

Predictive Policing and Enhancing Security Performance through Artificial Intelligence Applications

Yapay Zeka Uygulamaları Vasıtasıyla Öngörücü Kolluk ve Güvenlik Performansının İyileştirilmesi

Bensalem Kheira^{1,*}

¹ Prof. Dr., Bensalem Kheira, Lecturer A, Djilali Bounaama University, Faculty of Law, Khemis Miliana, Algeria, <https://ror.org/05n2gz355>, <https://orcid.org/0009-0004-5406-1260>, bensalemkheira44@gmail.com

Prof. Dr., Bensalem Kheira, Öğretim Üyesi A, Djilali Bounaama Üniversitesi, Hukuk Fakültesi, Khemis Miliana, Cezayir, <https://ror.org/05n2gz355>, <https://orcid.org/0009-0004-5406-1260>, bensalemkheira44@gmail.com

* Corresponding author

Araştırma Makalesi

Süreç

Geliş Tarihi: 06.04.2024

Kabul Tarihi: 06.11.2024

Yayın Tarihi: 30.12.2024

Benzerlik

Bu makale, en az iki hakem tarafından incelenmiş ve intihal yazılımı ile taranmıştır.

Değerlendirme

Ön İnceleme: İç hakem (editörler).

İçerik İnceleme: İki dış hakem/Çift taraflı körleme.

Telif Hakkı & Lisans

Yazarlar dergide yayınlanan çalışmalarının telif hakkına sahiptirler ve çalışmaları CC BY-NC 4.0 lisansı altında yayımlanmaktadır.

Etik Beyan

Bu çalışmanın hazırlanma sürecinde bilimsel ve etik ilkelere uyulduğu ve yararlanılan tüm çalışmaların kaynakçada belirtildiği beyan olunur. Bensalem Kheira

Etik Bildirim

turkisharr@gmail.com

Çıkar Çatışması

Çıkar çatışması beyan edilmemiştir.

Finansman

Bu araştırmayı desteklemek için dış fon kullanılmamıştır.

Yayıncı

Published by Mehmet ŞAHİN Since 2016-Akdeniz University, Faculty of Theology, Antalya, 07058 Türkiye.

Atıf

Kheira, B. (2024). Yapay zeka uygulamaları vasıtasıyla öngörücü kolluk ve güvenlik performansının iyileştirilmesi. *Turkish Academic Research Review*, 9/4, 444-454, <https://doi.org/10.30622/tarr.1464788>

