

Predictive Policing: Recent Developments in Law, Criminology, and Technology

KISFONAI, BERNADETT*

ABSTRACT *Predictive policing uses data-driven tools and algorithms to anticipate crime risks and help police allocate resources more effectively. Although recent advances in artificial intelligence have made these systems more sophisticated, growing research highlights important legal and ethical concerns. Models built on historical arrest data can unintentionally reproduce existing biases, creating feedback loops that disproportionately impact marginalized communities. These risks have intensified calls for greater transparency, accountability, and stronger legal safeguards. International responses differ widely. Several U.S. cities have already banned or restricted predictive policing due to civil rights concerns, while the European Union's AI Act classifies such systems as "high-risk" and prohibits certain individual-level crime prediction models. Scholars increasingly stress the need to balance technological innovation with robust protections. Current research focuses on developing responsible frameworks – such as bias audits, human oversight, explainability, and community involvement – to ensure that predictive policing can enhance public safety without compromising fundamental rights.*

KEYWORDS *predictive policing, algorithmic crime forecasting, machine learning, civil rights, data protection (GDPR).*

1. Introduction

The use of data analytics is becoming increasingly popular, whether for predicting market conditions or industry trends or developing sales strategies. Police around the world can use data analytics to make their work more effective. The new direction is called “algorithmic crime forecasting,” and it is already believed in many areas that it can transform law enforcement by enabling police to anticipate and prevent crimes, rather than simply react to them afterwards. In November 2009, the National Institute of Justice, in partnership with the Office of Justice Programs (OJP) and the Los Angeles Police Department, held the Predictive Policing Symposium to discuss this emerging idea and its implications for the future of policing. Researchers, law enforcement officers, crime analysts,

* PhD student, University of Pécs, Faculty of Law, Doctoral School of Law.

and academics gathered in Los Angeles for three days to examine the policy implications, privacy issues, and technology of data-driven policing.

Predictive methods use data-driven analytics and algorithms to predict crime risk, allowing police to allocate resources more effectively. Over the past two decades, this approach has become a defining topic in police science internationally. Today, the development of artificial intelligence (AI) and machine learning has given new impetus to predictive models. Police Big Data analysis is becoming increasingly sophisticated, and many police departments – especially in the United States – have already used such algorithms to predict crimes, potential perpetrators, or even victims. In 2022, researchers at the University of Chicago presented a machine learning model that predicted crime in certain areas of the city a week in advance with about 90% accuracy.¹ In practice, most predictive systems analyze past crime patterns, with one of the best-known such software, namely PredPol, which was introduced in 2013 and maps out future crime hotspots and their expected timing. Similar predictive tools have been tested in several major US cities to support patrol planning. Predictive algorithms have also appeared in criminal justice: for example, in the US, the Public Safety Assessment (PSA) and COMPAS systems help judges by assigning a risk score of detainees based on a database of previous cases, on the ground of the likelihood of recidivism.

This study examines the development, legal framework, and ethical implications of predictive policing, highlighting international trends and their relevance to Hungary. In addition, the study seeks to assess the current Hungarian legal framework and identify potential areas for regulatory improvement. Moreover, the study applies a comparative legal and criminological approach, relying on international literature and EU legal documents.

2. The evolution of intelligence-led policing in the era of Big Data

Until the end of the 20th century, policing was typically reactive, meaning that crimes were responded to afterwards, and the focus of law enforcement was on investigating incidents that had already occurred. Starting in the 1990s, a turning point occurred with the emergence of the so-called intelligence-led policing (ILP).² The essence of ILP is that law enforcement agencies increasingly base their decisions on data analysis and intelligence information. A pioneering example of this is the “Kent model” applied in the county of Kent in England, where the police began to prioritize certain data signals (priority policing) in response to the increase in property crimes.³

¹ V. Rotaru et al., “Event-Level Prediction of Urban Crime Reveals a Signature of Enforcement Bias in U.S. Cities,” *Nature Human Behaviour* 6, no. 8 (2022): 1056–68, <https://doi.org/10.1038/s41562-022-01371-3>.

² Ferenc Szendrei, “Az Európai Bűnügyi Hírszerzési Modell,” *Rendőrségi Tanulmányok* 5, no. 1 (2022): 301.

³ Csaba Csapó, “A korszerű rendőrség alapjai,” *Pécsi Határőr Tudományos Közlemények* 10 (2009): 48.

