mgr Jurgita Baltrūnienė
Lecturer, Mykolas Romeris University, Academy of Public Security (Lithuania)
Kaunas Regional Prosecutor's Office Kaunas District Prosecutor's Office, Lithuania
ORCID: 0000-0001-8323-0570

PLACE OF ARTIFICIAL INTELLIGENCE IN THE DETECTION AND INVESTIGATION OF CRIME: THE PRESENT STATE AND FUTURE PERSPECTIVES

Rola sztucznej inteligencji w wykrywaniu i ściganiu przestępstw: stan obecny i perspektywy

Summary
The article analyses an area that has not yet received sufficient scientific attention: the use of artificial intelligence in the investigation of criminal offences. Artificial Intelligence (AI) is a widely discussed topic with rapidly developing technologies that will undoubtedly occupy an important place in criminal investigation and law enforcement activities. Artificial Intelligence (AI) is a rapidly evolving group of technologies. These technologies can provide economic and social benefits in a wide variety of industries and social activities. AI systems are widely used in the interactive world, search engines, digital assistants, computer game development, and security systems, as well as by law enforcement authorities and their techniques. In law enforcement authorities, AI systems are applied in process automation (document analysis, automatically generated messages, etc.), vehicles (automatic license plate scanning, recording of violations), facial recognition systems (in airports, when crossing the state border), robots (automatic demining robots) and internet technologies. Currently, significant investments and resources are being allocated in Lithuania and worldwide in order to improve AI algorithms and usage possibilities[1] in both law enforcement authorities and ordinary people's lives.

Keywords: Artificial Intellect (AI), criminal offence, law enforcement authorities

[1] E. Čivilis et al., *Lithuanian Artificial Intelligence Strategy. A Vision of the Future*, Ministry of Economy and Innovation, 8 March 2019, https://eimin.lrv.lt/uploads/eimin/documents/files/DI_strategija_LT(1).pdf (accessed 01.03.2022).

Introduction

Digital technologies in general and the proliferation of data processing and analytics enabled by artificial intelligence (AI) in particular, bring with them extraordinary promises and risks since AI development has made a big leap forward in recent years, making it one of the strategic technologies of the 21st century, with the potential to generate substantial benefits in efficiency, accuracy, and convenience, and thus bringing positive change to the European economy and society, but also great risks for fundamental rights and democracies based on the rule of law, therefore, AI should not be seen as an end in itself, but as a tool for serving people, with the ultimate aim of increasing human well-being, human capabilities and safety[2]; Many of the Law Enforcing Agencies across the world are using the most up-to-date solutions to prevent crime. One such solution is the 'facial recognition' which is being widely implemented in various sectors other than the law to maintain security. Artificial intelligence in policing is a framework which is evaluated with the help of computers.[3]

The aim of this article is to disclose the challenges of using artificial intelligence in law enforcement authorities. The search for articles was carried out in the scientific database. Due to the rapid development of artificial intelligence technologies, the overview includes the works published in English no later than 5 years ago. The articles selected for analysis have the title and contain the keywords that match the objective of the scientific literature review. Publications selected for the present analysis contained the analysis of the latest AI systems, the amount of data collected and their possible errors; analysis of scientific sources and documents, comparative method, generalisation method.

Artificial Intellect

AI is not a designed replacement for human intellect. It is human-made software[4]. It performs certain functions. The endless potential of AI and the accompanying new solutions should be analysed very carefully, delving into each specific method applied by AI systems. AI can be improved in individual segments rather than as a single system. For a long time, scientists have been looking for ways to make machines as intelligent as possible. At different times, people kept coming up with new ideas. However, these split into separate branches because someone copied other people's

[2] European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters (2020/2016(INI)), https://www.infolex.lt/teise/Default.aspx?Id=1929&crd=1261672 (accessed 16.08.2022).

[3] *How Artificial Intelligence In Policing Helps Crime Detection* INNEFU, 1 February 2021, https://www.innefu.com/blog/how-artificial-intelligence-in-policing-helps-crime-detection (accessed 1.03.2022).

[4] European Commission, *Definition of AI developed by the High-Level Expert Group on Artificial Intelligence at the European Commission*, 7 December 2018, 795 final, https://eur-lex.europa.eu/resource.html?uri=cellar:22ee84bb-fa04-11e8-a96d-01aa75ed71a1.0011.02/DOC_2&format=PDF (accessed 1.03.2022).

ideas.[5] Each of the directions of AI development is important in its own way and is applied in various areas of human activity. With the help of the necessary methods, it is possible to prevent future crimes of various types and to facilitate the investigation of existing crimes.

Currently, there is no single universally accepted concept of artificial intelligence, but it can be defined as a branch of computer science that specializes in decision-making or classification. Machine learning, as a branch of artificial intelligence, is often used for image recognition, when algorithm initially learns from a large database[6]. After the learning process, the algorithm can be applied to analyse the newly uploaded data[7], e.g., search for victims of crime, including missing children, certain threats to the life or physical safety of natural persons or of a terrorist attack, and the detection, localisation, identification or prosecution of perpetrators or suspects of the criminal offences referred to in Council Framework Decision 2002/584/JHA[8] if those criminal offences are punishable in the Member State concerned by a custodial sentence or a detention order for a maximum period of at least three years and as they are defined in the law of that Member State[9].

