi, Peerenboom, & Kelly, 2001). These concepts are complemented by the notion of civilian control, which emphasizes transparency, accountability, and democratic oversight over organizations authorized to apply coercive measures (Loader & Walker, 2007; Prenzler & Ronken, 2001).

HISTORICAL DEVELOPMENT OF ARMED SECURITY GUARDS IN HUNGARY

The roots of organized civilian guarding in Hungary date back to the civil guards established in 1914. These organizations operated nationwide on the basis of uniform rules and procedures, and their activities were strictly bound by law and official instructions (Christián, 2022).



The institutionalized protection of industrial and public service facilities was established through the creation of the Industrial Guard in 1953. Operating under the control of the Ministry of the Interior, the Industrial Guard provided armed protection for nationalized large companies, transport systems, and energy facilities (Szigeti, 2025).

By the 1960s, the Industrial Guard developed into a nationwide organization and was unified under the designation of a civilian armed guard. Following the political transition of the 1990s, the role and legal basis of civilian armed guarding were fundamentally transformed, culminating in the adoption of Act CLIX of 1997 and its implementing regulation, Decree 27/1998 (VI. 10.) BM.

LEGAL AND ORGANIZATIONAL FRAMEWORK

The establishment of armed security guards is decided by the police, while the obligation to finance their operation is imposed on the owners or operators of the protected facilities. Originally, only the police were authorized to order armed security protection; since 2011, this competence has been extended to heads of relevant ministries.

More recently, a government decree adopted in 2024 introduced additional provisions concerning the issuance of special personal and property protection certificates, further strengthening centralized risk assessment and regulatory control in the ASG system.

This regulatory logic is consistent with earlier developments in the Hungarian private security sector. As Rottler and Kovács (2022) emphasize, the first statutory-level regulations of private security were designed to delineate clearly the boundaries of permissible activities while preserving effective state oversight. These early regulatory dilemmas continue to resonate in the legal framework governing armed security guards, particularly regarding licensing, supervision, and the balance between public authority and private operation.

Armed security guards are employees subject to Act I of 2012 on the Labor Code (Mt.), which clearly distinguishes them from state law enforcement officers. Interpretative challenges arise from the overlapping provisions of criminal procedure law, misdemeanor law, and the Act on Personal and Property Protection (Be., 2017; Szabs. tv., 2012; Szvmt., 2005).

These interpretative challenges are particularly relevant in operational situations involving apprehension and detention. While criminal procedure law permits any person to apprehend an offender caught in the act, misdemeanor legislation and personal and property protection law establish additional procedural obligations regarding proportionality, necessity, and immediate handover to police authorities (Be., 2017; Szabs. tv., 2012; Szvmt., 2005).

In ASG-protected facilities, this legal complexity may result in uncertainty regarding the scope of permissible action. Consequently, clear internal protocols, continuous legal training, and close cooperation with the police are indispensable to ensure lawful and effective intervention by armed security guards.

CHALLENGES, RISKS AND CIVILIAN CONTROL

In recent years, the scope of tasks and competencies assigned to armed security guards has expanded beyond traditional facility protection. ASGs are to an increasing extent involved in the protection of correctional facilities, border-related infrastructure, and immigration detention centers, where elevated security risks and the potential for violent incidents require enhanced preparedness and clearly defined operational powers.



This expansion reflects broader changes in the security environment, including migration-related pressures and the growing need to protect state-managed facilities that operate under exceptional legal regimes. In these contexts, armed security guards often perform tasks that closely resemble those of sworn law enforcement officers, while remaining subject to civilian employment status and labor law.

The widening of ASG responsibilities also raises questions regarding professional preparedness and equipment. Previous professional experience indicates that the effectiveness of armed security guards in high-risk environments is closely linked to structured command training, regular continuing education, and access to appropriate non-lethal and, where justified, automatic or semi-automatic firearms (Szigeti, 2022).

From an organizational perspective, the introduction of standardized 'unit set' equipment concepts, similar to those applied in police services, may enhance operational flexibility. Such arrangements allow on-duty shifts to deploy reinforced armament when justified by risk assessment, while maintaining proportionality and legal compliance.

The long-term operation of armed security guards presents organizational, financial, and human resource challenges. Operators bear responsibility for maintenance costs, continuous training, and the provision of appropriate technical resources (IAEA, 2016; IAEA, 2021).