The method allowed the police to focus on the most active criminal groups, which resulted in a significant reduction in the number of crimes and enabled more efficient use of resources.⁴ According to Jerry Ratcliffe's famous summary,⁵ the ILP strategy is based on four pillars: the police focus on repeat or active criminals, identify hot spot areas, connect extraordinary events based on information (recognizing crime patterns), and take the necessary crime prevention measures.⁶ The concept of ILP became particularly prominent after the terrorist attacks of September 11, 2001, as it highlighted the importance of better data sharing and analysis in the fight against terrorism.⁷ The European Union has also recognized the importance of this method, and subsequent EU security strategies emphasized improving access to cross-border police information or law enforcement authorities. While intelligence-led policing marked the first step towards proactive law enforcement, the rise of Big Data has taken this concept to a new, algorithm-driven level.

Entering the 21st century, digitalization and the era of Big Data have brought another change in the approach to law enforcement. Modern IT systems and the ever-increasing amount of data (e.g. criminal databases, surveillance camera footage, social media content) have made it possible for the police to operate in a far more data-centric manner.⁸ According to the literature, information collection and analysis are becoming a fundamental element of police work in maintaining future security, and the goal of proactive, intelligence-led policing is to seek the answer to the question "what will happen?" instead of the "what happened?" approach. This paradigm shift is embodied by the concept of data-driven policing, which builds on the crime statistics and analysis techniques of previous decades, but at the same time expands them, and attempts to predict future crimes.⁹ The essence of predictive policing is that it uses data from past crimes – primarily spatial and temporal patterns – to predict where and when new crimes may occur, thus enabling preventive police measures.¹⁰ The first such systems appeared in the USA in the late 1990s and proved to be partially successful in reducing crime. However, data protection and ethical concerns also arose at that time – for example, publicly available interactive crime maps may have contributed to the stigmatization of certain disadvantaged urban areas. The

⁴ Csapó, "A korszerű rendőrség alapjai," 48.

⁵ Jerry H. Ratcliffe, *Intelligence-Led Policing*. (Cullompton: Willan Publishing, 2008), 24–58.

⁶ Stephen L. Mallory, *The Concept of Asymmetrical Policing*, Working Paper Series No. 12 (Geneva: DCAF, 2007), accessed October 26, 2025, https://www.dcaf.ch/sites/default/files/publications/documents/WPS_No12_new.pdf.

⁷ Szendrei, "Az Európai Bűnügyi Hírszerzési Modell," 301.

⁸ Dorottya Lang-Fuksa, "Opportunities for Improving Road Safety," in *Collection of Papers: Law Between Protection and Abuse*, ed. Dimitrije Čeranić, Svjetlana, Ivanović, Đorđe Marilović, Radislav Lale, Samir Aličić (Faculty of Law, University of East Sarajevo, 2025), 358–73.

⁹ Attila Suhajda, "Néhány gondolat a prediktív rendészetről," *Rendőrségi Tanulmányok* 2, no. 3 (2019): 75–85.

¹⁰ Suhajda, "Néhány gondolat a prediktív rendészetről," 76.

challenge of the Big Data era is that the use of vast amounts of data leads to the creation of data-driven decision support systems, which, in addition to their effectiveness, also carry new hazards (e.g. erroneous conclusions, discriminatory profiling).¹¹

2. 1 Machine learning algorithms and data types in predictive systems

The operation of algorithmic crime forecasting systems is closely linked to modern machine-learning models, which are able to learn patterns from large amounts of historical data and indicate future risks. Machine learning is a subfield of artificial intelligence and allows a program to independently process data and learn from it. We distinguish three main learning paradigms: supervised learning, unsupervised learning and reinforcement. Supervised learning relies on labelled datasets, unsupervised detects hidden structures, while reinforcement learning optimizes actions based on feedback.

The types of data used by predictive systems are extremely diverse, as the more relevant information they integrate, the more accurate the predictions can be. Initially, the analyses relied mainly on historical crime statistics and the associated location-time data.¹² However, today many other data sources are also included.

Information related to the location (address, coordinates) and time (time, date, time of day) of each crime is essential. Hot spot maps and time series trends can be generated using GIS software. The temporal patterns of time series data (seasonal, holiday crime waves) can be analyzed using ARIMA and GARCH models to identify trends and seasonal effects.¹³

Predictive models often incorporate socioeconomic characteristics (population density, unemployment, income levels), infrastructural features (lighting, transport hubs), and contextual factors (weather, traffic). The data can help understand why a given area becomes risky. GIS-based analyses can combine geographic layers, showing that crime is more concentrated around certain urban spaces (undergrounds, parks).

