DOI azonosító: https://doi.org/10.53304/PS.2026.1-2.07

KISFONAI, BERNADETT PATRÍCIA

Artificial Intelligence in Law Enforcement: International Experiences and Domestic Prospects

Introduction

Nowadays, the rapid growth of artificial intelligence (AI) is fundamentally transforming the operation of law enforcement agencies worldwide, including in Hungary. AI applications developed to support more efficient, faster and targeted task performance are increasingly popular. Still, in recent years, so-called predictive policing has received increasing attention, aiming to anticipate crimes and identify potential perpetrators by analysing existing data. Based on patterns inherent in police data, some systems can "predict" the expected location, time, or even the persons involved in crimes, enabling the police to intervene proactively. The specific goal of these systems was to optimise the deployment of already overburdened police forces in specific urban districts.

In addition to predictive analysis, AI also supports law enforcement through facial recognition, video analytics, automatic number plate recognition (ANPR), and digital forensics.

This study primarily examines complex networks, especially their effects on crime prevention, and supports these findings with international examples, thereby reinforcing the importance of systems. A relatively new research field in Hungary holds great potential, as network analysis can help us better understand crimes. AI is a particularly useful tool for uncovering hidden connections, and a deeper understanding of the complex network approach is not only scientifically interesting but also has practical significance for developing crime-prevention strategies.

The Predictive Policing and Network Approach

In the early stages of AI's development, it focused primarily on solving problems that, while intellectually challenging for humans, were relatively simple for computers—especially those that could be described formally, using mathematical rules. The real challenge, however, was the tasks that we humans perform instinctively, almost without thinking, but are difficult to codify into rules. Such tasks include recognising spoken words or faces—activities that we perform intuitively yet are extremely difficult to model at the machine level.[1] Based on this approach, the essence of predictive policing is that the police use large amounts of data to predict and prevent crimes.[2] Analytical models have made it possible to model where and when an increased risk of crime is expected. Traditional predictive models focus more on spatial-temporal data. Still, the network approach, which analyses the relationships among offenders and other relevant actors to predict future crime, has increasingly become the focus of research.[3] The approach applies tools from complex network systems to law enforcement, seeking to leverage network research results to support crime prevention. However, crime does not occur in a vacuum; perpetrators, victims, and locations are often embedded in interconnected networks. Criminological research from the ROXANNE project also supports the fact that crimes and victimisations are not randomly distributed in either social or geographical space.[4] Understanding an individual's social connections can help predict

[1] Goodfellow, I. – Bengio, Y. – Courville, A.: Deep Learning. MIT Press. Cambridge, 2016. 15–20. o.

[2] Bezerédi, I.: Complex law enforcement AI policy: strategic and technological proposals from the perspective of ChatGPT and other LLMs. Law Enforcement Scientific Journal (Online), Issue 2024/1. 41–63. o.

[3] Link, S. N.: Social network analysis in predictive policing: concepts, models and methods. In: Social Network Analysis in Predictive Policing. Springer, 2016. 7–13. o.
Source: https://doi.org/10.1007/978-3-319-41492-8
Accessed: 19.07.2025

[4] ROXANNE Project (2021): Social network analysis for criminology in ROXANNE.

their future behaviour, movements, and risk of criminal activity. Mapping these relationships enables the reconstruction of broader networks of crime and victimisation. From a network research perspective, we look for patterns of connections – for example, networks of cooperation among criminals – but the analysis of complex networks reveals critical nodes. Network analysis has been shown to reveal common properties of connections and networks, thereby enhancing the predictability of criminal events. Below, we first review theoretical network concepts and models, then present some practical applications – international experiences and, finally, domestic opportunities – that fall within the scope of network-based predictive policing.

