

Bói, László – Berei, Róbert: The role of the main crime geographical factors in Józsefváros's crime

Frigyer, László: As the lava of the Krakatau

Kiss, Valentin Bence: The law enforcement application of maps

Mezei, Kitti – Gyaraki, Réka: Transforming Law Enforcement with AI: Insights from the EU AI Act and Hungary's Perspective

Abstracts of the 5th criminal geographical conference

News from the world of the Hungarian and international criminal geography

CGJ

CRIMINAL GEOGRAPHICAL JOURNAL

ACADEMIC AND APPLIED RESEARCH IN CRIMINAL GEOGRAPHY SCIENCE

VOLUME VII. / NUMBER 1-2. / March 2025



Academic and applied research in criminal geography science. CGR is a peer-reviewed international scientific journal. Published four times a year.

Chairman of the editorial board:

SZABOLCS MÁTYÁS Ph.D. associate professor (Ludovika University of Public Service, Hungary)

Honorary chairman of the editorial board:

JÁNOS SALLAI Ph.D. professor (Ludovika University of Public Service, Hungary)

Editor in chief:

VINCE VÁRI Ph.D. associate professor (Ludovika University of Public Service, Hungary)

Editorial board:

UFUK AYHAN Ph.D. associate professor (Turkish National Police Academy, Turkey)

JOHANNA FARKAS Ph.D. associate professor (Ludovika University of Public Service, Hungary)

MARJAN GJUROVSKI Ph.D. assistant professor (State University 'St. Kliment Ohridski', Macedonia)

LADISLAV IGENYES Ph.D. assistant professor (Academy of the Police Force in Bratislava, Slovakia)

IVAN M. KLEYMENOV Ph.D. professor (National Research University Higher School of Economics, Russia)

DRAGANA ČVOROVIĆ Ph.D. associate professor (Univ. of Criminal Investigation and Police Studies, Serbia)

KRISTINA A. KRASNOVA Ph.D. associate professor (Russian State University of Justice, Russia)

VELIBOR LALIC Ph.D. associate professor (University of Banja Luka, Bosnia-Herzegovina)

EDINA LILLA MÉSZÁROS Ph.D. assistant professor (University of Oradea, Romania)

ZSUZSA PISKÓTI-KOVÁCS Ph.D. research associate (Eszterházy Károly University, Hungary)

ANDREA PÓDÖR Ph.D. associate professor (Óbuda University, Hungary)

BAYRAM ALI SONER Ph.D. professor (Turkish National Police Academy, Turkey)

DANE SUBOŠIĆ Ph.D. professor (University of Criminal Investigation and Police Studies, Serbia)

ANDREA SZABÓ Ph.D. (Ludovika University of Public Service, Hungary)

MIKLÓS TIHANYI Ph.D. associate professor (Ludovika University of Public Service, Hungary)

CONSTANTIN -VASILE ȚOCA Ph.D. senior lecturer (University of Oradea, Romania)

ANTAL TÓTH Ph.D. associate professor (Eszterházy Károly University, Hungary)

GABRIELLA ÜRMÖSNÉ SIMON Ph.D. associate professor (Ludovika University of Public Service, Hungary)

DAVID ZÁMEK Ph.D. associate professor (Institute of Public Administration Prague, Czech Republic)

ZHENJIE ZHOU Ph.D. professor (Beijing Normal University, China)

Technical editor: LÁSZLÓ FRIGYER assistant lecturer and TIBOR TIRTS master teacher (Ludovika University of Public Service, Hungary)

Linguistics reviewer: GABRIELLA ÜRMÖSNÉ SIMON Ph.D. associate professor (Ludovika University of Public Service)

All correspondence should be addressed to the chair of the editorial board

criminalgeography@gmail.com

Vol. VII. 2025/1-2.

Designed by Antal Forró

CONTENTS

Lectori salutem.....	7
Bói, László – Berei, Róbert: The role of the main crime geographical factors in Józsefváros's crime.....	9
Frigyer, László: As the lava of the Krakatau.....	19
Kiss, Valentin Bence: The law enforcement application of maps.....	25
Mezei, Kitti – Gyaraki, Réka: Transforming Law Enforcement with AI: Insights from the EU AI Act and Hungary's Perspective.....	33
Abstracts of the 5 th criminal geographical conference.....	49
News from the world of the Hungarian and international criminal geography.....	55

Mezei, Kitti Ph.D. associate professor

Ludovika University of Public Service, Faculty of Law Enforcement
mezei.kitti@uni-nke.hu

Gyaraki, Réka Ph.D. police Major, assistant professor

Ludovika University of Public Service, Faculty of Law Enforcement
gyaraki.reka@uni-nke.hu