Civilian control represents a key element of legitimacy for organizations exercising coercive powers. In the case of armed security guards, civilian oversight mechanisms, public reporting, and complaint procedures enhance transparency and accountability (Vári, 2020a; Vári, 2020b).

From a historical perspective, the importance of civilian control in security governance has already been highlighted in private security regulation. Rottler and Kovács (2022) point out that insufficient transparency and weak oversight mechanisms in the early phases of private security development posed risks to legitimacy and public trust. These lessons are directly applicable to the contemporary operation of armed security guards, where civilian oversight remains a crucial safeguard against the misuse of coercive powers.

OPERATIONAL ENVIRONMENT AND TECHNOLOGICAL DEVELOPMENT

The scope of facilities protected by armed security guards includes objects of national defense, national security, nuclear facilities, public utilities, assets of cultural importance, as well as central telecommunications and broadcasting facilities. In the 2010s, critical infrastructure protection requirements, particularly in the nuclear sector, significantly expanded protection obligations (Government Decree 190/2011; OAH, 2022; Act LXXXIV of 2024).

In addition to classic mechanical security elements, integrated electronic security systems play an increasingly important role. Access control, intrusion detection, video surveillance, fire alarm and extinguishing systems, and centralized monitoring platforms form the backbone of modern facility protection (Tóth, 2023a).

Criminological research confirms the deterrent effect of video surveillance, especially when cameras are clearly visible, monitored in real time, and integrated with active intervention mechanisms (Gill & Spriggs, 2005; Welsh & Farrington, 2008; Vári et al., 2025).



At the same time, the extensive use of surveillance technologies raises data protection and privacy concerns. In the ASG environment, compliance with purpose limitation, data minimization, and transparency requirements is essential, in accordance with European data protection guidelines (EDPB, 2020).

The operational effectiveness of armed security guards is to an increasing extent determined by the integration of technological solutions into everyday guarding activities. Unlike purely private security services, ASGs operate in environments where the protection of state interests, critical infrastructure, and public services requires a higher level of reliability, continuous operation, and regulatory compliance.

In the Hungarian system, armed security guards are typically responsible for facilities where technological failure or malicious interference (sabotage) could result in severe societal consequences. These include nuclear facilities, drinking water supply systems, energy infrastructure, transport hubs, and healthcare institutions (Government Decree 190/2011; OAH, 2022; Act LXXXIV of 2024). Accordingly, technological protection measures used by ASGs must support uninterrupted operation, rapid detection, and immediate intervention.

Beyond traditional mechanical protection, modern ASG-supported facility security relies on integrated electronic security systems. Access control and identification systems regulate the movement of personnel and vehicles within protected areas, while intrusion detection systems provide early warning against unauthorized access. These systems are particularly important in ASG-protected facilities, as they allow armed guards to concentrate their physical presence at critical points rather than performing continuous patrols over large areas (Tóth, 2023a).

Video surveillance systems (CCTV) represent a core technological tool in the operational practice of armed security guards. Experience in facility protection shows that CCTV does not function as a stand-alone security solution, but significantly increases effectiveness when combined with trained personnel and clearly defined response protocols (Gill & Spriggs, 2005; Welsh & Farrington, 2008). In ASG environments, cameras support situational awareness, incident reconstruction, and evidence preservation.

Based on experience in facility security and public-space surveillance, CCTV represents a key element of physical and technical protection as part of electronic alarm systems. While CCTV alone does not provide complete protection, its preventive and deterrent effects have been empirically demonstrated (Tóth, 2023a). The effectiveness of surveillance systems depends significantly on the targeted training of operators and is statistically correlated with operators' employment status, gender, and age; purpose-oriented training produces measurable improvements in performance (Tóth, 2023b).

Both international and domestic research indicates that surveillance systems are most effective when detection is followed by immediate, 'active intervention'. This approach increases the success rate of responses, particularly in cases of violent crime, while crime-related effects are not merely displaced but often diffusely reduced in surrounding areas as well. An evaluation framework can be developed to measure and compare effectiveness, supporting not only operational audits but also security planning and system design.

With the rapid proliferation of security technologies, the 'price of convenience' is that previously visible control points may become 'invisible' risks. Consequently, in layered facility protection the balance between user convenience and the visibility of surveillance must be consciously designed (e.g. camera markings, warning signs, access logging). In the ASG environment, this necessitates enhanced transparency requirements, including purpose limitation, data minimization, defined retention periods, and, where required, data protection impact assessments (DPIA), in line with legal and ethical standards applicable to public video surveillance (EDPB, 2020).