Network concepts in law enforcement

Complex network theory offers several concepts that are considered extremely useful for analysing crime data. First, centrality measures highlight which nodes (persons, locations) in a network are most influential. In law enforcement networks, high-centrality actors are typically individuals who maintain many connections, who function as intermediary bridges between others, or who are relatively close to other members of the network (closeness centrality).[5] The results of ROXANNE showed that, in a real investigation of an anonymous telephone network (based on 124 actors, 178 call/SMS connections), a few individuals played an exceptionally central

Source: https://www.roxanne-euproject.org/news/blog/social-network-analysis-for-criminology-in-roxanne
Accessed: 16.07.2025

[5] Johnson, J. – Reitzel, J. – Norwood, B. – McCoy, D. – Cummings, B. – Tate, R. R. (2013): Social network analysis: a systematic approach for investigating. FBI Law Enforcement Bulletin
Source: https://leb.fbi.gov/articles/featured-articles/social-network-analysis-a-systematic-approach-for-investigating
Accessed: 18.07.2015

role, suggesting they may be the network's controllers or information centres.[6]

Community detection in network research identifies groups of nodes whose members are more closely connected than to the rest of the network.[7] Network analysis can reveal, for example, if there are actually distinct groups within a seemingly dispersed set of offenders.

However, we can discuss the scale-independent properties of many real-world networks, including social and potentially criminal networks. According to the theory, a few nodes have unusually high numbers of connections, while the majority have few, so that, mathematically, their degree distribution approaches a power law.[8] In criminal networks, this means there are often "hub actors" connected to many other offenders, while most offenders have few points of connection.

Finally, dynamic graph models should be mentioned, meaning that criminal networks are not static; their connections are always changing. New actors can enter, old ones can drop out. A dynamic network model can help deal with changes over time[9]. The link prediction method is the best example of this, as they try to model which two actors are expected to

[6] ROXANNE Project (2021): i.m.

[7] Yang, J. – Leskovec, J.: Overlapping community detection at scale: a nonnegative matrix factorization approach. In: Proceedings of the Sixth ACM International Conference on Web Search and Data Mining. ACM, 2013. 587–596. o.
Source: https://doi.org/10.1145/2433396.2433471
Accessed: 19.07.2025

[8] Xu, J. – Chen, H.: The topology of dark networks. Communications of the ACM, Issue 2008/10. 58–65. o.
Source: https://doi.org/10.1145/1400181.140019
Accessed: 19.07.2025

[9] Yang, C.: CrimeGraphNet: link prediction in criminal networks with graph convolutional networks. arXiv. 2023.
Source: https://doi.org/10.48550/arXiv.2311.18543
Accessed: 19.07.2025

form a connection within the network in the future.[10] Another aspect of dynamic networks is real-time analysis, meaning modern systems strive to detect changes in the network by working with constantly updated data.[11]

Complex network systems in crime prevention

Building upon the theoretical concepts outlined above, this section explores how various network systems are applied in crime prevention. Based on the above, it can be concluded that the applicable networks are extremely diverse; essentially, any system in which relationships or interactions connect elements falls within this classification. Social networks are the most obvious application area in crime prevention. It has long been known in criminology that offenders often act in groups and in pairs; the so-called co-offending networks are also often active.[12] Social networks, in a broader sense, also include networks of friends, relatives, and acquaintances. Whether a person becomes a criminal or a victim can be greatly influenced by their environment.[13] A pilot program in Chicago, US, became known as the Strategic Persons List. It was a person-based predictive model that assigned people a score based on their likelihood of being perpetrators or victims of serious crimes.[14] However, such an approach is susceptible to false alarms

[10] Al Hasan, M. – Zaki, M.: A survey of link prediction in social networks. In: Aggarwal, C. C. (ed.): Social Network Data Analytics. Springer, 2011. 243–275. o.
Source: https://doi.org/10.1007/978-1-4419-8462-3_9
Accessed: 19.07.2025

[11] Of course, all this requires strong computational support and often the application of machine learning models. For example, graph neural networks can be used for predictive purposes; one experimental model is CrimeGAT, which applies such techniques to make predictions in criminal networks (Yang, 2023).

[12] Di Méo, G.: Historical co-offending networks: a social network analysis approach. The British Journal of Criminology, Issue 2023/6. 1591–1611. o.
Source: https://doi.org/10.1093/bjc/azad057
Accessed: 19.07.2025

[13] Di Méo (2023): 1604. o.

