Pakistan Journal of Criminology
Vol. 16, No. 04, October—December 2024 (619-631)

The Use of Artificial Intelligence in Investigating, Combating and Predicting Crimes

Eldar Šaljić[1], Duško Tomić[2]

Abstract

Artificial intelligence in law enforcement can be harnessed due to its powers to faster classify, analyze, evaluate and interpret large data sets and information, which are the main pillars of national and international law enforcement authorities. This article presents application use cases for AI in criminal investigations against extremists and cyber criminals. An outlook into combatting crime is presented through the case of an AI tool made to combat child abusers on the dark web. Additionally, the article presents the predictive measures of artificial intelligence to aid law enforcement agencies in evaluating online behavior and predicting where crimes might occur before any real victims emerge. The article presents conclusions and recommendations for law enforcement applications and future research in a similar area.

Keywords: AI, investigation, combating, predicting crimes

Introduction

While the idea of machine learning and artificial intelligence was proposed by Alan Turing after his research on computer systems during the Second World War, significant breakthrough was achieved in the 2010s and the 2020s, when Big Tech companies and other developers were able to create artificial intelligence software that was able to come close to resemble human behavior. Today, companies commercialize artificial intelligence by incorporating it into different forms of software and achieve higher results for web searching, image processing, translating and interpreting, but also in analysis and data evaluation (Faghiri, 2022).

Artificial intelligence has become one of the most important tools of the "smart world" in the 2020s, being found in mobile phones and all kinds of software and being utilized by different subjects for tasks of high analytical difficulty (Akhgar et al. 2021). Therefore, it is only natural that in criminal justice and criminal investigations, artificial intelligence and its supreme analytical

[1] American University in the Emirates. Academic City. PO Box: 503000, Dubai, UAE. eldar.saljic@aue.ae
[2] American University in the Emirates. Academic City. PO Box: 503000, Dubai, UAE. dusko.tomic@aue.ae

abilities are the next breakthrough aid for law enforcement when it comes to crime analysis and criminal investigation.

Today, law enforcement agencies and governments must create new regulations and adapt to the digital age and the use of non-human agents in certain types of crimes. Artificial intelligence models can be utilized in criminal investigations for forensic analysis of collected data, which can also be used to evaluate financial crime and / or organized crime and its financial involvement (e.g. money laundering, corruption, etc.). Furthermore, artificial intelligence can be involved in criminal investigations when DNA sampling or DNA deviations are expected, as well as when gunshot patterns and the gun connected to should be investigated (Akhgar et al., 2021).

It is because of its abilities for data processing, evaluation, and pattern recognition that criminal investigators ought to use artificial intelligence when investigating, combatting, and predicting crime. Given that the introduction and the use of artificial intelligence in criminal investigations is inevitable, this article researches the possible use cases of AI in criminal investigations by presenting different applications of artificial intelligence in different aspects: criminal investigation, fight against crime, and prediction of crimes.

Research questions

This paper will aim to answer the following research questions:

1. How can artificial intelligence best be used in criminal investigations?

2. In what way can artificial intelligence be used to fight crime?

3. Can artificial intelligence be used to predict crime?

Methodology

The information obtained in this article was collected through the literature review method, as well as the critical evaluation of the use cases for recommendations for future research and future applications for law enforcement. The paper uses a qualitative approach with the aim of providing a starting point for more direct future research in the field of artificial intelligence in criminal justice. Additionally, the paper uses an exploratory approach in the field of artificial intelligence in criminal justice to classify and explore the fields in which artificial intelligence can be applicable in investigating, combatting and predicting crime.

To reach the conclusions and answer the research question, the paper uses the findings after the critical analysis of the most recent literature in the field of artificial intelligence and criminal investigations and crime predictions. This paper analyzed the most recent sources from peer-reviewed journals and online articles. Furthermore, the paper analyzed and extracted cases and examples about the use of artificial intelligence in context of criminal justice and in the case of crime prediction.

The purpose of this paper is to provide a qualitative base for future research and to provide guidance for additional approaches to fighting and combatting crime, and reaches the discussions through the exploratory literature review method of the most recent peer-reviewed journal articles and other secondary sources.