**TRANSFORMING LAW ENFORCEMENT WITH AI:
INSIGHTS FROM THE EU AI ACT AND HUNGARY'S PERSPECTIVE¹****Abstract**

This paper examines the transformative potential and challenges of integrating artificial intelligence (AI) into law enforcement, focusing on the European Union's AI Act and its implications for Hungary. It explores the ethical and legal issues surrounding applications like predictive policing, real-time biometric identification, and offender profiling, emphasising the risks of data biases and violations of fundamental rights. While Hungary has yet to deploy AI in law enforcement, the paper identifies promising areas for adoption, including video analysis, behavioural profiling, and open-source intelligence gathering. The findings underscore the importance of balancing innovation with robust governance to safeguard rights and public trust. By analysing the intersection of criminal geography, technology, and law enforcement, this study highlights how AI can serve as a catalyst for smarter resource allocation and more effective crime prevention strategies.

Keywords

Artificial intelligence, EU AI Act, high-risk AI systems, law enforcement, predictive policing

1. Introduction

Integrating artificial intelligence (AI) into law enforcement presents both transformative opportunities and significant challenges. This paper examines the role of AI in policing within the framework of the European Union's AI Act, focusing on its regulatory implications and potential law enforcement applications in Hungary. By analysing the classification of AI systems as high-risk, the ethical concerns surrounding their use, and the current technological

¹ The research was supported by the European Union project RRF-2.3.1-21-2022-00004 within the Artificial Intelligence National Laboratory framework and by the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

capabilities, the paper explores how AI can enhance efficiency and decision-making while ensuring compliance with fundamental rights.

Cases involving law enforcement use have been mainly classified as high-risk AI systems. The AI Act defines law enforcement authority and law enforcement activities.² Importantly, the AI Act will exclude AI systems used for military, defence, or national security purposes from the scope of the AI Act, regardless of whether public or private entities utilise them [Article 2 (3)]. This exclusion is justified by both international law and the specific competencies governing defence and security within the EU. The exclusion is supported by Article 4(2) of the Treaty on European Union (TEU), which designates defence and national security matters as the sole responsibility of Member States. Additionally, the specificities of the Member States' defence policies, covered by Chapter 2 of Title V of the TEU, are subject to public international law. However, if these systems are also used for non-excluded purposes, such as civilian or law enforcement activities, they must comply with the AI Act. Conversely, AI systems developed for civilian or law enforcement purposes that are subsequently used for military, defence, or national security purposes are not subject to the AI Act. This allows entities engaged in national security, defence, and military activities to use AI systems without being affected by the regulation (Recital 24). Arguably, these rules create a loophole that allows Member States to exempt themselves from the rules for any activity they deem relevant for "national security" (Leufer et al. 2023).

2. The AI Act's risk-based approach

2.1. Forbidden AI systems in law enforcement

Following its risk-based approach, the AI Act proposes a category of prohibited AI systems. This entails a completely prohibited category (Title II), which includes the prohibition of real-time remote biometric identification for law enforcement purposes in publicly accessible spaces³ with narrow exceptions where the use is strictly necessary to achieve the public interest,

² Law enforcement authority "means any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security"; law enforcement "means activities carried out by law enforcement authorities or on their behalf for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including safeguarding against and preventing threats to public security."

³ Publicly accessible space "means any publicly or privately owned physical place accessible to an undetermined number of natural persons, regardless of whether certain conditions for access may apply, and regardless of the potential capacity restrictions". In the context of the AI Act, a publicly accessible space refers to any physical area open to an indeterminate number of people, whether publicly or privately owned, and regardless of its use, such

which outweighs associated risks. These situations include searching for victims of crime, addressing threats to life or physical safety, and locating or identifying perpetrators or suspects of serious criminal offences (such as human trafficking or sexual exploitation or for the prevention of terrorist attacks) punishable by a custodial sentence or detention order of at least four years. Thus, the prohibition does not apply where these systems are used for any of the listed specific purposes because the severity threshold for such offences ensures that real-time biometric identification systems are proportionate and justified. In principle, relying on such an exception will require thorough assessments, technical and organisational measures, notifications and a warrant.⁴ However, the AI Act allows the use of real-time and post-event biometric identification for law enforcement and private purposes under certain conditions in general, so there is no ban in these cases (Raposo 2022).