Artificial intelligence and various intelligent systems, after examining their development, diffusion trends, advantages, are still an incompletely understood phenomenon that raises more questions than provides answers. The word "intelligence" refers to the ability to think, learn and make independent decisions, as this is done by a human being, so it is difficult to understand it as an artificial phenomenon that can perform actions and even make decisions[10]. The extent of the debate is also confirmed by the creation of general artificial intelligence movements, which have even begun to be classified into digital, utopian, technosceptic, and useful artificial intelligence[11].

[5] „Journal of Computer Engineering (IOSR-JCE)" IOSR, 31 May 2015, https://www.iosrjournals.org/#school-overview (accessed 1.03.2022).

[6] M. Wada, Z.Y. Ge, S.J. Gilmore, V.J. Mar, *Use of artificial intelligence in skin cancer diagnosis and management*, „The Medical Journal of Australia" 2020, No. 213(6), p. 256–259, https://doi.org/10.5694/mja2.50759 (accessed 10.10.2022).

7 Ibid.

[8] Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 07 August 2002, p. 1).

[9] Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act) and amending certain Union legislative acts, https://www.infolex.lt/teise/default.aspx?id=1929&crd=1245298&qi=6997231#footnoteref39 (accessed 16.08.2022).

[10] E. Colson, *What AI-Driven decision making looks like*, „Harvard Business Review", 8 July 2019, https://hbr.org/2019/07/what-ai-driven-decision-making-looks-like (accessed 2.04.2022).

[11] M. Tegmark, Life 3.0: *Being Human in the Age of Artificial Intelligence*, London, Penguin Books 2018.

Artificial Intelligence in criminal law and its use by the police and judicial authorities in criminal matters

It is necessary to note that "the design, development, deployment and use of AI must fully respect fundamental rights and existing legal rules.[12] The same degree of protection in the use of AI should be applied in the digital and in the physical world. Under Article 52(1) of the Charter of Fundamental Rights of the European Union, any limitation on the exercise of the rights and freedoms laid down by the Charter may only be made if it is necessary and genuinely satisfies an objective of general interest recognised by the EU or the need to protect the rights and freedoms of others, subject to the principle of proportionality, and must be provided for by law and respect the essence of the fundamental rights and freedoms.[13]

These possibilities have led to a large movement aimed at embedding human intelligence into the field of AI. AI demonstrates the great utility of human rights and law in assessing and addressing complex impacts on society.[14] It also needs to be noted that digital technologies, including AI, can enhance the protection and promotion of fundamental rights and democracy. Digital technologies provide a wider range of public services, by making public services more accessible, more economical, DI can facilitate the documentation of protection violations of fundamental rights, or AI can be used for detecting and countering hybrid threats. Scientists note that the use of AI could facilitate more effective results of the work of law enforcement authorities.[15] More and more financial, human and intellectual resources are being invested in the development of AI, facilitating the tasks performed by law enforcement authorities, which would help ensure public safety at the national and EU levels. It should be noted that the main areas that are of particular interest in terms of the use of AI systems in law enforcement are data analysis systems, as well as the interpretation of new, previously unknown, models and their interfaces.[16] By increasingly enabling AI-based systems in the activities of law enforcement authorities, the data protection rules and the protection of other legal and ethical norms must be ensured and appropriate safeguards must be established. Both private companies and public sector

[12] Council of the European Union, *The Charter of Fundamental Rights in the Context of Artificial Intelligence and Digital Transformation*, 21 October 2020, https://data.consilium.europa.eu/doc/document/ST-11481-2020-INIT/lt/pdf (accessed 1.03.2022).

[13] Ibid.

[14] F.A. Raso, H. Hilligoss, V. Krishnamurthy, Ch. Bavitz, L. Kim, *Artificial Intelligence & Human Rights: Opportunities & Risks*, Berkman Klein Center for Internet and Society at Harvard University, Research Publication No. 2018-6, 25 November 2018, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3259344 (accessed 1.03.2022).

[15] Council of the European Union, *The Charter of Fundamental Rights in the Context of Artificial Intelligence and Digital Transformation*, op. cit., supra note 8.

[16] D. Murauskas, *Dirbtinio intelekto metodai teisės taikymo srityje – galimybes varžo etiniai klausimai (Artificial Intelligence methods in the field of application of the law – opportunities limited by ethical issues)*, „Spektrum" (Vilnius University), 11 November 2019, https://naujienos.vu.lt/dirbtinio-intelekto-metodai-teises-taikymo-srityje-galimybes-varzo-etiniai-klausimai/ (accessed 1.03.2022).

organizations are increasingly using personal data in order to try to understand and predict the behaviour of different groups of people, and to take targeted measures to prevent the activities of certain individuals.