Öz

Dijital dönüşüm çağı, küresel manzarada devrim yaratarak ülkeleri yapay zeka (AI) uygulamalarını etkin bir şekilde entegre etmek için altyapılarını modernize etmeye zorluyor. Bilim ve teknolojiye sürekli ilerlemelerle birlikte, toplumlar artık karmaşık olayları tahmin etmek ve ele almak için benzeri görülmemiş yeteneklere sahiptir. Bu makale, yapay zekanın afet yönetimi ve kolluk kuvvetlerindeki dönüştürücü potansiyelini araştırmakta ve zorlukların öngörülmesi ve azaltılmasındaki kritik rolünü vurgulamaktadır. Yapay zeka, kapsamlı veri analizi ve makine öğreniminden yararlanarak hem doğal afetlere hem de suçun küreselleşmesine karşı proaktif müdahalelere olanak sağlamaktadır. Afet yönetiminde, öngörücü yapay zeka modelleri, deprem gibi olayları tahmin etmek için sismik aktivite, jeolojik modeller ve çevresel değişkenler dahil olmak üzere kapsamlı veri kümelerini analiz eder. Bu modeller, yetkililerin erken uyarılarda bulunmasını, acil durum planları geliştirmesini ve olası can kayıplarını ve ekonomik kayıpları azaltmasını sağlar. Felaketleri önceden tahmin etme yeteneği, yapay zekanın toplumsal dayanıklılığı ve hazırlığı artırmadaki daha geniş faydasını yansıtmaktadır. Tahmine dayalı teknolojilerin entegrasyonu yalnızca acil zorlukları ele almakla kalmaz, aynı zamanda sürdürülebilir kalkınma için uzun vadeli stratejileri de güçlendirir. Buna paralel olarak, suçun küreselleşmesi, kolluk kuvvetleri için geleneksel metodolojileri aşan yenilikçi çözümler gerektiren benzersiz zorluklar ortaya koymaktadır. Kestirimci polislik, modern suçun karmaşıklığıyla mücadele etmek için yapay zeka odaklı analitiği kullanan ileriye dönük bir yaklaşım olarak ortaya çıkmıştır. Tahmine dayalı polislik sistemleri, geçmiş suç verilerini, davranış kalıplarını ve çevresel faktörleri inceleyerek potansiyel sıcak noktaları belirler, suç faaliyetlerini tahmin eder ve kaynakları daha stratejik bir şekilde tahsis eder. Bu metodoloji yalnızca operasyonel verimliliği artırmakla kalmaz, aynı zamanda suçları meydana gelmeden önce önleyerek adalet ilkeleriyle de uyum sağlar. Tahmine dayalı polislikte yapay zeka uygulaması örneği tanınmanın ötesine geçer. Gelişmiş algoritmalar, suç faaliyetlerinin dinamik doğasına uyum sağlayarak, gelişen eğilimleri ve suçlular tarafından kullanılan yenilikçi metodolojileri ele alır. Bu uyarlanabilirlik, suçun giderek daha sofistike ve ulus ötesi hale geldiği bir çağda kritik önem taşımaktadır. Ayrıca, öngörülü polislik, kolluk kuvvetleri ve halk arasında işbirliğini teşvik ederek daha güvenli topluluklar oluşturulmasına katkıda bulunur. Teknolojiyi sosyal katılımı bütünleştiren bu sistemler, etkili polisliğin temel bileşenleri olan güven ve işbirliğini güçlendirir. Bu çalışma, afet yönetimi ve kolluk kuvvetlerinde öngörücü YZ'nin ikili önemini vurgulamaktadır. Her iki alanda da YZ, reaktif stratejileri proaktif çerçevelere dönüştürerek riskleri en aza indirir ve toplumsal refahı artırır. Tahmine dayalı modellerin kullanımı, YZ'nin küresel zorlukları bütünsel olarak ele alma potansiyelini örneklendirmekte ve yenilik, güvenlik ve esneklik ile karakterize edilen bir gelecek sağlamaktadır. YZ'nin entegrasyonu etik ve operasyonel hususlar sunarken, doğal afetlerin azaltılması ve suçla mücadeledeki faydaları potansiyel dezavantajlarından çok daha ağır basmaktadır. Sonuç olarak, YZ'nin kritik sistemlere entegrasyonu, çağdaş zorlukların ele alınmasında değerli bir ilerlemeyi temsil etmektedir. Doğal afetlerin öngörülmesinden suç faaliyetlerinin önlenmesine kadar, YZ uygulamaları toplumsal tepkileri yeniden şekillendiren yenilikçi çözümler sunmaktadır. Bu makale, giderek daha fazla birbirine bağlanan bir dünyada hazırlıklı olmayı, dayanıklılığı ve güvenliği teşvik etmek için öngörücü teknolojilerden yararlanmanın önemini vurgulamaktadır. Ülkeler, altyapılarını modernize ederek ve yapay zeka odaklı stratejileri benimseyerek dijital çağın karmaşıklıklarını etkili bir şekilde yönetebilir, sürdürülebilir ilerleme ve küresel istikrarın önünü açabilir.

Anahtar Kelimeler: Yapay zeka, öngörücü polislik, sorgulama, dijital dönüşüm, teknolojik ilerleme.

Research Article

History

Received: 06.04.2024

Accepted: 06.11.2024

Date Published: 30.12.2024

Plagiarism Checks

This article has been reviewed by at least two referees and scanned via a plagiarism software.

Peer-Review

Single anonymized-One internal (Editorial Board), Double anonymized-Two external.

Copyright & License

Authors publishing with the journal retain the copyright to their work licensed under the **CC BY-NC 4.0**.

Ethical Statement

It is declared that scientific and ethical principles have been followed while carrying out and writing this study and that all the sources used have been properly cited. Bensalem Kheira

Complaints

turkisharr@gmail.com

Conflicts of Interest

The author(s) has no conflict of interest to declare.

Grant Support

The author(s) acknowledge that they received no external funding in support of this research.

Published

Published by Mehmet ŞAHİN Since 2016-Akdeniz University, Faculty of Theology, Antalya, 07058 Türkiye

Cite as

Kheira, B. (2024). Predictive policing and enhancing security performance through artificial intelligence applications. *Turkish Academic Research Review*, 9/4, 444-454, <https://doi.org/10.30622/tarr.1464788>