One of the major concerns with facial recognition technology is the lack of consent in collecting and storing individuals' biometric data. Another banned use case is databases based on bulk scraping of facial images (Sobel 2021) since there are cases in which specific harms stem from the online deployment of AI biometric systems (Georgieva – Hoekstra 2022). Bulk scraping of facial images can be defined as the automated collection of large volumes of facial images and associated metadata from publicly accessible web sources, using algorithms or bots, typically to build or enhance facial recognition datasets, often without explicit user consent. These images are then used to train facial recognition systems or create massive facial image databases (see Solove 2024). An issue of considerable controversy revolves around the involvement of private companies in implementing these technologies. For example, in February 2020, media outlets revealed leaked documents indicating that Clearview AI had secured contracts with over 600 law enforcement agencies globally, including Europe (Sanz 2022). This technology equips users with the capability to potentially identify every individual they encounter in real-time, significantly enhancing law enforcement's ability to swiftly and accurately match faces against extensive databases. The system enables an investigating officer, for example, to submit an image of a person of interest for analysis and conduct a search within a database compiled by Clearview AI. This database purportedly contains publicly accessible images sourced from

as commercial, service, transport, or entertainment spaces (e.g., shops, banks, gyms, airports). Spaces remain publicly accessible if access requires fulfilling certain conditions (e.g., buying a ticket or prior registration). However, areas restricted to specific individuals by law or authority (e.g., workplaces, company premises, prisons) are not considered publicly accessible. Online spaces are excluded, as they are not physical.

⁴ Real-time biometric identification is held permissible for law enforcement if the following prerequisites apply: a) *ex-ante* permission by a judicial authority; b) targeted search; and c) link with the investigation of committed serious crimes listed in Article 83(1) Treaty on the Functioning of European Union (terrorism, trafficking in human beings and sexual exploitation of women and children, illicit drug trafficking, illicit arms trafficking, money laundering, corruption, counterfeiting of means of payment, computer crime, and organised crime).

online postings, which may not necessarily pertain to the individual under investigation, raising concerns about privacy and the ethical implications of such technology (González Fuster 2020). The AI Act will ban the use of predictive policing software to assess an individual's risk of committing future crimes based on personal traits. The final version of the ban is considerably weaker than that proposed by the EP in June. Such uses of AI-based tools in policing and criminal justice risk discrimination and a violation of fundamental rights, including the right to a fair trial and the presumption of innocence. Predictive policing usually encompasses various approaches (only some of which are prohibited), which can be broadly categorised into four types: predicting crimes by forecasting high-risk locations and times, identifying potential offenders at risk of committing or repeating crimes, creating profiles resembling those of past offenders, and predicting potential victims of crimes to identify vulnerable individuals or groups (Egbert - Leese 2020). Predictive policing systems have already been deployed in Europe, in Austria, Germany and Switzerland (EUFRA 2022).

2.2. High-risk AI systems in law enforcement

An AI system is considered high-risk either because it is a safety component of an already strictly regulated product group or because it is used in an area where it poses a significant risk of harm to the health, safety or fundamental rights of natural persons. However, the AI Act states that “any AI system referred to in Annex III shall not be considered as high-risk if they do not pose a significant risk of harm, to the health, safety or fundamental rights of natural persons, including by not materially influencing the outcome of decision making” [Article 6 (3)]. The cases exempt from the high-risk classification are narrow procedural tasks, improvements to the results of previously completed human activities, decision or outlier detection without replacing human assessments, and those in which the AI system is designed to detect decision-making patterns or deviations, not to replace or influence previous human assessments without proper review [Article 6 (3) a)-d)]. AI systems will be considered not to pose a significant risk of harm if they meet at least one of four criteria. Nonetheless, the AI Act also makes it clear that any AI system will automatically be considered to be high-risk if the AI system performs the profiling of individuals. General-purpose AI systems used as high-risk AI systems or integrated into them will require providers to take additional steps, too.

Annex III categorises post-biometric identification and emotional inference for law enforcement purposes as high-risk applications. As a result, law enforcement agencies must comply with stricter requirements if they plan to utilise these tools. As permitted by relevant EU or national law, biometrics encompasses remote biometric identification systems, excluding

AI systems used solely for identity verification. It also includes AI systems for biometric categorisation based on sensitive attributes and those used for emotion recognition.

High-risk AI uses also include law enforcement use cases since their actions involving certain AI systems can wield significant power imbalances, potentially leading to surveillance, arrest, or deprivation of individuals' liberty, impacting fundamental rights as guaranteed by the EU Charter of Fundamental Rights. These are, according to Annex III, AI systems intended to be used by law enforcement authorities or on their behalf or by Union institutions, bodies, offices or agencies in support of law enforcement authorities for assessing the risk of individuals becoming victims of criminal offences, employing polygraphs and similar tools, evaluating the reliability of evidence in criminal investigations or prosecutions, assessing the risk of individuals offending or re-offending, not solely based on profiling or assessing personality traits, characteristics, or past criminal behaviour, and finally, profiling individuals during the detection, investigation, or prosecution of criminal offences within the constraints of Directive (EU) 2016/680. According to the AI Act, predictive policing tools generally fall under the high-risk AI systems category.