Europol's Organised Crime Threat Assessment and the Annual Threat Landscape Report of the European Union Agency for Cybersecurity (ENISA)[17] note that the scale, frequency and sophistication of cybercrime and attacks are increasing. In 2021 alone, the governments of European countries experienced 198 cyber security incidents, the most important target of which was the public administration sector. Highly skilled and resourceful malicious actors not only from the EU but also from third countries take advantage of the fact that the global open internet has no borders and that the current systems of entities with different jurisdictions are uneven and apply differently. As evidenced by the numerous incidents where criminals targeted vulnerable areas in order to extort money, cyberattacks and cybercrime are often interconnected and pose a constant threat that is constantly changing. Cybercriminals may be motivated simply by increasing opportunities to profit from their activities, while the malicious behaviour of other state and non-state entities is motivated not only by financial gain, but also by more complex geopolitical and ideological ambitions. Data collected by ENISA shows that state-backed hackers targeting public and private supply chains have also reached a "new level of complexity and impact"[18].

The Justice and Home Affairs and Telecommunications Councils held discussions on the Commission's proposed Artificial Intelligence Act. In order to clarify the most difficult issues, the Joint Opinion on the Commission proposal published in June 2021 by the European Data Protection Board and the European Data Protection Supervisor[19] calls for a general ban on the use of AI-based remote biometric identification systems in public spaces. European Parliament resolution of 6 October 2021[20] highlights the risk of bias arising from the use of artificial intelligence applications and algorithms in real-time remote biometric identification systems, and stresses the need for strict, man-made, supervisory and strong legal powers, particularly in law enforcement or in cross-border contexts.

AI is rapidly being integrated into law enforcement authorities in the performance of their functions. However, it should be kept in mind that AI can also have negative effects. For example, improper data collection by AI systems may harm human rights as a result of large amounts of data being collected and possible errors in analysis. Proper data analysis could in many cases save the existing data from bias and discrimination patterns. It should be noted that the creation and development as well as the deployment and use of AI must be in full compliance with fundamental

[17] ENISA – European Union Agency for Cybersecurity.

[18] *ENISA Annual Threat Landscape Report*, 27 October 2021.

[19] Joint Opinion 5/2021 of the European Data Protection Board and the European Data Protection Supervisor on the proposal for a regulation of the European Parliament and of the Council establishing harmonized rules on artificial intelligence (Artificial Intelligence Act).

[20] European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, op. cit.

rights and existing legal rules[21]. Both the digital and physical worlds should provide the same level of protection for the use of AI.

AI applications may offer great opportunities in the field of law enforcement, in particular in improving the working methods of law enforcement agencies and judicial authorities, and combating certain types of crime more efficiently, in particular financial crime, money laundering and terrorist financing, online sexual abuse and exploitation of children as well as certain types of cybercrime, thereby contributing to the safety and security of EU citizens, while at the same time they may entail significant risks for the fundamental rights of people; whereas any blanket application of AI for the purpose of mass surveillance would be disproportionate[22].

It should be noted that the key areas that are of particular interest in terms of the use of AI systems in law enforcement are data analysis systems, as well as the interpretation of new, previously unknown, models and their interfaces[23]. From the information provided, it can be concluded that AI must be protected from possible external influences, and when applying AI it is necessary to ensure personal rights and freedoms. Based on the economic and regulatory power of the EU, joint actions in the development of AI-based systems, coordination activities and joint investments can have a huge potential for European industry, competitive advantage, strengthening the internal market and ensuring security. In addition, the EU standards on AI reliability can be applied worldwide as good practices, in which case AI systems would be developed, adopted and made available to the market, including law enforcement authorities, taking into account the values, principles and legal regulation protected by the EU.

It is necessary to combat inappropriate content online, including hate crimes, while protecting the right to freedom of expression and the right to information. It should be emphasized that it is very important in what circumstances and to what extent the results obtained using the AI system are intended to influence the specific content. In this case, AI systems work only with targeted human intervention.

The activities of law enforcement authorities must first be assessed in accordance with the principle of division. Assessment should not be addressed towards the law enforcement authorities themselves, but towards the functions performed by them in order to implement the tasks set for these authorities.[24] Authors examining the issue of law enforcement functions recognize that the issues of the functions and mutual interaction of law enforcement authorities are among the most important in ensuring the

[21] Council of the European Union, *The Charter of Fundamental Rights in the Context of Artificial Intelligence and Digital Transformation*, op. cit.

[22] European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, op. cit.

[23] D. Murauskas, op. cit.