[14] 5 Peteranderl, S.: Under fire: the rise and fall of predictive policing. American Council on Germany. 2019.

and ethical issues – the Chicago "heat list" program was ultimately criticised. Nevertheless, social network analysis is now standard practice in supporting investigations.

Telecommunications networks are extremely valuable to modern law enforcement, as they serve as maps of electronic communication between people (phone calls, SMS, and Internet messages). Since criminals often use these channels to communicate, graphs constructed from communication data can reveal the hidden structure of criminal organisations.[15] It is important to emphasise that the analysis of telecommunications networks also raises significant privacy and ethical issues. However, the raw technological opportunity is given. Urban transportation networks – such as road networks, public transport routes and human mobility systems – play a key role in the geographical distribution and spread of crime. The street network of cities can be interpreted as a graph in which the nodes are intersections and the edges are streets. Empirical research has shown that certain topological characteristics of the street network – such as throughput or centrality – correlate with crime frequency.[16] High-traffic routes and busy intersections with large numbers of people offer more opportunities for both random and planned crimes. In addition, perpetrators often take advantage of the easy access and quick escape routes of such places. New-generation predictive policing tools analyse the relationship between crime

Source: https://www.acgusa.org/wp-content/uploads/2020/03/2020_Predpol_Peteranderl_Kellen.pdf
Accessed: 19.07.2025

[15]Ferrara, E. – De Meo, P. – Catanese, S. – Fiumara, G.: Detecting criminal organizations in mobile phone networks. Expert Systems with Applications, Issue 2014/13. 5733–5750. o.
Source: https://doi.org/10.1016/j.eswa.2014.03.024
Accessed: 19.07.2025

[16] Mao, Y. – Huang, S. – Ning, Y. – Wang, C.: Unraveling the nexus: how street network morphology influences crime in Detroit. Humanities and Social Sciences Communications, Issue 2025/12. 981. o.
Source: https://doi.org/10.1057/s41599-025-01558-2
Accessed: 19.07.2025

and the road network in real time using geospatial data and are increasingly being used to predict traffic accidents.

In the field of road safety, Sweden provides an effective example, with around 2,200 fixed speed cameras operating nationwide that significantly contribute to compliance with speed limits, thereby reducing road accidents. In Hungary, amendments to the legal environment may be justified to allow for the expansion of the speed camera network – for example, by installing it more densely, introducing average speed measurement systems, and including smaller settlements. Stricter sanctions and a consistent police presence could be additional tools to encourage compliance.[17] In Sweden, the development of traffic culture is largely due to the conscious education of road users beginning in childhood: road safety education in schools has been a mandatory part of the basic curriculum since 1936. This long-term attitude formation has contributed to compliance with traffic rules becoming a social norm. It may also be worthwhile for Hungary to incorporate road safety knowledge into the school curriculum, from the basic rules of pedestrian and bicycle traffic to preparatory education for driving.[18]

Last but not least, a broader category of criminological relational networks can be highlighted, within which we can classify all networks exhibiting criminological connections. This could include, for example, networks of connections between crimes. Its analysis can help identify serial crimes and determine whether an event is connected across multiple networks. Europol uses such a network-based criminal intelligence analysis when it researches connections between cases in different countries (based on aspects such as weapons, car registration numbers, money movements,

[17] Lang-Fuksa, D.: Swedish road to transport safety. In: Bándi, G. – Pogácsás, A. (eds.): Law in the Service of the Sustainable Development Goals: Selected Doctoral Studies. Pázmány Press. Budapest, 2025. 143–158. o.
[18] Lang-Fuksa (2025): 145. o.

passport numbers).[19] In a broader sense, criminal knowledge graphs also belong here, because we understand them as a set of networked databases in which people, crimes, physical evidence, locations, and the relevant relationships among them are represented as "edges". Such graphs serve to support complex investigations. A special relational network is the criminal life-path network, in which the nodes are persons, and the edges do not represent a specific social relationship but rather some kind of criminological relation.