AI technologies can revolutionise crime prevention and law enforcement by leveraging geospatial data and historical crime patterns to identify high-crime areas. This approach enhances the efficiency of resource allocation, improves public safety, and facilitates proactive policing strategies. Operational since 2017, Denmark's POL-INTEL project leverages the Gotham system developed by Palantir Technologies. This system integrates various data sources to create a mapping system that identifies areas with higher crime rates, assisting in strategic decision-making for law enforcement (Collier 2020). The Dutch police have implemented the Crime Anticipation System, which uses historical crime data and machine learning algorithms to predict where and when future crimes might occur. This approach enables the proactive deployment of police resources to anticipated hotspots (Ferguson 2017). Germany has utilised the Precobs (Pre Crime Observation System) software, which analyses past crime data to predict potential future incidents, particularly focusing on burglary patterns. This system has been employed in cities like Munich and Nuremberg, aiming to allocate police resources more effectively (Egbert 2018). By combining historical crime data, geospatial analysis, and AI-driven methodologies like hotspot analysis, law enforcement can transition from reactive policing to proactive strategies. These techniques enable safer communities while promoting efficient use of resources. AI-backed geospatial data was criticised for disproportionately targeting minority neighbourhoods. It is important to ensure that datasets are

free from racial, socio-economic, or geographic biases. A regular audit is needed for the AI models to prevent the reinforcement of systemic inequalities (Mohler et al. 2015; Brayne 2021). If AI systems lack high-quality training data, fail to meet performance standards or lack transparency, they may discriminate or produce unjust outcomes. This can hinder the exercise of procedural rights, such as the right to an effective remedy, a fair trial and the presumption of innocence (Gless 2020; Palmiotto 2018). Since the use of AI tools by law enforcement and other authorities risks creating inequality or exclusion, it is crucial to consider how these tools impact the defence rights of suspects, especially regarding the challenges in understanding how these systems work and the difficulties in contesting their results in court, particularly for individuals under investigation. Therefore, the AI Act requires that providers of high-risk AI systems observe comprehensive mandatory compliance obligations for risk mitigation, data governance, detailed documentation, record-keeping, human oversight, transparency, robustness, accuracy, and cybersecurity (Section 2).

2.3. Limited-risk AI systems

As provided by Article 50 of the AI Act, other, non-high-risk, limited AI systems are subject only to transparency obligations. They apply in specific cases and include obligations, such as the obligation to inform individuals when interacting with a chatbot, the obligation to disclose and clearly label where visual or audio deepfake content has been manipulated by AI, or the obligation to inform and obtain the consent of people who are exposed to permitted emotion recognition and biometric categorisation systems. The transparency obligations prescribed for providers in the AI Act will be applicable to only a small portion of deepfakes. The AI Act will not protect against the malicious use of deepfakes. There are further issues with these rules. It is problematic that in certain situations, they place the burden of risk onto users, allowing providers to avoid responsibility for their conduct (Helberger - Diakopoulos, 2023; Veale - Borgesius 2021). The transparency obligations in Article 50 will not be applicable to the use of AI systems for law enforcement purposes, as it would undermine the interests of crime detection, prevention and investigation.⁵

3. Law enforcement applications of AI in Hungary

The functions of the police are defined in Act XXXIV of 1994. These include, among others, border protection, combating terrorism, crime prevention and detection, the recovery of

⁵ When notified, individuals may attempt to evade justice or alter their behaviour, potentially undermining the effectiveness of the technology.

property, and immigration and asylum-related tasks.⁶ The roles in law enforcement, crime prevention, public administration, and related areas have been established to fulfil these legal obligations. Within this framework, the application of AI in domestic law enforcement is explored. AI and its development present not only challenges for law enforcement but also opportunities to enhance certain functions within the organization. The primary and most essential requirement is for law enforcement agencies to perform their duties professionally while adhering to current legislation. The critical question is: how can AI assist in achieving these goals?

AI's development and adoption have a significant impact—both positive and occasionally negative—across various fields, including industry, medicine, biological research, and economics. In these areas, AI, including advanced techniques such as deep learning, is being increasingly employed to mitigate human error and fatigue. Similarly, many countries have already incorporated AI into law enforcement as a decision-making and investigative tool for maintaining public safety and to support policing in public spaces and during events (e.g., through body cameras, facial recognition technology, etc.).