Literature Review

Mijwil and Aljanabi (2023) attempted to present certain views of the artificial intelligence ChatGPT by presenting its ways to combat cybersecurity. The article summarizes cyberspace into different layers and then adds an article written by ChatGPT (2023). The suggestions given by ChatGPT (2023) can be classified as general knowledge fed into artificial intelligence, without certain breakthrough suggestions (e.g. regular assessments, cooperation with law enforcement, encrypting data, collaboration with law enforcement, education of employees, etc.). The article did not provide much insight into the practice of using AI to combat cybersecurity but showed more sophisticated artificial intelligence is in summarizing information and presenting it in a scientific way. The article concluded by presenting how researchers may collaborate with AI in the future regarding better cybersecurity and analyzing suggestions given by artificial intelligence such as ChatGPT (Mijwil, Aljanabi, & ChatGPT, 2023).

Al Qatanaweh et al., (2023) investigated crimes involving the use of artificial intelligence and whether criminal justice is prepared to act on the national and international level. The research also investigated the challenges of crimes involving the use of artificial intelligence and presented legislative and practical ways in which the judicial system can be adapted to include and prosecute criminal actors using artificial intelligence. The researchers made aware in their research that artificial intelligence can also be used for malicious purposes and in criminal activities, such as hacking, data theft, and / or identity theft. Furthermore, the researchers made clear that legally, it is difficult to prove that artificial intelligence was used for certain crimes, resulting from the difficulty to prosecute and classify different forms of hacking on national and international levels (Al Qatawneh et al., 2023). Nevertheless, the paper calls for a unified

framework and inclusion of artificial intelligence as a player in criminal investigations, which would result in an easier way to identify the use of artificial intelligence in criminal operations and would adapt an international approach to combat the malicious use of artificial intelligence.

Naseer & Shaheen (2023) investigated the role of artificial intelligence in the fight against violent extremist behavior on the internet. The method they have described is called Natural Language Processing. The authors claim that this use of AI aims to study how other computers and humans use language in their behavior online. Furthermore, this method would allow to identify threatening language use or extremist language use posted online, flagging the users and their computers as suspicious in the process (Naseer & Shaheen, 2023). The paper concludes with the suggestion of how to effectively use artificial intelligence to prevent violent extremist activity online, some of which are very effective and can help law enforcement to effectively point out suspicious online accounts and investigate them to determine whether these users can be a threat to society and national security (n.d.). Furthermore, the paper calls for international cooperation due to the fact that artificial intelligence is a global phenomenon and that the future crimes using artificial intelligence will be international and will not know state borders.

Balturiene (2022) investigated the role of artificial intelligence in criminal investigations and found that some law enforcement agencies already use artificial intelligence for tasks that would require much more time if done by humans or *simple* computers. Artificial intelligence is used in automated processes like analyzing documents, generating automatic messages, license plate scanning, facial recognition systems and law enforcement robots for bomb defusal or pattern recognition in criminal investigations. The researcher indicates that the Lithuanian state police started using artificial intelligence when processing crimes involving stolen vehicles from Western Europe and the United States of America. The program used conducts a search and possible deviations of vehicle identification numbers (VINs) when scanning newly registered cars (Lithuania is a common place for importing and repairing stolen vehicles from the West before turning them over to other Eastern European countries) (Baltruniene, 2022). Additionally, artificial intelligence is being used at airports for facial recognition, which is the case in Lithuania and in the United Arab Emirates (n.d.). This article shows the current state of AI in law enforcement and in criminal investigation. It further indicates that technology needs to be further developed but is limited to the ethical constraints of full implementation of AI into criminal investigations. According to the author, the correct and legal use of artificial intelligence systems for criminal investigations must be defined in such a way to protect human rights.

Furthermore, this means that internationally, states must define an ethical framework for artificial intelligence, which is already occurring in the European Union. These changes would lead into a digital era of AI in criminal investigations and predictions with the ethical considerations for protecting humans and considering human rights when applying artificial intelligence (Baltruniene, 2022).