More advanced predictive systems – individual risk-assessment models – also incorporate data about individuals. Such data can include previous arrests and convictions, criminal connections (known gang members), the person’s age, gender, and possible mental health problems. In the USA and some European countries (United Kingdom, Switzerland), there were programs that used person-based prediction, in addition, the Chicago Police Department’s “heat list” program compiled a list of several hundred people who, based on available data, could be suspected of being perpetrators or victims of gun violence in the near future.¹⁴

¹¹ János Sallai, “Bűnözésföldrajz: a rendőrség szolgálatába állított tudomány,” *Belügyi Szemle* 62, no. 9 (2014): 95–107.

¹² Suhajda, “Néhány gondolat a prediktív rendészetről,” 76.

¹³ Peter J. Brockwell and Richard A. Davis, *Introduction to Time Series and Forecasting* (Springer, 2016), 23–35.

¹⁴ Tim Lau, *Predictive Policing Explained*, Brennan Center for Justice (2020), <https://www.brennancenter.org/our-work/research-reports/predictive-policingexplained>.

In these cases, the types of data used have extended to personal identifiers and contact networks, which in turn raises serious data protection issues. In Europe, a more cautious approach is typical: for example, in some states in Germany, predictive software only uses anonymized, aggregated criminal data and focuses more on spatio-temporal patterns.¹⁵ It is important to emphasize that the accuracy and reliability of data are crucial, as incorrect, incomplete or distorted data can lead to misleading predictions. Therefore, the integration and cleaning of police databases, as well as the continuous monitoring of data quality, are essential parts of the technological background of predictive systems.

2. 2 Types of predictive models and application examples

There are several models in the field of data-driven policing, depending on the type of prediction we want to make. We generally distinguish three main groups: area-based, event-based and person-based models.¹⁶ The approaches seek to answer different questions. Area-based models try to predict where and when a crime is likely to occur. Event-based models examine what type of event is likely to occur at a given location or time. Finally, person-based models focus on who the perpetrator or even the victim might be.¹⁷ These three models therefore approach crime prevention from different perspectives, but their common feature is that they support police decision-making by building on data, statistics and patterns. In the following section, we briefly review the characteristics and practical examples of these types.

Model Type	Main Question	Key Features	Practical Example
Territorial (Location-Based)	Where and when is crime likely to happen?	Uses geographic and time-based data to find “hot spots” of criminal activity.	PredPol (Geolitica) – predicts burglary risk zones based on previous incidents.
Event-Based	What kind of crime might occur?	Focuses on predicting the type or pattern of incidents in a specific context or location.	Models combining crime type data with human mobility flows (e.g., events, weekends).
Person-Based	Who might be involved in a crime — as offender or victim?	Analyzes social networks, past records, or risk factors to identify individuals at higher risk.	Chicago’s “Strategic Subject List” (SSL) program.

Main Types of Predictive Policing Models (Source: Author’s own editing)

¹⁵ Suhajda, “Néhány gondolat a prediktív rendészetről,” 77.

¹⁶ Ourania Kounadi et al., “A Systematic Review on Spatial Crime Forecasting,” *Crime Science* 9, no. 1 (2020): Article 7, <https://doi.org/10.1186/s40163-020-00118-7>.

¹⁷ Grant Drawve, Steven C. Moak, and Everritt R. Berthelot, “Predictability of Gun Crimes: A Comparison of Hot Spot and Risk Terrain Modelling Techniques,” *Policing & Society* 26, no. 3 (2016): 312–331., <https://doi.org/10.1080/10439463.2014.942851>.