AI could also play a valuable role in predictive policing. While this approach is not yet widely used in Hungary, AI can act as an assistant rather than replacing physical police officers. The aim of this study is to examine the potential domestic applications of AI, alongside the international practices that have yet to be adopted in Hungarian law enforcement.

Currently, AI is not employed by Hungarian law enforcement agencies such as the Hungarian Police or the National Tax and Customs Administration. However, there is a clear intention to explore its use, and experts are investigating the possibilities. In the context of public order, traffic policing, and law enforcement investigations, IT tools capable of serving as evidence or facilitating evidence collection are already indispensable. Digitally recorded data offer significant potential, which could be further enhanced by AI-driven applications.

The use of AI by law enforcement agencies could increase efficiency and provide substantial support in areas such as facial recognition, video and voice analysis, public order protection, event security, traffic policing, and crime prevention. However, before implementing AI solutions, it is essential to assess the readiness and training of personnel to ensure successful adoption. Potential areas where AI could be deployed in law enforcement include:

- Internal document management and document search support
- Big Data analytics,

⁶ Paragraph (1) of Article 1 of Act XXXIV of 1994 on the Police

- audio transcription,
- identification of still and moving images (e.g., based on behaviour or movement patterns),
- profiling,
- processing CCTV camera footage,
- enhancing airport security,
- image processing systems to support border protection,
- tools for sound, image, and text recognition and analysis.

A closely related area is using AI to support open-source data collection by law enforcement's criminal investigation units. Collecting, acquiring, and analysing open-source data from the Internet and available databases remains a significant challenge, but AI could significantly enhance these capabilities.

3.1. Possibilities for the predictive use of AI

One of the possibilities of AI is its use in a predictive process. As we will describe in the profiling section for offenders, it can indicate the possibility of re-offending, but it can also be used to detect most crimes, whether in the online space or the physical space. For many years, law enforcement has been using databases relevant to investigations. One such database is eModus,⁷ the latest version of the former criminal records system.⁸ The eModus manages the forensic characteristics of unsolved crimes in the unknown offenders section of the register (Juhász 2022). The known offenders' section of the register contains the details, description, forensic characteristics and the forensic characteristics of the perpetrators (suspects) of modus offences committed by them. Here, we deal with the pseudonyms or nicknames of the persons and their tattoos, which are of particular importance among the descriptive features and other particular characteristics.

Persons with tattoos who have committed an offence not covered by the modus collection are also included in the register with a restricted set of data (Juhász 2022).

The data stored in eModus can be used, among other things, for e-sight. Currently, in 2022, the development of this system and the verification of the factuality of the data entered is underway. The eModus system is one of the systems that is linked to the RobotZsarú system and which

⁷ 12/2021 (IV. 30.) ORFK Instruction on certain tasks related to the operation of the electronic Modus Operandi Register

⁸ It was a paper-based register, which was enacted by the Order of the Deputy Minister of the Interior of the MNK of 01/1967 on the Rules of Criminal Records (Chapter X).

allows law enforcement users to deduce new locations, victims and methods from previous offences and offender data, even in the case of serial offences.

3.2. Exploration possibilities using data and text mining

Law enforcement agencies can use common search engines available on the Internet, such as Google, Bing, Chrome, etc., to help them carry out their tasks. In addition to general internet searches, there is also the possibility of using different databases. One of these databases is the public register (address register, identity register, wanted persons register). The other database is the integrated case management system RobotZsaru, which is partially linked to these central registers, but other data stored in it are entered by law enforcement personnel. The content of these data records, decisions, the data and facts entered in them are recorded differently, and often the databases are not linked, or the necessary data and characteristics are not recorded.

Since the different databases are not interconnected (often due to legal restrictions), some data and information can be accessed, for example, by requesting data, sometimes with the permission of a prosecutor or a judge. For this reason, there is still a need for appropriate legislation on the databases used for detection purposes, but it would be timely to have proper 'interoperability' and 'transparency' between these data.

3.3. Other applications of AI in investigations and detection

AI can respond to specific, targeted searches for illegal content or criminally relevant information on the Internet. Based on images or videos of the searched items, the algorithm can, with appropriate programming and learning, search the information on the Internet in such a way that the content or information is filtered out of the large data set with the lowest possible error rate. This technology could be applied to identify child pornography, stolen objects/vehicles or even copyrighted content. The system is capable of performing recurrent searches on a given criterion, allowing even 24-hour continuous online monitoring of the content searched.

During investigations and detections, facial image recognition and video analysis would, among other things, filter and analyse illicit content, which would, for example, make the work of police officers easier, especially in the case of images and videos that are either psychologically stressful or often impossible to detect with the human eye.