Faghiri (2022) researched artificial intelligence and its applications for police and law enforcement. Additionally, the researcher investigated the role of artificial intelligence in the legislation of the United Arab Emirates and its use in criminal justice and sentencing. The aim of the paper was to suggest the necessity application of artificial intelligence in criminal justice and criminal investigations in the UAE. The research indicated that artificial intelligence could provide help in criminal investigations in collating information and collating data to analyze large data sets and facts connecting crime to certain suspects. Furthermore, artificial intelligence can help in surveillance of large areas and singling out certain behavioral aspects that might stand out from common public behavior (Faghiri, 2022). Additionally, the United Arab Emirates use artificial intelligence to monitor and analyze traffic to reduce traffic jams occurring in the country and ensure that the traffic flows in a controlled fashion. Furthermore, artificial intelligence is used in image recognition and the recognition of registration plates when investigating traffic violation in the UAE (Faghiri, 2022). However, the researcher warns that the use of artificial intelligence in predicting crimes could lead to violations against privacy and private data being compromised. Hence, the author calls for the UAE to redefine the framework for the use of artificial intelligence and adapt it to the laws dealing with personal data and criminal investigations. The research recommends that the UAE must develop the use of artificial intelligence in policing and in criminal investigations, and that it must redefine the current and existing laws for cybercrime and criminal prosecution to include the protection of personal data and define the ethical borders when prosecuting criminal behavior with the application of artificial intelligence (Faghiri, 2022).

Kobis et al., (2022) provided a concrete example of using artificial intelligence to investigate corruption cases. The research paper provides an insight into one case of how artificial intelligence can be used to help and support criminal investigations that require the analysis of large data sets and various sources of information and behavior. According to the paper, there are two approaches to use AI to investigate corruption cases, whereas the first approach is being conducted “top-down” (implemented by government and law enforcement) or “bottom-up” (by common citizens or by journalists) (Kobis et al., 2022). The

research paper presents certain suggestions where AI can be implemented by criminal investigators to monitoring and surveillance of suspected individuals by improving the time of data processing and information analysis, while journalists and NGOs (non-governmental-organizations) can use artificial intelligence to analyze data from an external point – by analyzing the statements of certain companies and individuals and compare it to their behavior (Kobis et al., 2022). However, the paper concludes that both approaches are still in their infancy and that it will take time to define and regulate the judicial framework for using artificial intelligence in investigating corruption. Top-down approaches could lead to misuse cases by government and law enforcement to decrease privacy and minimize private data protection, while bottom-up approaches could lead to increased distrust in governmental bodies, which could, in return, threaten the internal security and stability of countries.

Further use cases for the use of AI to combat criminal behavior are found in Androschchuk, et al., (2022). The researchers presented a use case for artificial intelligence in combatting transnational crimes across Ukrainian borders. Furthermore, the example details the use of artificial intelligence to extract information and data by analyzing resources and communications online. According to the authors, the use of artificial intelligence in cross-border organized crime has led to an increase in efficiency of 20% (Androschchuk, Balendr, Grinchenko, Farion, & Mostovyi, 2022). Although the paper was more of a technical nature, qualitative insights were given in a model that would use artificial intelligence to determine organized crime cases based on mathematical models (n.d.). However, the model was just able to reorganize the border patrol officers and renew the models of shift organization by analyzing the highest probability of smuggling and other organized crime activities (n.d.). The Ukrainian border patrol was able to increase efficiency by 20% through a reorganization of placing more officers in times of possibly increased activity, while reducing them in times of reduced organized-crime activity.

Findings: AI in Criminal Investigations and Fight Against Crime

As discussed, the abilities of artificial intelligence for much faster analysis and processing of data and information are beneficial for law enforcement in their criminal investigations. Therefore, it can be said that law enforcement of the future would rely on artificial intelligence and its support when analyzing the collected data in different criminal cases. There are several examples of how AI can be used in different criminal investigations that are presented below.

Corruption and financial fraud

Artificial intelligence can aid law enforcement in investigating corruption and financial criminal cases by analyzing the financial data and statements given by businesses and individuals with the obligation to make financial statements (e.g. politicians). By analyzing the presented data and comparing it with the actions of the suspects, artificial intelligence models can verify whether the investigated subject has conducted financial fraud or corrupt actions. Additionally, artificial intelligence models can be used in forensic accounting to investigate fraudulent activities such as financing of terrorism or organized crime, money-laundering and other fraudulent financial activities (Kobis et al., 2022).