3. The legal regulatory environment of Predictive Policing

When applying predictive policing, it is essential to take into account a number of fundamental rights and constitutional principles. Human dignity is an inviolable value that all state measures, including algorithmic crime forecasting, must respect. Article II of the Fundamental Law explicitly states: “Human dignity is inviolable.”¹⁸ The collection and analysis of data for the purpose of crime prevention directly affects the area of privacy and data protection, which must be protected with particular emphasis. Article VI (1) of the Fundamental Law guarantees respect for private and family life,¹⁹ home and communications, while Article VI (3) states that everyone has the right to the protection of their personal data.²⁰

Everyone must be presumed innocent until proven guilty by a final court judgment.²¹ The principle – enshrined in Article XXVIII (2) of the Fundamental Law and Charter of Fundamental Rights of the European Union, Article 48. – sets a limit on treating anyone as a suspect or subjecting them to adverse measures solely on the basis of an algorithmic prediction. Predictive models cannot serve as a basis for criminal liability in themselves. In addition, the European Parliament has also stressed that such predictions are unreliable with regard to individual behavior and therefore cannot form the sole basis for police intervention.²² In practice, this requires that someone cannot be automatically treated as a criminal based on a prediction, meaning that further human consideration and concrete evidence are always needed.

The prohibition of discrimination (equal treatment) is also a sensitive part of the proper application of data-driven policing algorithms. Neither Article XV. (1)-(2) of the Hungarian Fundamental Law nor Article 21 of the EU Charter of Fundamental Rights allow discrimination, in particular, on the basis of characteristics such as race, colour, ethnic origin, gender, religion or political opinion.²³ However, predictive policing analytical tools can easily reproduce existing biases and biases by following patterns in historical data. If a system disproportionately identifies certain areas or groups as high-risk based on historical crime data, it can lead to indirect discrimination against the groups concerned.²⁴ Therefore, when using predictive models based on profiling, it is

¹⁸ *Fundamental Law of Hungary*, April 25, 2011, Article II.

¹⁹ *Charter of Fundamental Rights of the European Union*, 2007/C 303/01.

²⁰ Litska Strikwerda, “Predictive Policing: The Risks Associated with Risk Assessment,” *The Police Journal* 94, no. 3 (2021): 422–436., <https://doi.org/10.1177/0032258X20982120>.

²¹ *Charter of Fundamental Rights of the European Union*, 2007/C 303/01.

²² European Parliament. *Artificial Intelligence in Criminal Law and Its Use by Police and Judicial Authorities in Criminal Matters*. Resolution of October 6, 2021. 2020/2016(INI). 2022/C 132/02., https://www.europarl.europa.eu/doceo/document/A-9-2021-0232_HU.html.

²³ *Charter of Fundamental Rights of the European Union*, 2007/C 303/01. Article 21 Prohibition of discrimination.

²⁴ European Parliament, *Artificial Intelligence in Criminal Law*.

necessary to ensure that the algorithm does not result in discriminatory practices on racial, ethnic or other grounds. The principles of legal certainty, necessity and proportionality must be given special attention, although the principle of the rule of law requires that state interventions be predictable and foreseeable, based on legal authorisation and must not restrict rights more than strictly necessary. According to Article B) (1) of the Fundamental Law, Hungary is a state governed by the rule of law. This includes the requirement of legal certainty. This requirement is also reflected in the EU Charter of Fundamental Rights: Article 52 (1) states that the exercise of fundamental rights may be restricted only by law, respecting the essence of the rights, in accordance with the principle of proportionality, and only in cases where necessary and genuinely justified.²⁵ From a fundamental rights perspective, the use of algorithmic crime forecasting must therefore remain within a clear legal framework and may only be permitted if it is absolutely necessary to protect public safety and is not excessive in relation to the aim. The use of secret or opaque algorithms – based on which citizens are in advance unaware on what basis they may come under the police’s attention – could undermine legal certainty.

The National Authority for Data Protection and Freedom of Information (NAIH) is responsible for monitoring the enforcement of constitutional law.²⁶ At EU level, Article 7 of the EU Charter of Fundamental Rights enshrines the right to respect for private life and Article 8 specifically enshrines the right to the protection of personal data, requiring fair processing, purpose limitation, the right of access and rectification of the data subject and the existence of an independent supervisory authority. Predictive policing typically uses large amounts of personally identifiable data and therefore constitutes data processing to which the laws on the protection of personal data are strictly applicable. The principles of the GDPR (General Data Protection Regulation) – such as purpose limitation, data minimisation, data quality and integrity, and accountability – are also mandatory for predictive analytics. In addition, Article 22 of the GDPR prohibits decisions based solely on automated processing from having a significant impact on the data subject, unless authorised by law and subject to appropriate safeguards. These requirements also appear in Hungarian law: pursuant to Section 6 of Act CXII of 2011 on the Right to Informational Self-Determination (Act CXII of 2011), a decision made exclusively by automated means – in particular by means of profiling – that adversely or significantly affects the data subject, may only be made if it is expressly permitted by law or EU law and at the same time ensures the protection of the data subject's rights (such as compliance with the requirement of equal treatment, the availability of information about the methods applied and the possibility of human review).²⁷ Therefore, from a data protection perspective, predictive policing systems can only operate within strict frameworks, requiring an appropriate legal basis and

²⁵ *Charter of Fundamental Rights of the European Union*, 2007/C 303/01.