In addition to facial recognition, the use of behavioural systems can help investigations.

Behavioural biometrics include:

- handwriting: handwriting image, dynamics,

- speaking tone,
- typing rhythm,
- movement: gait, changes in body position (Földesi 2017).

However, the efficiency of such technologies is influenced by environmental factors. In relatively sparse environments where individual movements are discernible, these tools perform well, but their effectiveness diminishes in densely populated or crowded settings, where distinguishing individual behaviours becomes significantly more challenging (Dobó – Gyarakı 2021).

Myo Thida and colleagues proposed two distinct modelling techniques to detect human activity and track individuals within crowds. The first approach, known as the macroscopic modelling technique, focuses on analyzing and understanding the collective movement patterns of people in crowded environments. This method examines the overall dynamics of crowd behavior rather than individual movements, providing insights into how groups of people navigate shared spaces. The second technique complements the macroscopic approach by targeting individual-level analysis, offering a more granular perspective on human activity within the crowd. Together, these methods provide a comprehensive framework for detecting and tracking human activity in complex, high-density scenarios, enabling applications in areas such as public safety, event management, and urban planning (Thida 2023).

3.4. The possibility of profiling in law enforcement and investigations

Profiling has the potential to improve the detection of different types of crime and to enable investigating authorities to model known and unknown offences and thus either detect or predict certain newer methods of offending that are likely to be used.

Profiling is a criminal analytical and evaluative activity used to detect unknown offenders, which is a combination of data already obtained in the course of an investigation, data from previous and similar crimes collected and organised specifically for this purpose, and scientific experience, mainly of a psychological nature, which can be obtained by other means, to provide investigators with an insight into the internal and external characteristics of the offenders. The profile drawn up in advance provides a typological picture of the offender, which can be used to narrow down the pool of potential perpetrators (Kiss 1995).

The literature on profiling, human profiling, is still mostly psychological, i.e. in certain situations, such as during interrogations, the perpetrator's body language, use of language (idioms, dialect), family and social relations, etc. However, in our country, the so-called specific profiling (profile analysis) has only been carried out in relation to the crime of homicide.

It is called specific profile analysis when a hypothetical picture of an unknown perpetrator of a specific crime is developed. It aims to narrow down the possible offenders based on the information obtained to describe the physical, psychological and sociological characteristics of the offender and his past and expected future behaviour (Istanoviszki 2012).

3.5. The applicability of AI in the field of public order, public safety and traffic policing

The use of facial recognition, image recognition and video analysis systems are appropriate in the fields of public order, public security and traffic policing. Over the last decades, the presence of public cameras in public spaces, public institutions, shopping centres, public transport, and on busy and less busy roads has become more and more natural. They can help in investigations in the event of crime, accidents or events, as they not only monitor but also record and store the footage for a short period of time, in accordance with the law. However, the examination of these recordings and the detection of the incriminated event or person is time-consuming and manpower-intensive, and there is a greater possibility of human error. Traffic and risk screening can often be used without human intervention to find the searched, or wanted person in a crowd, or even if you signal an accident risk situation, the presence of a device dangerous to public safety, AI can provide the opportunity to carry out the necessary analyses without bias and without distractions or misleading situations.

Two methods are commonly used for face recognition: the pattern-based (or photometric) method, where global features of the face or parts of the face (e.g. eyes, mouth) are compared with stored patterns, and the geometric-based method, where certain details of the face (eyes, nose, chin, etc.) are analysed based on their relative positions and dimensions (Németh – Tóth 2019).

In certain locations or objects, in certain situations, in certain cases, the face, voice, movement or even biometric identification of persons can be of great importance where access is restricted or subject to prior verification. Examples of this are AI-driven systems used in airport passenger screening in several countries, which in addition to identifying persons, also examine their behaviour and facial expressions, and dedicated IT applications that can screen out passengers at risk based on their answers to questions about entry into the country.

In traffic, it can play an essential role in predicting accident-prone locations and vehicle congestion, but also in border protection, anticipating migration flows, marking a more vulnerable border section, and detecting illegal border crossings at night, as these algorithms can work with a much lower error rate.

3.6. Digitisation applications currently available

Compact, modular search/text mining/analysis/evaluation systems using AI are now widely available and can quickly and efficiently process virtually any amount of data, regardless of its format, structure, language or form. Examples of AI applications have already been available in our country including decision-support or signalling AI applications already used by financial institutions to flag account numbers and financial flows that are at high risk of money laundering and fraud, thereby enabling, among other things, financial institutions to meet their obligations to prevent terrorism and money laundering.