Abstract

The digital transformation era has revolutionized the global landscape, urging countries to modernize their infrastructures to integrate artificial intelligence (AI) applications effectively. With continuous advancements in science and technology, societies now possess unprecedented capabilities to predict and address complex phenomena. This paper explores the transformative potential of AI in disaster management and law enforcement, emphasizing its critical role in anticipating and mitigating challenges. By leveraging comprehensive data analysis and machine learning, AI enables proactive responses to both natural disasters and the globalization of crime. In disaster management, predictive AI models analyze extensive datasets, including seismic activity, geological patterns, and environmental variables, to forecast events such as earthquakes. These models empower authorities to issue early warnings, develop contingency plans, and reduce potential casualties and economic losses. The ability to anticipate disasters reflects the broader utility of AI in enhancing societal resilience and preparedness. The integration of predictive technologies not only addresses immediate challenges but also strengthens long-term strategies for sustainable development. In parallel, the globalization of crime presents unique challenges for law enforcement, requiring innovative solutions that transcend traditional methodologies. Predictive policing has emerged as a forward-looking approach that harnesses AI-driven analytics to combat the complexities of modern crime. By examining historical crime data, behavioral patterns, and environmental factors, predictive policing systems identify potential hotspots, forecast criminal activities, and allocate resources more strategically. This methodology not only enhances operational efficiency but also aligns with the principles of justice by preventing crimes before they occur. The application of AI in predictive policing extends beyond pattern recognition. Advanced algorithms adapt to the dynamic nature of criminal activities, addressing evolving trends and innovative methodologies employed by offenders. This adaptability is critical in an era where crime has become increasingly sophisticated and transnational. Furthermore, predictive policing contributes to building safer communities by fostering collaboration between law enforcement agencies and the public. By integrating technology with social engagement, these systems strengthen trust and cooperation, essential components of effective policing. This study accentuates the dual significance of predictive AI in disaster management and law enforcement. In both domains, AI transforms reactive strategies into proactive frameworks, minimizing risks and enhancing societal well-being. The use of predictive models exemplifies the potential of AI to address global challenges holistically, ensuring a future characterized by innovation, safety, and resilience. While the integration of AI presents ethical and operational considerations, its benefits in mitigating natural disasters and combating crime far outweigh potential drawbacks. In conclusion, the integration of AI into critical systems represents a valuable advancement in addressing contemporary challenges. From forecasting natural disasters to preventing criminal activities, AI applications provide innovative solutions that reshape societal responses. This paper stress the importance of leveraging predictive technologies to foster preparedness, resilience, and security in an increasingly interconnected world. By modernizing infrastructures and embracing AI-driven strategies, nations can navigate the complexities of the digital era effectively, paving the way for sustainable progress and global stability.

Keywords: Artificial intelligence, predictive policing, querying, digital transformation, technological progress.

Introduction:

With the emergence of digital environments in the modern era and the adoption of smart city strategies by nations utilizing cutting-edge technologies in the age of artificial intelligence, there has been a notable shift in criminal policy towards employing modern scientific methods for crime detection, while respecting civil liberties and legal safeguards. Artificial intelligence techniques, such as surveillance cameras that identify individuals and their locations and predictive policing, which utilizes statistical analysis to anticipate and prevent crimes, have become integral tools in law enforcement (Al-Sha'ar, 2020). Predictive policing aims to detect and prevent crimes early, utilizing scientific evidence to establish criminal responsibility, while upholding constitutional rights to protection of personal data.

Artificial intelligence in the realm of crime serves as a double-edged sword. On one hand, it has facilitated the globalization of crime through some of its applications, such as programs that learn user behaviors to mimic them, leading to the exchange of ideas and discussions that may result in terrorist activities with crime-affiliated extremists. Chatbot programs powered by artificial intelligence can recruit children and teenagers from within their homes to carry out terrorist attacks and become involved in organized crime.

Moreover, criminal activities have increased with this new pattern, where artificial intelligence technologies are exploited to alter and manipulate images or video clips, depicting individuals engaging in criminal acts, thereby making them susceptible to blackmail, particularly in pornographic activities that tarnish individuals' reputations, coercing them to comply voluntarily with these criminals.

Hence, artificial intelligence applications are capable of increasing fraud and crime rates. However, this can be countered by deploying artificial intelligence applications as well, as one researcher stated, "Artificial intelligence only defies artificial intelligence." Through effective tools utilized by judicial authorities and security agencies in combating crime, such as the creation of strategic predictive analytics relying on historical crime data to identify its types, locations, and severity, authorities can predict and prevent crimes in specific areas. This proactive approach aids security agencies in preparing and mobilizing human and material resources and deploying patrols in hotspots where criminal activities are likely to occur. Additionally, surveillance systems equipped with advanced technologies and utilizing sophisticated computer algorithms for analysis and identification of suspicious activities enable preemptive crime detection and prevention.