Network type	**Field of application**	**Examples**	**Advantages**	**Challenges**
Social networks	analysis of relationship systems (perpetrators, victims)	Chicago "heat list" program (Strategic Subject List)	Targeted prevention, identification of key actors, recognition of network patterns	Ethical issues, privacy concerns, false positives
Telecommunications networks	Analysis of phone calls, SMS, and online communication data	European ROXANNE project, mobile communication analysis of police investigations	Revealing hidden connections, real-time data analysis, and the possibility of rapid intervention	Serious data protection and ethical issues, risk of misuse of personal data

[19] Europol: Decoding the EU's most threatening criminal networks [Decoding the EU's Most Threatening Criminal Networks]. European Union Agency for Law Enforcement Cooperation. Luxembourg, 2024. 6–30. o.

Transportation networks	Analysis of urban road networks, public transport routes, geographic prediction of crimes, and increasing traffic safety	Swedish speed camera system, predictive GIS analyses	Precise identification of spatial hotspots, discovery of quick escape routes, linking accident and crime prevention	The need for legislative amendments, the cost, and the practical obstacles to network deployment
Criminological relational networks	Uncovering connections between crimes, supporting complex investigations	Europol crime analysis, criminal knowledge graphs, criminal life-course networks	Supporting complex investigations, effectively combating international crime, and identifying previously unnoticed connections	Complexity of data integration, emergence of false correlations, and handling large amounts of data

Table 1.
Comparison of network types used in law enforcement

Domestic situation and opportunities

In Hungary, predictive policing and network analysis are still in their early stages, but the interest is already palpable. Despite varying capacities, Hungarian police forces are beginning to explore how existing databases might be integrated into network-based predictive models. Future initiatives

within the Hungarian police could focus on launching pilot projects to explore the spatial dynamics of organised crime and vehicle-related offences. AI-based network analysis tools can help identify key players or explain why new transport routes may correlate with increased crime in a given area.

Future systems will also be affected by EU regulations, as the AI Act will strictly prohibit systems that score people based on personal data or past profiles. Finally, when examining the domestic opportunity, it is advisable to learn from international examples, which Hungary can use to develop a cautious yet smartly implemented network-based predictive policing model. The most effective approach combines human expertise with AI: while machines map networks and identify risks, final decisions remain with law enforcement professionals. The advantages of network analysis are effectively applied – such as better recognition of connections, faster data processing and proactive action – in crime prevention, while respecting the rule of law and ethical principles.

Conclusions

The application of AI to law enforcement carries both enormous promise and significant risk. The essence of the promise is that, for the first time, law enforcement agencies will have a tool that allows them to step out of their purely reactive role, improve city safety, and allocate resources more efficiently. This potential is also evident from international examples, as more and more countries and cities are experimenting with such systems to increase public safety. However, experience suggests that this technology is not a "magic wand" and, if used without supervision and control, it can become a tool for cementing prejudices. Whether it is about racial inequalities in American cities or the stop-and-search practice of the British police, AI is only as "smart" as the smart data it is fed with. The importance of algorithmic auditability and accountability should be emphasised.

Opaque “black box” AI solutions can undermine public trust and even the rule of law. The way forward is certainly to integrate AI into police work, but with human oversight and adherence to ethical standards. Innovation should be welcomed only if it does not violate fundamental rights and if democratic control over its use remains.

In conclusion, AI in the service of law enforcement is like a double-edged sword. While AI can be a powerful tool against crime, it must be wielded with caution to avoid unintended harm. International experiences offer abundant lessons that Hungary can draw on as well. The domestic opportunities are given, as we have the expertise and cautious openness to AI. The most important thing is that these technologies are introduced in the future in a responsible, transparent, and law-abiding manner. This is how artificial intelligence can truly enhance society's security without destroying its sense of justice. While AI is not a panacea, it can, if used wisely, become a valuable supporting tool for 21st-century law enforcement – both in Hungary and around the world.