[24] E. Visockas, *Pasitikėjimas teisėsaugos institucijomis Lietuvoje (Trust in law enforcement authorities in Lithuania)*, „Teisės problemos" 2016, No. 2(2), p. 93–107, https://teise.org/wp-content/uploads/2017/02/Visockas-2016-2.pdf (accessed 1.03.2022).

effectiveness of law enforcement activities.[25] All law enforcement authorities, taking into account the goals and tasks set for them, carry out law enforcement activities, which are revealed through the functions performed.[26] In Lithuania, law enforcement authorities are authorized to implement the law, and it is also stipulated that they must carry out specific activities that are characteristic of each of them and are regulated in the relevant normative acts.[27] Therefore, law enforcement functions should be referred to as the activities involving enforcement of legal norms, defence and protection of human rights and administration of justice, consultation, representation and, where necessary, defence functions.[28]

The said functions indicate that law enforcement authorities are forced to keep up with modern trends and make every effort to ensure that functions are implemented and tasks are carried out in the shortest possible time and as efficiently as possible. To improve the quality of the functions performed, AI applications developed for law enforcement authorities are adapted to increase the effectiveness of activities carried out by law enforcement authorities.

Law enforcement authorities should be able to act in a rapidly changing criminal environment in order to strengthen the protection and security of all individuals.[29]AI--based applications can provide cybersecurity by helping to gather intelligence on potential threats, analysing past experiences, and identifying certain trends in potential risks and threats. AI systems also offer the possibility of reducing the response time to calls, and can facilitate the handling of various calls in accordance with best security practices.

The activities carried out by the police or other law-enforcement authorities are focused mainly on the prevention, investigation, detection or prosecution of criminal offences, including police activities without prior knowledge if an incident is a criminal offence or not. Such activities can also include the exercise of authority by taking coercive measures such as police activities at demonstrations, major sporting events and riots. They also include maintaining law and order as a task conferred on the police or other law-enforcement authorities where necessary to safeguard against and

[25] P. Kuconis, V. Nekrošius, *Teisėsaugos institucijos (Law Enforcement Authorities)*, Justitia, Vilnius 2001.

[26] M. Davies, H. Croall, J. Tyrer, *An Introduction to the Criminal Justice System in England and Wales*, Addison-Wesley Ltd, Boston 2005.

[27] Ibid.

[28] G. Danišauskas, *Teisėsaugos funkcijų vykdančių institucijų rūšys bei teismo vieta šių institucijų sistemoje (Types of authorities carrying out law enforcement functions and the place of the court in the system of these authorities)*, „Socialnių Mokslų Studijos"/„Social Science Studies" 2009, No. 3(3), p. 2–14, https://ojs.mruni.eu/ojs/societal-studies/article/download/1415/1356 (accessed 1.03.2022).

[29] European Commission, *Annex to the Communication from the Commission to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions on the shaping of the European approach to artificial intelligence*, EUR-Lex, 25 April 2018, 237 final, https://eur-lex.europa.eu/legal-content/LT/TXT/?uri=-COM:2018:237:FIN (accessed 1.03.2022).

prevent threats to public security and to fundamental interests of the society protected by law which may lead to a criminal offence. Member States may entrust competent authorities with other tasks which are not necessarily carried out for the purposes of the prevention, investigation, detection or prosecution of criminal offences, including the safeguarding against and the prevention of threats to public security, so that the processing of personal data for those other purposes, in so far as it is within the scope of Union law, falls within the scope of Regulation (EU) 2016/679[30][31].

All member states are members of the International Criminal Police Organization (Interpol). To fulfil its mission, Interpol receives, stores and circulates personal data to assist competent authorities in preventing and combating international crime. It is therefore appropriate to strengthen cooperation between the Union and Interpol by promoting an efficient exchange of personal data whilst ensuring respect for fundamental rights and freedoms regarding the automatic processing of personal data. Where personal data are transferred from the Union to Interpol, and to countries which have delegated members to Interpol, this Directive, in particular the provisions on international transfers, should apply. This Directive should be without prejudice to the specific rules laid down in Council Common Position 2005/69/JHA[32] and Council Decision 2007/533/JHA[33].

The implementation of artificial intelligence in the field of law enforcement and for the needs of judicial institutions should not be considered a purely technically feasible option, but as a political decision on the structure and objectives of law enforcement and criminal justice systems; whereas modern criminal law is based on the idea that authorities only respond to an offence only after it has already been committed, without assuming that all people are dangerous and need constant surveillance to prevent possible offending; whereas AI-based surveillance methods pose a significant threat to this approach, and as such it is imperative that legislators around the world carefully consider the implications of allowing technologies that reduce the human role in law enforcement and judicial decision-making processes.

[30] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (see Official Journal p. 1).

[31] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA, https://www.infolex.lt/teise/default.aspx?id=1929&crd=917855 (accessed 17.08.2022).

[32] Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol (OJ L 27, 29 January 2005, p. 61).

[33] Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 07 August 2007, p. 63).