In practical terms, this entails the integration of 'privacy by design' and 'privacy by default' principles, public information measures and camera maps, as well as strict role- and access-management proce-



dures in the operation of CCTV and access control systems, particularly at critical entities. Camera networks optimized primarily for convenience but deployed sporadically or integrated poorly carry a higher risk of function creep and loss of public trust; accordingly, real-time operation, lawful information provision, and regular audits constitute prerequisites for both effectiveness and social acceptance.

The effectiveness of surveillance systems has also been confirmed by criminological research. Based on a questionnaire survey conducted within a prison population, the deterrent effect of CCTV was found to be comparable to the presence of uniformed police officers, particularly when cameras were clearly visible, monitored in real time, and integrated with police patrol activity ($n=172$; 76% vs. 74% 'maximum' deterrent effect) (Vári et al., 2025).

In the same study, 82% of respondents indicated that cameras installed in public spaces would deter criminal activity, while 81% believed that even a clearly visible CCTV warning sign has a preventive effect. Overall, 83% attributed a crime-preventive impact to surveillance systems. At the same time, a negative correlation was identified between time spent in detention and fear induced by cameras, suggesting that the longer an individual had been incarcerated, the less they were influenced by the mere presence of CCTV. This finding supports the need for targeted, risk-based interventions. Consistent with international evidence, the magnitude of the effect is highly dependent on location and type of crime: reductions are particularly notable in property crime, whereas sporadic and non-integrated deployment may lead to territorial displacement. The combination of real-time surveillance and police presence yields the most substantial results (Vári et al., 2025).

Empirical research confirms the deterrent effect of surveillance systems when operated under conditions relevant to ASG work. Hungarian criminological studies indicate that visible, real-time monitored cameras can produce a deterrent effect comparable to that of uniformed police officers (Vári et al., 2025).

The integration of video analytics and behavioral analysis further enhances ASG capabilities, but requires strict compliance with data protection principles, including purpose limitation, proportionality, and data minimization (EDPB, 2020).

Cyber-physical convergence also shapes the technological environment of armed security guards. The integration of physical security systems with IT and OT creates new vulnerabilities that must be addressed through network segmentation, logging, and continuous monitoring (NIST, 2023; Humayed et al., 2017).

Due to cyber-physical convergence, the operational environment of armed security guards to an increasing extent includes cybersecurity considerations. In ASG-protected facilities, physical security systems such as CCTV, access control, and intrusion detection are often integrated with information technology (IT) and operational technology (OT) networks. This integration improves efficiency and situational awareness, but simultaneously introduces new vulnerabilities that require risk-based management approaches (IAEA, 2016; NIST, 2023).

International nuclear and critical infrastructure guidelines emphasize that IT/OT integration must be accompanied by network segmentation, hardening, logging, and continuous monitoring in accordance with the principle of defense in depth (IAEA, 2021; Humayed et al., 2017). For armed security guards, this means that effective physical protection can no longer be separated from cybersecurity awareness, as cyber incidents may directly compromise physical access controls and surveillance capabilities.

In high-risk sectors such as nuclear energy, international standards emphasize the principle of defense in depth, which requires the coordinated operation of human, organizational, and technological layers (IAEA, 2016; IAEA, 2021). Within this system, armed security guards represent the human layer supported by technological force multipliers.



CONCLUSIONS AND RECOMMENDATIONS

Beyond financing and operational challenges, the long-term development of the armed security guard system is closely linked to the issue of institutionalized interest representation. At present, armed security guards operate within a fragmented professional environment, where representation of interests, professional standards, and collective advocacy are limited and uneven.

International experience in the regulation of security professions shows that chamber-type organizations or statutory professional bodies can play a key role in balancing state oversight with professional autonomy. Such bodies typically contribute to the development of ethical standards, qualification requirements, and continuous professional education, while also serving as interlocutors between the state, employers, and practitioners.

In the Hungarian context, the introduction of a chamber-type model for armed security guards could enhance coherence within the sector. A centralized professional body could support the harmonization of training curricula, facilitate the dissemination of best practices, and contribute to the consistent interpretation of legal norms affecting ASG operations.

From the perspective of civilian control and accountability, institutionalized interest representation may also strengthen transparency. A chamber-type organization operating under statutory regulation could participate in complaint-handling mechanisms, professional audits, and disciplinary procedures, thereby reinforcing public trust in armed security guard activities.