²⁶ *Fundamental Law of Hungary*, Article VI (4).

²⁷ Hungary, *Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information*.

purpose-specific data storage and use, based on the principle of minimum data requirements. Since such systems may often handle sensitive data for public security purposes, it is of utmost importance to protect this data and to ensure that special categories of data can only be used exceptionally, with legal permission and with guarantees.²⁸

3. 1 Hungarian regulatory situation and challenges

In Hungary, there is currently no separate, explicit legal provision for the application of data-driven policing, the area is delimited by more general legislation and the framework of data processing standards applicable to the police. On the one hand, the constitutional foundations of police activity are laid down by the Fundamental Law itself, and the previously mentioned fundamental rights (human dignity, privacy, equal treatment, fair trial, data protection) constitute binding guidelines for the executive branch. Article VI. (3)–(4) of the Fundamental Law declares the right to the protection of personal data and establishes the independent data protection authority (NAIH),²⁹ while Article XXVIII. guarantees fair trial and the presumption of innocence in criminal proceedings.³⁰ Specific rules on police data processing are contained in several pieces of legislation. Act XXXIV of 1994 on the Police (PPA) empowers the police to collect information for crime prevention and crime-fighting purposes, but at the same time stipulates that police measures must respect fundamental rights and be proportionate to the legitimate aim (according to Section 2(1) of the PPA, the police are obliged to comply with the requirement of proportionality in their measures). The PPA also contains guarantees for preventive information collection, for example: Section 17(4) states that the police may only collect data for crime prevention purposes in relation to a crime that can be reasonably suspected, and the method of data collection may not infringe the rights of the data subjects. Furthermore, the Police Act and related legislation regulate cases of secret information collection and surveillance in detail, which can often be relevant in dealing with threats indicated by predictive systems.

In the field of data protection regulation, Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information plays a key role. Section 3(5) of Act CXII of 2011 states that the scope of the law also extends to partially or fully automated data processing, including police data processing. The Infotv. deals with data processing for law enforcement purposes in a separate chapter (Chapter VI/A.), transposing the provisions of the EU Directive 2016/680/EU. According to the law, the data controller must categorize personal data stored in police records according to whether the person concerned is a suspect, convicted person, victim, witness or otherwise involved in the crime.³¹ Thus, if the police identify a person as a potential perpetrator with the help of an algorithm, this can only be recorded in the database as a police assessment and

²⁸ Act CXII of 2011.

²⁹ *Fundamental Law of Hungary*, Article VI (4).

³⁰ Marcell M. Tóth, “A digitalizáció egyes kihívásai a büntetőeljárásban,” *Belügyi Szemle* 72, no. 2 (2024): 185–210.

³¹ Act CXII of 2011.

cannot be confused with proven facts. The Infotv. also regulates in detail the rights of data subjects in law enforcement data processing: although certain rights may be restricted by the police in the interests of the investigation, the data subject may later request to determine what data has been processed about him or her and what automated profiling has been carried out.³² In addition, the NAIH's supervisory authority also extends to police data processing, ensuring independent supervision.

Automated decision-making in public administration and law enforcement has only appeared sporadically so far, however the legal environment already contains relevant frameworks. Hungary has included restrictions on automated decision-making in national law in the spirit of Article 22 of the GDPR.³³ In addition, we can see an example in practice of how an authority applies automated risk analysis in a regulated manner. The Passenger Information Unit (PIU) – in Hungary the Terrorism Information and Crime Analysis Centre (TIBEK) – carries out automatic hazard assessments based on passenger data transmitted by airlines, in order to prevent terrorism and serious crime. The algorithm operating within the PNR system identifies higher-risk passengers using predefined profiles, but the law requires that individuals flagged as high-risk must be reviewed by a human analyst as well before any action is taken.