The European Parliament resolution underlines the fact that many current algorithmically driven identification technologies currently in use disproportionately misidentify and misclassify and therefore cause harm to racialised people, individuals belonging to certain ethnic communities, LGBTI people, children and the elderly, as well as women; recalls that individuals not only have the right to be correctly identified, but they also have the right not to be identified at all, unless it is required by law for compelling and legitimate public interests; stresses that AI predictions based on characteristics of a specific group of persons end up amplifying and reproducing existing forms of discrimination; considers that strong efforts should be made to avoid automated discrimination and bias; calls for robust additional safeguards where AI systems in law enforcement or the judiciary are used on or in relation to minors.[34]

The European Parliament resolution highlights the power asymmetry between those who employ AI technologies and those who are subject to them; stresses that it is imperative that use of AI tools by law enforcement and judicial authorities does not become a factor of inequality, social fracture or exclusion; underlines the impact of the use of AI tools on the defence rights of suspects, the difficulty in obtaining meaningful information on their functioning and the consequent difficulty in challenging their results in court, in particular by individuals under investigation.

AI-based systems and applications are a relatively new area of law enforcement activity. In Lithuania, many law enforcement authorities are already actively investigating the application of AI and the possibility of involving robots in performing certain functions in order to strengthen crime prevention and control. A wide range of AI applications are being developed in line with national crime prevention priorities. The relationship between law enforcement authorities and AI is not unambiguous. Some countries are more advanced than others in terms of the use of these AI technologies.[35]

Applications and algorithms created by the AI model are used in the implementation of the competences of these law enforcement authorities.[36] Law enforcement authorities have different types of systems, one of the components of which are AI algorithms.[37]

It is necessary to pay attention to the risks associated with data leaks, data security breaches and unauthorized access to personal data or other information, such as those related to criminal investigations or court cases, that are processed using

[34] European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, op. cit.

[35] *What is artificial intelligence and how is it used?*, „European Parliament News", 29 March 2021, https://www.europarl.europa.eu/news/en/headlines/society/20200827STO85804/what-is-artificial-intelligence-and-how-is-it-used (accessed 1.03.2022).

[36] European Commission, *Feasibility Study on a Forecasting and Early Warning Tool for Migration Based on Artificial Intelligence Technology*, Publications Office of the European Union, ECORYS, 15 February 2021, https://op.europa.eu/lt/publication-detail/-/publication/5afa29f0-700a-11eb-9ac9-01aa75ed71a1/language-en/format-PDF/source-191372680 (accessed 1.03.2022).

[37] Ibid.

artificial intelligence systems. The safety and security aspects of AI systems used by law enforcement or judicial authorities must be carefully considered and sufficiently robust and resilient to prevent the potentially catastrophic consequences of malicious attacks against AI systems. The importance of security by design, as well as specific human oversight before operating certain critical applications and therefore calls for law enforcement and judicial authorities only to use AI applications that adhere to the privacy and data protection by design principle in order to avoid function creep[38], to establish the correct location of legal responsibility and liability for potential harm, given the complexity of development and operation of AI systems. It is necessary to create a clear and fair regime for assigning legal responsibility and liability for the potential adverse consequences produced by these advanced digital technologies; that the aim must, first and foremost, be to prevent any such consequences materialising to begin with; It is necessary to apply the precautionary principle in all applications of AI in the context of law enforcement, and that legal responsibility and liability must always rest with a natural or legal person, who must always be identified for decisions taken with the support of AI; therefore, there is a need to ensure the transparency of the corporate structures that produce and manage AI systems.

It is essential, both for the effectiveness of the exercise of defence rights and for the transparency of national criminal justice systems, that a specific, clear and precise legal framework regulates the conditions, modalities and consequences of the use of AI tools in the field of law enforcement and the judiciary, as well as the rights of targeted persons, and effective and easily available complaint and redress procedures, including judicial redress. It is necessary to assess the right of the parties to a criminal proceeding to have access to the data collection process and the related assessments made by or obtained through the use of AI applications, it is necessary for executing authorities involved in judicial cooperation, when deciding on a request for extradition (or surrender) to another Member State or non-EU country, to assess whether the use of AI tools in the requesting country might manifestly compromise the fundamental right to a fair trial. The Commission is called to issue guidelines on how to conduct such an assessment in the context of judicial cooperation in criminal matters; and insists that Member States, in accordance with applicable laws, should ensure that individuals are informed when they are subject to the use of AI applications by law enforcement authorities or the judiciary;

If humans only rely on the data, profiles and recommendations generated by machines, they will not be able to conduct an independent assessment. There exist potentially grave adverse consequences, specifically in the area of law enforcement and justice, when individuals overly trust in the seemingly objective and scientific nature of AI tools and fail to consider the possibility of their results being incorrect, incomplete, irrelevant or discriminatory. It is emphasised that over-reliance on the results provided by AI systems should be avoided, and that the authorities should build confidence and knowledge to question or override an algorithmic recommendation,

[38] European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters, op. cit.

and it is important to have realistic expectations on such technological solutions and not to promise perfect law enforcement solutions and detection of all offences committed.