These applications, already developed and in use, are able to analyse the detected criteria in relation to the criteria or directions given. In law enforcement, this method will make static databases, which until now have been operated independently, processable and capable of providing correlations and results that could never have been obtained using human resources alone. A comprehensive search/analysis/evaluation system of this kind would provide an opportunity to restructure the already traditional and outdated analysis/evaluation activities while supporting the work of specialised crime prevention, detection and investigation services with increased efficiency.

It is also necessary to talk about the disadvantages of the use of AI in the home country because it is easier to deduce from this which areas AI would be indispensable. In addition to the positive potential of using AI in offender profiling, there can also be drawbacks. While discriminatory and other negative perceptions of a person are formed based on experience or external factors, data on the skin colour, gender identity, and religion of offenders can be more prominent in the database (e.g., creole colour as a definition of skin colour may not only apply to Roma identity.) In New York, a commission on AI found that "AI in decision-making "can help increase efficiency in some areas", but also noted that the increasing use of facial recognition and other algorithm-driven technology in law enforcement and immigration control risk deepening racism and xenophobia and could lead to human rights abuses." (Nick-Cumming 2020)

A further disadvantage of the aforementioned specific profiling is that the AI may make racist assumptions about certain ethnic groups, age, and gender, which may undermine confidence in law enforcement and investigations, mislead investigations and thereby cause greater harm when recording the transcripts of suspect interviews, it is possible to take into account not only the personal data of the person interviewed but also other external characteristics (height, gender, eyes, hair and skin colour, tattoos, gait, etc.) as well as their education, occupation, and marital status.

First of all, we feel it is necessary to clarify that one of the most important steps towards the application of AI has been taken, as there is a clear positive attitude from organisations and authorities. Understanding the (near) future application of AI is inevitable for law enforcement professionals, not only because of the possibility of its use within the organisation but also because of the crucial importance that can be attached to the investigation of crimes committed using AI or the damage and accidents caused by self-driving cars, drones, etc., which are increasingly being mentioned.

In any case, the first thing that needs to be done is to change the legislation, which would allow databases to become interoperable without or with a shortening of the lengthy authorisation procedures in certain cases (sometimes 1-2 days or even 1 week, depending on the workload of the prosecution services), even allowing AI to decide on the granting of authorisations.

The full standardisation of the systems used by law enforcement agencies will be necessary, which would make it easier to train AI, and, after the creation of the appropriate legal framework, the preparation of simplified interrogations, protocols, and expert opinions, which should be filled in, even in the form of questionnaires, instead of long descriptions.

4. Summary

The paper explores the integration of AI into law enforcement, focusing on the European Union's AI Act and its implications, particularly in Hungary. It examines the opportunities, risks, and regulatory challenges associated with deploying AI in policing and crime prevention. One significant focus is the EU AI Act, which categorises law enforcement AI applications as high-risk but exempts systems used for military, defence, or national security purposes. This creates a regulatory gap, as AI systems designed for civilian use could be repurposed for exempt activities without oversight.

The publication delves into prohibited and high-risk AI applications under the AI Act. Notably, the use of real-time biometric identification in public spaces is banned, except under specific conditions such as preventing terrorism or addressing severe public safety threats. Similarly, predictive policing based on personal traits is prohibited due to concerns over discrimination and violations of fundamental rights. High-risk classifications cover tools like post-event biometric identification and criminal profiling systems, which pose challenges in ensuring fairness, transparency, and non-discrimination. Integrating criminal geography with AI enhances law enforcement by using tools like geospatial analysis and hotspot mapping to identify crime patterns, optimise resource allocation, and improve community safety.

In the Hungarian context, while AI has yet to be implemented in law enforcement, the paper outlines potential application areas. These include document management, behavioural analysis, video and image recognition, predictive policing, and open-source intelligence gathering. However, significant challenges remain, such as the lack of interoperability between databases and the need for enhanced legal and technical frameworks.

The paper also explores the potential of AI in offender profiling and predictive capabilities. AI systems could improve the integration of psychological and forensic data for crime detection and prevention. However, the risk of biases in AI outputs raises concerns about discriminatory practices, which could erode public trust and compromise investigative processes.

Technological applications discussed include AI-driven tools for analysing surveillance data, managing traffic, and predicting high-risk situations. Systems like eModus and RobotZsarú demonstrate initial steps in integrating AI into Hungarian law enforcement by enabling pattern recognition and linking criminal databases.

The ethical risks of using AI are a critical concern. Issues such as biases in data, privacy violations, and discriminatory outcomes underline the need for robust governance. The publication highlights the importance of legal reforms, transparency, and oversight to address these challenges effectively.