Although the current domestic legal framework provides a number of general guarantees, new legislative and enforcement challenges arise with the spread of algorithmic crime forecasting tools. Besides, the domestic enforcement of the EU AI Act is also a challenge, as the AI Regulation will be directly applicable, Hungary will have to designate national authorities and a sanctioning system responsible for its implementation. It is expected that the NAIH and other specialized authorities will be given the authority to enforce the AI Regulation. It will be necessary to decide who will supervise the AI systems used by the police, and whether a separate specialized organization or body is needed.

Our current national regulations do not contain specific algorithm transparency or normative requirements for the police. In the future, it may be justified to create legislation or internal standards that require the police to use only properly, legally audited and ethically validated AI systems. It may also be necessary to supplement the Be. (Criminal Procedure Act) to specify under what conditions predictive software outputs may form the basis for police action. It may also be an important guideline for judicial practice, if it is stipulated by law that the results of predictive tools can be evaluated as evidence to a limited extent, only in accordance with other evidence. It is essential that, in the interests of legal certainty, citizens should know if any automated risk analysis has been carried out concerning them. The GDPR in principle guarantees data subjects the right to information and the right to request human intervention in relation to automated decisions, although in the law enforcement sector these rights can be limited in the interests of the investigation. It will be a challenge to find the right

³² Ibid.

³³ Hungary, *Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information*, Section 6.

balance between not compromising the effectiveness of law enforcement and at the same time not subjecting citizens to the surveillance of “black box” algorithms without their knowledge.

The legal and moral use of technology is not only a legal issue, but also an institutional and cultural one. In the future, it will be important for law enforcement agencies to develop guidelines for the use of AI. Furthermore, it is necessary to ensure that officers are properly trained. They must understand the limitations of the operation of analytical tools, the potential for bias in them, and that human accountability cannot be delegated to algorithms. These topics are already appearing at the National University of Public Service and other law enforcement training courses, but further training of practicing investigators and commanders is also justified. Finally, it is of particular importance that the regulation of predictive policing is an area that is also emerging globally, and therefore Hungary has the opportunity to adopt European best practices that can help develop the legal environment. In some countries, independent algorithm review committees have been established alongside the police, which continuously monitor the decisions of the applied AI systems in terms of discrimination or error. It will be crucial for domestic legislators to monitor international trends and the evolving Hungarian regulatory landscape. Therefore, Hungary’s challenge lies in aligning technological innovation with constitutional safeguards to ensure lawful and ethical policing.

4. Criminological approach and effects

AI-based crime-prevention systems fit within the broader criminological discourse on risk and surveillance, shifting focus from punishment to prevention. It represents a new, ‘pre-criminal’ approach to fighting crime. In the traditional approach, traditional criminology treats crimes as post-factual events – research is aimed at understanding crimes, perpetrators, victims and the justice process – in contrast, data-driven policing technologies aim to prevent future crimes.³⁴ In this new paradigm, the focus is on precaution and risk management, i.e. the emphasis is on the prior recognition and reduction of potential dangers, rather than merely the ex post treatment of crimes that have already occurred.³⁵

The literature associates this shift with the emergence of a “risk society”, i.e. a social order that focuses on the control and prevention of potential risks, and in which criminal law is also understood as a means of managing crime risks.³⁶ As a result, the scope of criminological research is changing and issues of risk factors, uncertainty, surveillance, and prevention are coming to the fore.

³⁴ Lucia Zedner, “Pre-crime and Post-criminology?” *Theoretical Criminology* 11, no. 2 (2007): 262–63, <https://doi.org/10.1177/1362480607075841>.

³⁵ Strikwerda, “Predictive Policing: The Risks Associated with Risk Assessment.”

³⁶ Ádám Kalmár, “A prediktív rendészet sajátos tényezői a vízi határforgalom-ellenőrzésben,” in *A rendkívüli helyzetek biztonsági tényezői*, edited by Gyula Gaál and Zoltán Hautzinger (Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport – Magyar Rendészettudományi Társaság, 2022), 153–58.

The pre-crime perspective marks a fundamental shift in criminological thinking. The post-crime perspective is replaced by a future-oriented perspective, the goal of which is to prevent crimes before they occur.³⁷ The new approach integrates methods and resources from other disciplines into crime prevention to increase safety.³⁸ Big Data and AI play an important role in the development of algorithmic crime forecasting, the ability to analyze vast amounts of data creates the basis for the police to look for predictable patterns in crime. It fits into the broader trend pursuant to which in the modern information society, data is becoming more valuable and decision-making based on data analysis is gaining more and more ground in the public sector.