The goal of artificial intelligence in the criminal field serves two important roles: preventive and deterrent. The first is preventive through forecasting and future insights to reduce crime using modern technologies that analyze predictive data, identify crime hotspots, and preemptively recognize criminals based on their behaviors and lifestyles. This is achieved by understanding the nature of human intelligence through the development of AI programs capable of simulating human behavior characterized by intelligence, thereby combating crime and predicting it before it occurs.

The second goal is deterrent, occurring after the crime has been committed, through the use of artificial intelligence to search for criminal evidence that proves the act and assigns responsibility to the perpetrator, providing irrefutable evidence for attribution.

The importance of research in the legal framework of predictive policing, with the necessity of accessing data and the legitimacy of the means used therein, can be considered both as precautionary measures at times and as investigative procedures at other times. The extent to which judges rely on these algorithms in determining criminal liability and imposing penalties lies within the realm of probability. Hence, it is crucial to delineate the legal framework that should regulate the applications of artificial intelligence in this domain.

The problem that can be raised in this context is: **within the framework of respecting criminal legitimacy and personal data for each individual, what is the legitimacy of activating predictive policing procedures using artificial intelligence applications to prevent future crimes?**

To answer this question, we divided our research into two main axes:

** The first axis addresses the legitimacy of predictive policing in risk management.

** The second axis deals with predictive policing techniques and their legitimacy.

We relied on an analytical approach to describe crimes and analyze artificial intelligence technologies to assess their legitimacy and the legality of the evidence derived from them.

First Axis: Legitimacy of Predictive Policing in Risk Management

In the context of globalization, new global changes, as well as economic, social, political, cultural shifts, and internal and external security threats, risk management has become a new and essential challenge for every state to confront and mitigate crimes preemptively. Predicting crime before it occurs involves studying the patterns of criminal behavior based on algorithms that form the backbone of artificial intelligence, as was the case with jurisprudential theories that have long observed criminals, sometimes analyzing them psychologically, sometimes socially, and sometimes biologically (Al-Sari, n.d.)'. Law enforcement agencies can better anticipate criminal developments through predictive policing.

Predictive policing is built on experimental maps continuously updated to include the types of crimes prevalent in neighborhoods, the network of active criminals, and the institutions most susceptible to robbery and theft. This data is fed into algorithmic engines to predict where the next crime will occur.

Risk management in policing is an established science in itself, where algorithms capable of self-learning through artificial intelligence are fed with citizens' data in a city, their criminal records, as well as the dates, locations, and nature of each crime that occurred in the area. Here, algorithms provide results about crime-prone categories and the closest locations to their occurrence.

It is also an art in terms of searching for the best methods to achieve the best results with the aim of controlling and containing risks and restoring balance to society in the shortest time and with minimal effort and losses.

First: The Concept of Crime Prediction:

If anticipation or prediction is a specific recognition of potential danger, crisis management's fundamental principle is the ability to predict crises, thereby alleviating their severity upon occurrence and enhancing their containment capabilities. This relies on thought, deduction, data reliance, analysis, prediction, and exploration, leveraging artificial intelligence applications resulting from the interaction between communications, mathematical, spatial, virtual, and real-world realms in crime prediction (Al-Eissawi, 2020, p. 89).

Prediction or forecasting is not only a sense of current or future danger that can alert to the source of danger or the person responsible. This is what is referred to as the science of security foresight. This is accomplished through establishing sound information systems in each institution of the state, civil society, and local authorities.

Prediction is defined as planning and making assumptions about future events using specialized techniques over different time periods. It is also defined as the art and science of predicting future events. It is an art because experience and personal judgment play a role in prediction and in selecting the appropriate method of prediction. It is a science because it uses objective mathematical and statistical methods and approaches to increase accuracy and reduce bias (Amer, 2017, p. 82).

This applies generally to prediction. However, if we employ this information in criminology, crime prediction is akin to precautionary measures, which are the clearest example of traditional methods of crime prevention before it occurs, such as commitment to mental health facilities, therapeutic institutions, and social care institutions. Most criminal legislations have sought to establish legal frameworks to mitigate future crime, such as parole systems and suspension of punishment for the purpose of not committing a new crime.

However, in the era of globalization, technology has played a significant role in detecting anticipated crimes by adopting artificial intelligence applications, through which crimes expected to occur in the future can be detected with sufficient lead time to apprehend suspects.

Second: The Legal Nature of Crime Prediction:

Modern jurisprudence has differed in establishing the legal nature of predictive policing, considering that this technique relies on artificial intelligence. Given the novelty of this subject, which relies on data, algorithms, equations, and conclusions, it was necessary to examine the most important similar systems to attribute and establish it. Several previous studies, notably the research conducted by Dr. Mahmoud Salama Abdel Moneim Sharif, concluded that the legal nature of crime inquiry is inherently different from other procedural systems.