In conclusion, the paper emphasises that while AI offers significant potential to enhance the efficiency and effectiveness of law enforcement, its deployment must be carefully managed. A balanced approach is essential to harness innovation while safeguarding fundamental rights and maintaining public trust.

References

- Brayne, S.** (2021): *Predict and Surveil: Data, Discretion, and the Future of Policing*. Oxford University Press.
- Collier, B.** (2020): Intelligence-led Policing: Balancing Public Safety and Privacy. *Policing and Society*, 30(4), 401–420.
- Dobó, J. – Gyarakı, R.** (2021): Possibilities of the use of artificial intelligence in the field of law enforcement. *Magyar Rendészeti*, No. 4.
- Egbert, S. – Leese, M.** (2020): *Predictive policing and its origins*. Routledge.
- Egbert, S.** (2018): Predictive Policing and the Politics of Patterns. *Surveillance & Society*, 16(1), 72–91.
- EUFRA:** EU Agency for Fundamental Rights (2022): *Bias in algorithms – Artificial intelligence and discrimination*. Publications Office of the European Union.

Ferguson, A. G. (2017): *The Rise of Big Data Policing: Surveillance, Race, and the Future of Law Enforcement*. NYU Press.

Földesi, Krisztina (2017): *The applicability of biometric identification procedures in police work*. Doctoral thesis. Budapest, Óbuda University.

Georgieva, I. – Timan, T. – Hoekstra, M. (2022): *Regulatory divergences in the draft AI Act – Differences in public and private sector obligations*. [https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729507/EPRS_STU\(2022\)729507_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2022/729507/EPRS_STU(2022)729507_EN.pdf)

Gless, S. (2020): *AI in the courtroom: a comparative analysis of machine evidence in criminal trials*. *Georgetown Journal of International Law*, 51(2), 195–253.

González Fuster, G. (2020): *Artificial intelligence and law enforcement*. [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU\(2020\)656295_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf)

Helberger, N. – Diakopoulos, N. (2023): *ChatGPT and the AI Act*. *Internet Policy Review*, 12(1). DOI: <https://doi.org/10.14763/2023.1.1682>.

Istanovszki, L. (2012): *Crime Analysis in Modern Law Enforcement*. Patrocinium, Budapest, p. 62.

Juhász, Gy. (2022): *The future of data collection for criminalistics, the electronic Modus Operandi Register and research possibilities*. *Belügyi Szemle*, No. 2022/1.

Kiss, A. (1995): *Profiling as a new criminological method?* In: László Pusztai (ed.) *Criminology and Criminalistics Studies 32*. OKRI, Budapest, pp. 217–233.

Leufer, D. – Rodelli, C. – Hídvégi, F. (2023): *Human rights protection...with exceptions: what's (not) in the EU's AI Act deal*. <https://www.accessnow.org/whats-not-in-the-eu-ai-act-deal/> Accessed 5 March 2024.

Mohler, G. O., et al. (2015): *Randomized Controlled Field Trials of Predictive Policing*. *Journal of the American Statistical Association*.

Németh, A.– Tóth, G. (2019): *Application of facial recognition systems*. *Internal Affairs Review*, 67(1), 129.

Nick-Cumming B. (2020): *U.N. Panel: Technology in Policing Can Reinforce Racial Bias*. *New York Times*, 07.12.2020.

Palmiotto, F. (2018): *The black box on trial: the impact of algorithmic opacity on fair trial rights in criminal proceedings*. In M. Ebers – M. Cantero Gamito (Eds.) *Algorithmic governance and governance of algorithms*. Springer.

Raposo, V. L. (2022): The use of facial recognition technology by law enforcement in Europe: a non-Orwellian draft proposal. *European Journal on Criminal Policy*, 29, 515–533.

Sanz, M. B. L. (2022): About ClearviewAI's mockery of human rights, those fighting it, and the need for EU to intervene. <https://edri.org/our-work/we-need-to-talk-about-clearview-ai/>

Sobel, B. L. W. (2021): A new common law of web scraping. *Lewis & Clark Law Review*, 25(1), 147–207.

Solove, D. J. – Hartzog, W. (2024): The Great Scrape: The Clash Between Scraping and Privacy. 113 *California Law Review* (forthcoming 2025). Available at SSRN: <https://ssrn.com/abstract=4884485> or <http://dx.doi.org/10.2139/ssrn.4884485>

Thida, Myo, et al. (2013): Contextual Analysis of Videos: The Detection of Events and Activities. Springer. DOI: 10.1007/978-1-4471-5288-3.

Veale, M. – Borgesius, F. (2021): Demystifying the draft EU Artificial Intelligence Act: analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, 22(4), 97–112.