The datasets and algorithmic systems used when making classifications, assessments and predictions at the different stages of data processing in the development of AI and related technologies may also result in differential treatment and both direct and indirect discrimination of groups of people, especially as data used to train predictive policing algorithms reflects ongoing surveillance priorities and consequently may end up reproducing and amplifying current biases. AI technologies, especially when deployed for the use of law enforcement and the judiciary, require inter-disciplinary research and input, including from the fields of science and technology studies, critical race studies, disability studies, and other disciplines attuned to social context, including how difference is constructed, the work of classification, and its consequences; therefore, it is necessary to systematically invest in integrating these disciplines into AI study and research at all levels; stresses also the importance for the teams that design, develop, test, maintain, deploy and procure these AI systems for law enforcement and judiciary of reflecting, where possible, the diversity of society in general as a non-technical means to reduce the risks of discrimination[39].

Predictive policing is among the AI applications used in the area of law enforcement and helps them to ensure more effective and active work, but warns that while predictive policing can analyse the given data sets for the identification of patterns and correlations, it cannot answer the question of causality and cannot make reliable predictions on individual behaviour, and therefore cannot constitute the sole basis for an intervention. Several cities in the United States have ended their use of predictive policing systems after audits. During the Civil Liberties, Justice and Home Affairs Committee's mission to the United States in February 2020, Members were informed by the police departments of New York City and Cambridge, Massachusetts, that they had phased out their predictive policing programmes due to a lack of effectiveness, discriminatory impact and practical failure, and had turned instead to community policing. This led to a decline in crime rates; although opposes the use of AI by law enforcement authorities to make behavioural predictions on individuals or groups on the basis of historical data and past behaviour, group membership, location, or any other such characteristics, thereby attempting to identify people likely to commit a crime.

AI has great potential in the application of recognition functions.[40] The use of these tools in law enforcement shortens investigation time, and also eliminates human error and the element of human fatigue.[41] The use of these tools reduces the need

[39] Ibid.

[40] D. González Fuster, *AI and Law Enforcement: Impact on Fundamental Rights*, European Parliament ThinkTank, 7 July 2020, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656295/IPOL_STU(2020)656295_EN.pdf (accessed 1.03.2022).

[41] R. Jenkins, D. Purves, *Artificial Intelligence and Predictive Policing: A Roadmap for Research*, Ethics+Emerging Sciences Group, 30 September 2020, http://aipolicing.org/year-1-report.pdf (accessed 1.03.2022).

for human resources of the institutions and is economical, as there is no need for a physical officer to perform such functions. AI is based on algorithms, and as the use of these systems expands, a larger database of information about certain crimes is created.[42] The most promising application of AI to law enforcement is the ability to identify and explain potentially dangerous acts, thus creating an opportunity to better predict and prevent crimes. This ability to predict criminal acts before they occur is known as predictive policing.[43]

In predictive policing, AI algorithms are used to identify and sort large amounts of data about various activities, and AI algorithms can also be used to identify people who may pose a threat. Such processes are known as risk or potential threat assessment. It is important to note that the collected historical data used to develop the algorithms raises serious concerns about the authenticity of the data. In particular, the data provided may be inaccurate as law enforcement officials may enter it incorrectly into the algorithmic system, particularly as crime data is often fragmented and unusable.[44]

The application of AI systems in the State Border Guard Service is not a novelty, these technologies are improved every year. The State Border Guard Service uses various types of technical applications that work with the help of algorithms developed by AI systems. In the literature, most of the information is provided about the technologies of identification of violations. These technologies are installed at state border checkpoints. The physical protection of the state border is usually ensured in various ways: boundary signs in the waters, control tracks, land posts in both forested areas and lawns, as well as by various types of barriers.[45] The state constantly strengthens physical border control, but control methods and measures change very often both within the state and outside the designated territory.[46] State border control is extended beyond the demarcated borders and is carried out using a wide range of

[42] C. Rudin, *Predictive policing: Using machine learning to detect patterns of crime*, „Wired", 2 July 2021, https://www.wired.com/insights/2013/08/predictive-policing-using-machine-learning-to-detect-patterns-of-crime/ (accessed 1.03.2022).

[43] Ch. Rigano, *Using Artificial Intelligence to address criminal justice needs*, „National Institute of Justice Journal", 17 January 2019, https://www.ojp.gov/pdffiles1/nij/252038.pdf (accessed 1.03.2022).

[44] M. Leese, *Predictive policing: Proceed, but with care, „Policy Perspectives"*, 6 December 2020, https://www.researchgate.net/publication/347443927_Predictive_Policing_Proceed_but_with_Care (accessed 1.03.2022).

[45] Resolution "On the Approval of the Description of the Procedure of Establishment of the Form, Size and Placement of the State Border Signs Marking the Border of the Republic of Lithuania on Land and in the Border Waters", Government of the Republic of Lithuania, Official Gazette „Valstybės žinios", 21 March 2007, No 44-16, https://e-seimas.lrs.lt/portal/legalAct/lt/TAD/TAIS.295850/asr (accessed 1.03.2022).