Public Safety and Protection

Artificial intelligence can be used to protect public places and ensure the safety of citizens in public by analyzing surveillance footage. Video evidence and surveillance footage have become some of the most valuable pieces of evidence in criminal investigations (Back, 2022). However, large-scale investigations on an international or global scale require the analysis of large amounts of data, which in return requires more personnel and investigators to be included in the investigation. Artificial intelligence possesses the ability to analyze large amounts of data in a short time when being fed the patterns (including movement, facial expression, body language, etc.). Hence, when investigating organized crime, artificial intelligence can analyze surveillance footage of large public areas, pinpoint suspicious behavior and evaluate whether the actions taken represent elements of organized crime or not (Back, 2022).

Creating Online Personas

Criminal investigations sometimes involve law enforcement officers investigating undercover in different environments (Baltruniene, 2022). Online communications on the surface web (accessible via the common browsers and search engines) can be searched and evaluated with algorithms. However, a sub-section of the internet, believed to be larger than the surface web is the dark web. The dark web is a collection of pages that are not indexed and not accessible to common search engines. Thus, they cannot be accessed with the most common browsers. Furthermore, the information about the location of the websites and the servers hosting them remains mostly hidden, since the dark web uses certain routing techniques that hide the identity of the users and their real location (Akhgar et al., 2021). Ever since its conception, the dark web was the most common way of communication and information exchange for organized crime groups and criminal activities (selling of narcotics, stolen goods, fake identities, etc.) (Davis & Arrigo, 2021). A large aspect of dark web crime is the sexual abuse

of children, and according to researchers, the number of websites and material shared on the dark web outreaches the number of available law enforcement officers to investigate them (Akhgar et al., 2021).

Investigations like child sexual abuse on the dark web can put high psychological strains on the investigators, and such criminal investigation requires the presence of many investigators. Artificial intelligence can offer support in such investigations where it can learn to operate on the dark web and through the creation of online personas which would impersonate users on dark web forums and aim to communicate with other users, offering information to investigators and increasing the steps in the persuade, making the response time and identification of the offenders much faster (Zlate, 2022). One such case is the case of "Sweety", which is an online identity created by programmers of activists fighting against child abuse online. Sweety was an account on a website that is used to facilitate online sex tourism between interested persons and minors offering webcam chats (Akhgar, Gercke, Vrochidis, & Gibson, 2021). The interested parties contacted Sweety with the intent of a webcam conversation. Sweety, an account that is controlled by activists, was aiming to move the conversation to an online messenger on the surface web, while also providing information to law enforcement about the identity and the location of the offenders (Zlate, 2022).

Since artificial intelligence can create independent models that can communicate and interacting with human users, the case of Sweety can be updated and improved to function autonomously and investigate the activities, analyze the chats, comparing patterns, and using certain tools to create background analyses and investigate the location of the servers and the users. Furthermore, artificial intelligence models can also communicate directly to and with the users. This would enable artificial intelligence to create reports and collect as much data as possible. The data would then be provided to law enforcement officials with files and suspicious online activities in the dark web, where investigators could further evaluate and decide what steps can be undertaken. Given the fact that artificial intelligence has become sophisticated in its communication and interaction with humans, it could be possible to utilize its communication capabilities to communicate with many more offenders and suspects than it would be done by human investigators. It remains an under-investigated field that promises to create additional capacities for law enforcement and the fight against dark web criminal activities.

There are of course other use cases where artificial intelligence can be utilized in criminal investigations and the fight against crime using AI. These would include improved DNA analysis, where artificial intelligence programs

would evaluate not just the DNA samples provided to law enforcement but could also calculate slight deviations in DNA and would predict certain DNA deviations that might be available but not known to law enforcement (Abate, et al., 2023). This would compare similar DNA results and could evaluate whether the DNA sample on file at the law enforcement can be of similar origin or of similar abilities. In return, these results could provide information about the heritage and the origin of the suspects whose DNA was found in crime scenes (Back, 2022). Another aspect of utilizing AI in criminal investigations is the investigation of gunshot patterns and gun detections. When certain patterns can be fed into artificial intelligence, it would be able to analyze certain patterns in crimes where a gun has been used and could reveal what sort of gun was used to commit certain crimes (n.d.).