Importantly, the establishment of such a body would not diminish state authority over the use of coercive measures. On the contrary, clearly defined professional representation could complement police and ministerial supervision by embedding compliance, training, and ethical considerations directly within the professional community.

Accordingly, the exploration of a chamber-type or hybrid interest representation model represents a potential avenue for future reform. By strengthening professional identity, supporting continuous development, and facilitating structured dialogue with the state, such a model could contribute to the sustainable evolution of the armed security guard system.

The financing of armed security guard operations represents one of the most sensitive and structurally challenging issues of the Hungarian ASG system. Under the current regulatory framework, the state defines the obligation to provide armed protection, while the financial burden of maintaining the guard is largely transferred to the owners or operators of the protected facilities.

This model reflects the legislator's intention to externalize the costs of protection to entities that directly benefit from enhanced security. However, in the case of facilities providing essential public services—such as drinking water supply, energy distribution, healthcare institutions, and other critical infrastructure—this approach raises questions of proportionality and state responsibility.

As highlighted in professional and academic discourse, the uninterrupted operation of critical services is a core state interest, regardless of the formal ownership structure of the operating entity. Consequently, the exclusive allocation of security costs to operators may place disproportionate financial pressure on organizations whose primary function is the provision of public services rather than profit generation (Szigeti, 2022).

In the context of drinking water supply, for example, security failures may have immediate and far-reaching consequences for public health and social stability. From this perspective, the protection of such facilities cannot be treated solely as a private operational matter, but must be understood as a component of public service continuity and national resilience.



International practice in the field of critical infrastructure protection to an increasing extent emphasizes shared responsibility models, where the state assumes a more active role in supporting the financing of security measures at facilities of strategic importance. Such support may take the form of direct subsidies, targeted grants, or co-financing schemes linked to compliance with enhanced security and resilience requirements.

In the Hungarian ASG system, the introduction of similar mechanisms could contribute to a more balanced distribution of responsibilities. State involvement in financing would not only alleviate the economic burden on operators, but also strengthen regulatory oversight, as financial support could be conditioned on compliance with professional, training, and transparency standards.

From a governance perspective, the question of financing is closely linked to the broader issue of public accountability. If armed security guards perform tasks that directly serve public safety and the protection of essential services, a purely market-based financing model may undermine long-term sustainability and strategic planning.

Accordingly, the reconsideration of financing arrangements represents a key element of future reform. A mixed model combining operator contributions with targeted state support could enhance the resilience of critical infrastructure, improve the professional standing of armed security guards, and better reflect the public interest nature of their tasks.

The Hungarian armed security guard system has undergone significant historical, legal, and technological development. Nevertheless, both the primary legislation and its implementing regulations require modernization to meet contemporary security challenges.

Taken together, these developments point toward a broader paradigm shift in security governance. Rather than focusing exclusively on static protection measures, contemporary ASG operations increasingly emphasize organizational learning, measurability of effectiveness, and multi-level responsibility systems. This shift aligns armed security guards with modern risk-based and resilience-oriented approaches to critical infrastructure protection.

From a professional perspective, the reform of education and training systems, the clarification of legal competencies, and the development of balanced financing solutions are essential. A coordinated, risk-based approach combined with transparent civilian oversight can ensure the long-term effectiveness of armed security guards in protecting critical infrastructure and public safety.

REFERENCES

- Act C of 2012 on the Criminal Code (Btk.) – Section 312.
Act CLIX of 1997 on armed security guards, nature conservation and field guard services. <https://njt.hu>
Act CXXXIII of 2005 on the rules governing personal and property protection and private investigation activities (Szvmt.).
Act I of 2012 on the Labor Code (Mt.).
Act II of 2012 on Misdemeanors, Misdemeanor Proceedings and the Misdemeanor Registration System (Szabs. tv.).
Act LXXXIV of 2024 on the resilience of critical organizations
Act XC of 2017 on Criminal Procedure (Be.) – Section 273.
Anderson, R., & Moore, T. (2006). The Economics of Information Security. *Science*, 314(5799), 610–613.



- Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. *European Journal of Operational Research*, 253(1), 1–13.
- Cherdantseva, Y., et al. (2016). A Review of Cyber Security Risk Assessment Methods for SCADA Systems. *Computers & Security*, 56, 1–27.
- EDPB. (2020). Guidelines 3/2019 on processing of personal data through video devices.
- Gill, M., & Spriggs, A. (2005). Assessing the Impact of CCTV.
- Hrudey, S. E., & Hrudey, E. J. (2014). Ensuring Safe Drinking Water.
- Humayed, A., et al. (2017). Cyber-Physical Systems Security—A Survey.
- IAEA. (2016). Computer Security at Nuclear Facilities.
- IAEA. (2021). Computer Security Techniques for Nuclear Facilities.
- Kaplan, S., & Garrick, B. J. (1981). On The Quantitative Definition of Risk.
- Loader, I., & Walker, N. (2007). Civilizing Security.
- NIST. (2023). SP 800-82 Rev. 3: Guide to Operational Technology (OT) Security.
- Prenzler, T., & Ronken, C. (2001). Models of Police Oversight.
- Rinaldi, S. M., et al. (2001). Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies.
- Cloud Security Alliance. (July 1, 2024). IT OT Convergence: Enhancing Security and Efficiency [Blog post].
- Decree 27/1998 (VI. 10.) BM on the issuance of the Operating and Service Regulations for armed security guards. <https://njt.hu>
- EU Directive 2022/2557 (Dec. 14, 2022) on enhancing the resilience of critical organizations
- European Data Protection Board. (January 30, 2020). Guidelines 3/2019 on processing of personal data through video devices (Version 2.0).
- Government Decree 190/2011 (IX. 19.) on physical protection in the context of the use of nuclear energy. <https://njt.hu>
- Hungarian Armed Security Guard Association. (n. d.). The history of the ASG. (Organizational summary).
- International Atomic Energy Agency. (2016). Computer Security at Nuclear Facilities (Nuclear Security Series No. 17).
- International Atomic Energy Agency. (2021). Computer Security Techniques for Nuclear Facilities.
- National Atomic Energy Agency (2022). FV guidelines (FV-2, FV-3, FV-4, FV-11, FV-18). <https://www.oah.hu>
- National Institute of Standards and Technology. (September 2023). SP 800 82 Rev. 3: Guide to Operational Technology (OT) Security (DOI: 10.6028/NIST.SP.800 82r3).
- OPSWAT & SANS Institute. (April 24, 2025). ICS/OT Cybersecurity Budgets Lag as Attacks Surge, Exposing Critical Infrastructure Risks [Report].
- OPSWAT: Cybersecurity (19 February 2025) What is IT/OT convergence? - OPSWAT
- Rottler, V., & Kovács, S. (2022). The Beginnings of Private Security and the Development of the Hungarian Private Security Sector up to the First Statutory-Level Regulation. *Belügyi Szemle*, 70(3), 539–558. <https://doi.org/10.38146/BSZ.2022.3.6>
- Szigeti, L. (15.04.2025) Head of the Hungarian Armed Security Guards Professional Association – presentation given at the Armed Security Guards professional conference, Balatonföldvár
- Szigeti, L. (2022) The role and tasks of armed security guards in protecting the capital's safe drinking water supply, Ludovika University of Public Service, Security Management MA thesis



- Tóth, L. (2023a). The role of video surveillance systems in increasing the efficiency of facility security. *Military Engineer*, 18(1), 99–113. <https://doi.org/10.32567/hm.2023.1.8>
- Tóth, L. (2023b). Opportunities for video surveillance systems to increase efficiency in the field of public space surveillance. PhD. Óbuda University
- Tóth, L. (2024). From visible friend to invisible enemy – The price of convenience. *Magyar Rendészet*, 24(2). Available at: [folyoirat.ludovika.hu/index.php/magyrend/article/view/7451/6032](https://www.folyoirat.ludovika.hu/index.php/magyrend/article/view/7451/6032).
- Vári, V. (2020b). The Civil Sphere, the State, and Law Enforcement. In IV. International Scientific Conference on Tourism and Security, Zalakaros, December 3, 2019. (pp. 29–40). REAL–MTAK publication.
- Vári, V. (2020a). Civilian Control of the Police: Difficulties and Opportunities. In Particular Concerning Hungary. In: Conference Proceedings, vol. 21, 51–60.
- Vári, V., Mátyás, S., Tihanyi, M., & Krasnova, K. (2025). CCTV and Crime Prevention Effectiveness: Experience of Hungary. *BRICS Law Journal*, 12(1), 40–55. <https://doi.org/10.21684/2412-2343-2025-12-1-40-55>.