[46] B. Ainhoa Ruiz, M. Akkerman, P. Brunet, *A Walled World: Towards a Global Apartheid Report,* Transnational Institute, 18 November 2020, https://www.tni.org/en/walledworld (access 1.03.2022).

remotely controlled systems[47] such as pre-departure registration, remote inspection and digital monitoring of incoming and outgoing objects. This monitoring can ensure order and prevent violation of the existing requirements. The border protection functions are also supported by the technologies used in the border service for the identification, profiling and risk analysis of biometric data. Remote identification of people posing any risk, from a historical perspective, has emerged quite recently with the introduction of various technologies in the State Birder Guard Service that operate on the basis of AI systems. This technology for monitoring the persons crossing the state border is designed to identify individuals. The primary need for modern state border protection is to identify the persons who enter the states.[48] Such applications of technology are based on the fact that it becomes possible to control persons crossing the state border and identify their possible illegal goals, ensuring security against terrorism and other attacks.[49] The problems of identification of persons have become especially relevant recently in the context of illegal migration, when persons began to cross national borders en masse using forged or invalid documents.[50] Therefore, the state border protection system uses more and more new AI technologies, which is encouraged at the EU level, paying particular attention to ensuring the safe use of AI systems.[51]

Conclusions

1. A frequent subject of discussions and research is AI technology and the systems underlying it, which receive varying degrees of appreciation from lawyers, researchers and practitioners. Some authors, when defining the concept of AI, emphasize the independence of information technology in making intelligent decisions, others emphasize the human influence on AI systems when they analyse and find the necessary information from the available data set when making the relevant decision. The concept of AI is not yet accurate. In order to properly define it, it is necessary to analyse the principles of its operation. At the moment, attempts are being made at the level of the European Union to assess the concept of AI and to define the principles of operation.

2. Law enforcement authorities often encounter AI systems, with their help they ensure public order and solve various crimes, analyse potential threats. When applying

[47] A.R. Zolberg, *Managing a world on the move*, „Population and Development Review", 15 July 2006, https://www.jstor.org/stable/20058950 (accessed 1.03.2022).

[48] J.C. Scott, *Seeing like a State: How Certain Schemes to Improve the Human Condition Have Failed*, Yale University Press, New Haven 2008.

[49] A. Shachar, *Borders in the time of COVID-19*, „Ethics and International Affairs", 8 March 2020, https://www.ethicsandinternationalaffairs.org/2020/borders-in-the-time-of-covid-19/ (accessed 1.03.2022).

[50] A. Todorov, *Face Value: The Irresistible Influence of First Impressions*, Princeton University Press, Princeton 2017.

[51] K. Crowford, *Time to regulate AI that interprets human emotions*, „Nature", 6 April 2021, https://www.nature.com/articles/d41586-021-00868-5 (accessed 1.03.2022).

AI-based systems in law enforcement authorities, problems may arise due to the application of these systems since human rights may be violated or restricted. All countries in the world face this problem, but some countries have established more specific legal norms that ensure the legality of AI technologies and their systems, while others do not have sufficient legal regulation. When applying the legislation governing AI activities, law enforcement authorities must take into account the correct and legal use of these systems. Each law enforcement authority, both foreign and Lithuanian, applies AI-based systems differently, using different legal instruments. Human rights violations are therefore possible in the application of these systems.

3. When examining the limits of law enforcement authorities with regard to protection of personal data when using AI, the paper mentions human rights and freedoms, which are provided for in the EU Charter of Fundamental Rights, and from which the common constitutional traditions and international obligations of the EU Member States to ensure the proper execution of rights arise. In this case, the development of AI systems and technologies must be carried out in such a way that human rights and freedoms are not violated. The protection of human rights, including the right to self-determination and autonomy, are among the most important rights that should be protected in the digital era. Therefore, when regulating the operation of AI systems, it is recommended to ensure the dignity of the person and the protection of his data.

Bibliography

Literature

Ainhoa Ruiz B., Akkerman M., Brunet P., *A Walled World: Towards a Global Apartheid*, Report, Transnational Institute, 18 November 2020, https://www.tni.org/en/walledworld (accessed 1.03.2022).

Čivilis E. et al., *Lithuanian Artificial Intelligence Strategy. A Vision of the Future*, Ministry of Economy and Innovation, 8 March 2019.

Colson E., *What AI-driven decision making looks like*, „Harvard Business Review", 8 July 2019.

Crowford K., *Time to regulate AI that interprets human emotions*, „Nature", 6 April 2021.

Danišauskas G., *Teisėsaugos funkcijų vykdančių institucijų rūšys bei teismo vieta šių institucijų sistemoje (Types of authorities carrying out law enforcement functions and the place of the court in the system of these authorities)*, „Socialnių Mokslų Studijos"/„Social Science Studies" 2009, No. 3(3).

Davies M., Croall H., Tyrer J., *An Introduction to the Criminal Justice System in England and Wales*, Addison-Wesley Longman Ltd, Boston 2005.

González Fuster G., *Artificial Intelligence and Law Enforcement: Impact on Fundamental Rights*, European Parliament ThinkTank, 7 July 2020.

How Artificial Intelligence in Policing Helps Crime Detection, INNEFU, 1 February 2021.