Artificial intelligence in crime prediction

Predicting crime and predicting criminal activities has been the subject of sci-fi novels and movies in the early 2000s. However, with the rise and the improvement of artificial intelligence in the late 2010s, predicting crimes using artificial intelligence seems to be the next step in developing AI models that would work with and for criminal investigators.

In this domain, there is a certain duality present – artificial intelligence is a set of computer programming powered by interlinked networks that calculate and form responses coherent to the amount of data and analysis fed to them. On the other hand, criminal investigations deal with human actors and organizations, where there is much more deviation, and many more dynamics involved. Nevertheless, there has been development in artificial intelligence used in a different domain to evaluate certain data sets of persons and predict their decision making through neural networks, which could be applicable to criminal investigations. Such practice is being used in business data analytics, where companies try to predict the products associated with certain demographics (Ivliev et al., 2023). The procedure involves a neural network and a dataset with common information (age, sex, income level, health data, marital status, etc.). Based on the dataset, neural networks and artificial intelligence is used to evaluate the common choice certain types of persons could choose or which persons might be more responsive to certain products offered (Abate et al., 2023).

The same sets could also be used to predict which demographics or individuals would be more likely to commit certain crimes, and which types of persons could be more likely to be associated with certain types of criminal behavior. One could also create a dataset that contains similar data as in the sets previously described. Additionally, the neural network would have to be fed with

data and information about previous cases and the demographics of the perpetrators to be able to associate certain types with certain crimes. Then, the artificial intelligence could indicate which demographics can be mostly associated with certain types of criminal behavior – e.g. low-income citizens from low-income families could be more likely to commit organized crime or robberies, whereas high-income citizens might be more likely to commit financial fraud or be high-level officials in criminal organizations.

Discussion: Ethics in the Use of Artificial Intelligence

So far, the paper has presented the use cases of artificial intelligence in crime investigation and criminal investigations. However, the fact that artificial intelligence and its use must be done cautiously and carefully with utmost consideration for ethics and human rights must not be forgotten, as well as the fact that criminal investigations always investigate humans and their criminal actions – these may or may not use technology, machines, and computers to reach their criminal goals, but there is still a human controller behind them, giving the orders.

Several of the literary sources considered have called for ethical considerations when applying and using artificial intelligence in criminal investigations mainly because artificial intelligence, as advanced as it may seem for certain tasks, still lacks certain human features like the sense for empathy, sympathy, sarcasm, and other ethical and philosophical criteria. Such criteria are very important in criminal investigations and must be always considered during interviews and interactions with the suspects (Faghiri, 2022).

This paper strongly believes that due to the lack of ethical abilities of artificial intelligence, the use of such should be limited to the technical abilities and to the analytical abilities of artificial intelligence. Interactions with humans should be highly technical and should be used to gather information, rather than evaluate whether the participant is guilty or not. Hence, artificial intelligence in criminal justice and criminal investigations should be a technical advantage over criminals, while the decision-making process should be left for human investigators to decide.

Regarding the ethical consideration for privacy, it should be noted that there is a certain threat to privacy should AI be used on a large-scale for surveillance and observation. Due to the ethical challenges to artificial intelligence (Kobis, 2022), or the lack thereof, human privacy could be threatened and with that combined basic human rights and human freedoms. This is also the case with the aim of predicting crimes. Entering basic datasets into a program using AI to evaluate who can be able to commit certain crimes is, although futuristic and theoretically possible, largely concerning, since not all crimes are committed equally and not all suspects can fit into a certain group of criminal offenders. In criminal justice theory and criminal investigations, there are always outliers and deviation in suspects, their backgrounds and behaviors, which is why it cannot be surely predicted who will commit certain crimes or who would be able to commit certain crimes in the future (Back, 2022). Additionally, entering such datasets into a neural network would pose the threat of, theoretically speaking, everyone becoming a suspect and everyone being able to become a subject of criminal investigation, which is the ethical challenge posed in science-fiction novels that

deal with artificial intelligence and prediction of the future (Mijwil, Aljanabi, & ChatGPT, 2023).