One of the theoretical explanations for the change in criminological perspective is that society lives in an era of uncertainty and danger, so the emphasis is shifting to recognizing and reducing risk. Thus, the need for proactivity appears in crime prevention and law enforcement as well: we do not simply want to react to crimes but we want to prevent them by thinking ahead.

4. 1 Benefits and effectiveness issues of risk-based crime prevention

The main promise of predictive policing is to increase the effectiveness of crime prevention and the proactivity of police work thus, in this light, modern algorithms are able to analyze past crime data and other factors, mentioned in the previous chapter. The police can allocate resources more efficiently and target patrols to high-risk neighborhoods. In addition, the application of Big Data and predictive analytics can also bring significant progress in the efficiency of investigations, as analytical tools can comb through large datasets to reveal hidden connections that would remain unnoticed by human analysts.

However, the effectiveness of predictive methods is mixed. First, predictive algorithms only work well for certain types of crime, those that occur in large numbers and patterns. For example, they may be useful for serial property crimes (burglary, theft), while they do not make sense for predicting rare or unique cases, such as homicides.³⁹ Second, there is a threat that crime will shift spatially or adapt to police strategy. If police focus exclusively on designated “hot spots,” police presence in other areas may decrease, which could counterproductively create new opportunities for criminals to operate there.⁴⁰ Furthermore, false alarms (false positive predictions) from algorithms can lead to wasted resources, while missed alarms (false negatives) can create a false sense of security.

³⁷ Kalmár, “A prediktív rendészet sajátos tényezői a vízi határforgalom-ellenőrzésben,” 156.

³⁸ Bence Mészáros, “A kriminálstratégia önállósodása,” *Belügyi Szemle* 66, no. 11 (2018): 65–70, 68.

³⁹ Mo Al-Youssef, “Predictive Policing: Wie die Polizei Verbrechen voraussagt,” accessed October 26, 2025, <https://www.derstandard.de/story/2000091840678/predictive-policing-wie-die-polizei-verbrechen-voraussagt>.

⁴⁰ Katalin Ligeti, *Artificial Intelligence and Criminal Justice*, AIDP-IAPL International Congress of Penal Law (2020), accessed October 26, 2025, https://www.penal.org/sites/default/files/Concept%20Paper_AI%20and%20Criminal%20Justice_Ligeti.pdf.

In practice, these systems have had limited and inconsistent results. Some early projects have been successful in reducing certain types of crime, but problems have arisen in many places. For example, several cities in the United States have withdrawn algorithmic crime forecasting programs after pilot implementation because audits revealed inadequate effectiveness and disproportionate bias effects.⁴¹ Police departments in New York and Cambridge reported that predictive analytical tools did not meet expectations and, in some cases, distorted police actions – therefore, they turned to community policing, which paradoxically led to an improvement in crime rates.⁴² In line with this, experts often emphasize that the field of predictive policing is still in its infancy and, while technologically promising, its application must be approached with great caution. The methods need to be continuously monitored and scientifically evaluated before they are widely introduced into everyday police practice.

Advantage–Challenge type	Short description
The benefits and challenges of predictive policing	The police are able to identify areas at risk in advance and take preventive measures.
Targeted allocation of resources	Patrol and investigative resources can be concentrated in high-risk locations.
Improving investigation efficiency	Algorithms can uncover hidden patterns in large data sets.
Limited applicability (only works for certain crimes)	They are mainly useful for pattern-based crimes against property; in rare cases, they are not.
Spatial shift of crime	Focusing on some areas may reduce police presence elsewhere.
False positive/negative predictions	False alarms can cause unnecessary intervention, and missed alarms can create a false sense of security.
Mixed experiences in international examples	New York, Cambridge and other cities have withdrawn their systems due to low efficiency and distorting effects.

The benefits and challenges of predictive policing (Source: Author's own editing)

⁴¹ European Parliament, *Artificial Intelligence in Criminal Law and Its Use by Police and Judicial Authorities in Criminal Matters*, Resolution of October 6, 2021 (2020/2016(INI)), 2022/C 132/02.

⁴² P9_TA (2021)0405 Artificial intelligence in criminal law.

5. Legal regulation and international reactions

Legal regulation and oversight of algorithmic crime forecasting have begun worldwide, and restrictive measures have been introduced in several places.