Jenkins R., Purves D., *Artificial Intelligence and Predictive Policing: A Roadmap for Research*, Ethics+Emerging Sciences Group, 30 September 2020.

„Journal of Computer Engineering (IOSR-JCE)" IOSR, 31 May 2015 (accessed 1.03.2022).

Kuconis P., Nekrošius V., *Teisėsaugos institucijos (Law Enforcement Authorities)*, Justitia, Vilnius 2001.

Leese M., *Predictive policing: Proceed, but with care*, „Policy Perspectives", 6 December 2020.

Murauskas D., *Dirbtinio intelekto metodai teisės taikymo srityje – galimybes varžo etiniai klausimai (Artificial Intelligence methods in the field of application of the law – opportunities limited by ethical issues)*, „Spektrum" (Vilnius University), 11 November 2019.

Raso F.A., Hilligoss H., Krishnamurthy V., Bavitz Ch., Kim L., *Artificial Intelligence & Human Rights: Opportunities & Risks*, Berkman Klein Center for Internet and Society at Harvard University, Research Publication No. 2018-6, 25 November 2018 (accessed 1.03.2022).

Rigano Ch., *Using Artificial Intelligence to address criminal justice needs*, „National Institute of Justice Journal", 17 January 2019, https://www.ojp.gov/pdffiles1/nij/252038.pdf (accessed 1.03.2022).

Rudin C., *Predictive policing: Using machine learning to detect patterns of crime*, „Wired", 2 July 2021, https://www.wired.com/insights/2013/08/predictive-policing-using-machine-learning-to-detect-patterns-of-crime/ (accessed 1.03.2022).

Scott J.C., *Seeing like a State: How Certain Schemes to Improve the Human Condition Have Failed*, Yale University Press, New Haven 2008.

Shachar A., *Borders in the time of COVID-19*, „Ethics and International Affairs", 8 March 2020 https://www.ethicsandinternationalaffairs.org/2020/borders-in-the-time-of-covid-19/ (accessed 1.03.2022).

Tegmark M., Life 3.0: *Being Human in the Age of Artificial Intelligence*, Penguin Books, London 2018.

Todorov A., *Face Value: The Irresistible Influence of First Impressions*, Princeton University Press, Princeton 2017.

Visockas E., *Pasitikėjimas teisėsaugos institucijomis Lietuvoje (Trust in law enforcement authorities in Lithuania)*, „Teisės problemos" 2016, No. 2(2).

Wada M., Ge Z.Y., Gilmore S.J., Mar V.J., *Use of artificial intelligence in skin cancer diagnosis and management*, „The Medical Journal of Australia" 2020, No. 213(6).

What is Artificial Intelligence and how is it used?, „European Parliament News", 29 March 2021.

Zolberg A.R., *Managing a world on the move*, „Population and Development Review", 15 July 2006, https://www.jstor.org/stable/20058950 (accessed 1.03.2022).

Sources of law

Council Common Position 2005/69/JHA of 24 January 2005 on exchanging certain data with Interpol (OJ L 27, 29 January 2005, p. 61).

Council Decision 2007/533/JHA of 12 June 2007 on the establishment, operation and use of the second generation Schengen Information System (SIS II) (OJ L 205, 07 August 2007, p. 63).

Council Framework Decision 2002/584/JHA of 13 June 2002 on the European arrest warrant and the surrender procedures between Member States (OJ L 190, 18 July 2002, p.1).

Council of the European Union, *The Charter of Fundamental Rights in the Context of Artificial Intelligence and Digital Transformation*, 21 October 2020 (accessed 1.03.2022).

Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.

ENISA Annual Threat Landscape Report, 27 October 2021.

European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters [2020/2016(INI)].

European Commission, *Definition of AI developed by the High-Level Expert Group on Artificial Intelligence at the European Commission*, 7 December 2018, 795 final.

European Parliament resolution of 6 October 2021 on artificial intelligence in criminal law and its use by the police and judicial authorities in criminal matters [2020/2016(INI].

European Commission, *Annex to the Communication from the Commission to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions on the shaping of the European approach to artificial intelligence*, EUR-Lex, 25 April 2018, 237 final.

European Commission, *Feasibility Study on a Forecasting and Early Warning Tool for Migration Based on Artificial Intelligence Technology*, Publications Office of the European Union, ECORYS, 15 February 2021.

Joint Opinion 5/2021 of the European Data Protection Board and the European Data Protection Supervisor on the proposal for a regulation of the European Parliament and of the Council establishing harmonized rules on artificial intelligence (Artificial Intelligence Act).

Proposal for a regulation of the European Parliament and of the Council laying down harmonised rules of Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts.

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (see Official Journal p. 1).

Resolution "On the Approval of the Description of the Procedure of Establishment of the Form, Size and Placement of the State Border Signs Marking the Border of the Republic of Lithuania on Land and in the Border Waters", Government of the Republic of Lithuania, Official Gazette „Valstybės žinios", 21 March 2007, No 44-16.

Conflict of interest

None

Source of funding

None