Conclusions

Artificial Intelligence in criminal investigations should be used as an aid because of its outstanding abilities to analyze many data sets and make certain conclusions faster than human investigators would. However, there are still some ethical challenges to be considered before artificial intelligence can become a large-scale tool for criminal predictions. Artificial intelligence still lacks certain human abilities and therefore there should be ethical frames put in place next to legal frames defining and regulating the use of artificial intelligence by countries using these methods in criminal investigations and criminal justice.

Some other ideas of AI in criminal investigation include the creation of online personas that would evaluate visitors to certain dark web groups and interact with suspects to collect information and investigate their possible location and their identity. Such chatbots are already in use, and the use of artificial intelligence would allow the chatbots to become independent until the full information and the full personal details are collected.

Crime predictions can be currently stated as the next step in the development of artificial intelligence. It is possible to connect the use of some analytical models and neural networks to be used for crime predictions. However, these models and use cases are ethically challenging and should only be used for research and training purposes.

Recommendations

After presenting the conclusions, the paper can provide the following recommendations:

- Developers and law enforcement officials should cooperate in creating models to create practical application tests for artificial intelligence in criminal investigations and crime predictions.
- There needs to be a unified international regulatory framework considering the application and use of artificial intelligence.
- There must be a base created for international cooperation considering information exchange of artificial intelligence used in malicious purposes and the development of artificial intelligence.
- There should be a global network of information exchange about the malicious use of artificial intelligence to combat it becoming a powerful tool in the hands of criminals.

References

Abate, D., Agapiou, A., Toumbas, K., Lampropolous, A., Petrides, K., Pierdicca, R., & Zingaretti, P. (2023). Artificial Intelligence to Fight Illicit Trafficking of Cultural Property. *Remote Sensing and Spatial Infromation Sciences 48*, 3-10.

Akhgar, B., Gercke, M., Vrochidis, S., & Gibson, H. (2021). *Dark Web Investigation.* Cham: Springer.

Al Qatawneh, I., Haswa, M., Jaffal, Z., & Barafi, J. (2023). Artificial Intelligence Crimes. *Adacemic Journal of Interdisciplinary Studies Vol. 12 No. 1*, 143-150.

Androschchuk, O., Balendr, A., Grinchenko, V., Farion, O., & Mostovyi, A. (2022). Methods of Extraction and Analysis of Intelligence to Combat Threats of Organized Crime at the Border. *Journal of Human, Earth, and Future Vol 3 No 3*, 345-371.

Back, S. (2022). *How Law Enforcement Utilizes AI to Deal with Crime.* Scranton: University of Scranton.

Baltruniene, B. (2022). Place of artificial intelligence in the detection and investigation of crime: the present state and future perspectives. *Problemy Wspolczesnej Kryminalistyki Vol 26*, 43-58.

Davis, S., & Arrigo, B. (2021). The Dark Web and anonymizing technologies: legal pitfalls, ethical prospects, and policy directions from radical criminology. *Crime, Law and Social Change, 76 no 4* , 367-386.

Faghiri, A. K. (2022). The Use of Artificial Intelligence In the Criminal Justice System. *Webology 19 (5)*, 19-40.

Ivliev, P., Ananyeva, E., Prys, I., & Burbina, Y. (2023). The use of IT Technologies in the prevention of Crimes. *BIO Web of Conferences vol. 65*, 08007-08009.

Kobis, N., Starke, C., & Rahwan, I. (2022). The promise and perils of using artifical intelligence to fight corruption. *Nature Machine Intelligence 4, no. 5*, 418-424.

Mijwil, M., Aljanabi, M., & ChatGPT. (2023). Towards Artificial Intelligence-Based Cybersecurity: The Practices and ChatGPT Generated Ways to Combat Cybercrime. *Iraqi Journal for Computer Science and Mathematics 4(1)*, 65-70.

Naseer, M., & Shaheen, G. (2023). Harnessing the Power of Artificial Intelligence: An In-Depth Review of its Effective Role in Countering Violent Extremism. *JURIHUM: Jurnal Inovasi dan Humaniora vol 4*, 569-580.

Zlate, N. (2022). Chatbots: Future Undercover Investigators in the Artificial Intelligence Era. *RAIS Social Science and Humanities vol 2*, 118-125.