The use of AI-based crime prevention systems tools in the United States has sparked several controversies in recent years. Several major cities, including Santa Cruz and Oakland, have banned predictive methods after it was found that such programs often lead to racially discriminatory outcomes. The Los Angeles Police Department also stopped using PredPol in 2020 after an internal audit found that the software reflected existing biases in practice and disproportionately targeted minority areas.⁴³ Overall, there are more critical voices than satisfied voices in the US at the moment. The EU appears to be taking a more cautious, preventive approach. The European Union's proposed AI regulation (AI Act) classifies predictive policing systems as high-threat AI applications. In fact, EU lawmakers explicitly prohibit certain high-risk data-driven policing technologies practices. Article 5(1)(d) of the AI Act prohibits AI systems that evaluate individuals' likelihood of committing a crime based on personal characteristics. Hungary, as an EU Member State, will have to adapt national legislation to comply with the AI Act's high-risk application framework by 2026, including enforcement mechanisms and sanctions. According to the final regulatory text, algorithmic crime forecasting systems that assess an individual's likelihood of committing a crime based on personal characteristics are classified as posing an unacceptable risk and are therefore prohibited.⁴⁴

Solutions based on predictive methods are not yet widely used in Hungary. According to public information, the domestic police do not currently use sophisticated crime prediction softwares such as those used abroad. However, risk analysis systems with similar logic already exist in state administration. It can be argued that if Hungarian law enforcement agencies start using predictive algorithms in larger numbers in the future, similar questions may arise as abroad. According to experts, it is necessary to create legal guarantees in advance that prevent violations of fundamental rights and ensure the transparency and verifiability of the source codes and operating mechanisms of the software used. Hungary is currently following the regulations being prepared within the framework of the EU, and its provisions are expected to guide domestic practice as well.

6. Future assurances

In light of the above, it becomes clear that the future of algorithmic crime forecasting depends on finding a balance between innovation and safeguards. The technology will continue to develop – AI-based crime prevention is expected to become an increasingly common part of everyday police work – but strong

⁴³ Tzu-Wei Hung and Chun-Ping Yen, "Predictive Policing and Algorithmic Fairness," *Synthese* 201 (2023): Article 206, <https://doi.org/10.1007/s11229-023-04189-0>.

⁴⁴ European Union, *Artificial Intelligence Act*, PE/24/2024/REV/1, Article 5(1)(d).

safeguards are needed. Criminologists say it is essential to create a framework in which the use of predictive models does not undermine fundamental rights but truly promotes public safety.⁴⁵

AI-based decisions should never be fully automated; a responsible human actor should always review or make the final decision.⁴⁶ This ensures that machine prediction does not become an exclusive judgment and that the specific circumstances of a given situation can be taken into account. The requirement is that the algorithms of predictive systems are transparent and auditable. Implementing authorities must be aware of the operating principles and independent experts must be able to audit the models. Data protection and civil rights organisations are calling for the datasets and weightings on which the system's decisions are based to be public or at least accessible to supervisory bodies.

The world of predictive methods holds both exciting opportunities and serious dilemmas. With the development of AI and data analytics, the police have the opportunity to not only react to crimes but also prevent them – with more targeted patrols. However, this progress is not without risks: if the appropriate legal and moral safeguards are lacking, people's fundamental rights can easily be undermined. International practices also reflect this. While some American cities have shut down predictive algorithms due to bias and lack of transparency, the European Union's new AI regulation has already imposed a legal ban on certain applications. For algorithmic crime forecasting to truly serve public safety – and not detract from it – an approach is needed that both encourages innovation and ensures the protection of fundamental rights. Only by combining innovation with accountability can the policing of the future remain not only effective but also just. Establishing transparent algorithmic audit mechanisms and interdisciplinary AI ethics committees within law enforcement could ensure that data-driven policing technologies align with both legal standards and societal trust.

7. Conclusion

Predictive methods demonstrate how rapidly technology is transforming criminal justice systems. However, without clear ethical and legal boundaries, even the most advanced systems may threaten fundamental rights. Therefore, the challenge for the coming decade will be to ensure that predictive algorithms serve justice — not replace it.

⁴⁵ Csapó, “A korszerű rendőrség alapjai,” 48.

⁴⁶ European Parliament, Artificial Intelligence in Criminal Law.