1. Precautionary Measures System:

Jurists in the field of criminal law have sought alternatives to punishment aimed at rehabilitating the offender. The positivist school prioritized concern for the criminal and how to reform, treat, and reintegrate them into society. Thus, a set of precautionary measures was enacted to prevent future crimes.

Returning to the Precautionary Measures System, it represents a set of measures that confront crime and criminals by taking actions to prevent the recurrence of crime and protect society from the danger posed by the offender. It bears resemblance to predictive policing, which aims to prevent future crimes. Both systems share the concept of criminal risk probability and the likelihood of future crime recurrence. In the precautionary system, the criminal, with his criminal record, determines the step of the criminality and the likelihood of recidivism. Similarly, in predictive policing, algorithms and personal data analysis determine the individual's risk level.

The precautionary system may also resemble predictive policing in their unified goal of preventing future crimes and their execution without the need for the victim's consent. Both systems impose measures without the individual's consent for the sake of prevention. However, it should be noted

that predictive policing, which seeks information without prior consent, operates under legal legitimacy and respects constitutional and personal data protection laws.

Despite the significant similarities between the two systems, predictive policing cannot be attributed to the precautionary system due to several considerations:

** It is widely accepted that the precautionary system is post-crime, whereas crime inquiry is pre-crime. Despite shared goals, they differ temporally, altering their legal nature.

** The precautionary system adheres to the legality principle, where no crime, punishment, or security measure is valid without legal basis. In contrast, the legal framework and regulation of predictive policing, particularly concerning individual freedom and personal information protected by law, are less defined. When can it be said that inquiry does not violate criminal legality principles?

** In terms of jurisdiction, the judiciary is authorized to issue precautionary measures against convicted individuals, while accessing the realm of artificial intelligence and searching for crime hotspots and criminal hubs falls under administrative entities like the police or gendarmerie equipped with intelligence offices.

Considering all these considerations, we find that the nature of precautionary measures differs from crime inquiry through data and analysis. The former is punitive, while the latter is procedural. Although both are aimed at combating crime, they undoubtedly differ in their legal nature.

2. System of Investigation and Inquiry:

As commonly understood, investigation aims to gather evidence to establish suspicion against individuals who may be accused before the judiciary, based on the totality of inquiries and information available to them. Among these pieces of evidence, algorithmic prediction methods may be employed, which are among the tools relied upon by judicial police in investigating crimes and criminals.

In criminal law, investigation involves the use of all lawful methods specified in criminal procedure laws, governed by legal principles aimed at pursuing criminals, apprehending them, and referring them to the judiciary with compelling evidence. However, these tools used do not rise to the level of conclusive scientific evidence. Every judicial record provides them with relative legal validity and evidential value, subject to the discretion of the criminal judge.

However, with the digital transformation and reliance on the police inquiry system, or what is known as predictive policing, artificial intelligence applications can intervene in research and investigative methods to early detect crimes, accurately diagnose crime hotspots, identify suspects, and refer them to justice based on this new evidence.

As in cases of neighbourhood gangs, predictive policing leads to identifying individuals who may be involved in rioting crimes due to algorithms confirming their frequent presence and activities in the neighbourhoods, based on their personal data, especially in such types of cases.

It is acknowledged that notification tools at the level of police stations, especially in traffic accidents, which monitor the speed of drivers in specific locations, can immediately alert other police officers on the road to stop these individuals, thus avoiding subsequent accidents.

However, the issue that arises in this context is the legality of the means used. Determining the legal nature of predictive policing must adhere to the principle of legal legitimacy and the legitimacy of the

algorithms used in data analysis through artificial intelligence applications. These applications analyze actions and positions in the present, past, or future through speeches, symbols, images, or specific actions that occurred in the past or present, or are expected to occur in the future. Undoubtedly, the use of data storage today has become more extensive and easier, leading the Algerian state to enact internal legislation and approve agreements to ensure the protection of data from risks, transgressions, and violations, the most important of which is Data Protection Law 18-07 dated July 10, 2018, Official Gazette No. 34.

Moreover, the adoption of artificial intelligence applications in collecting and accessing this data and analyzing the algorithms of suspected individuals necessitated states to enact legislation to ensure human privacy and individual freedom. This was further reinforced by the 2020 Constitution in Article 47, which stipulates "the protection of individuals in processing personal data as a fundamental right."

However, providing a legal description of the nature of predictive policing as being investigative may encounter some criticisms, as articulated by modern legal scholars:

**** Investigation always occurs after the commission of the crime, which is rooted in legal provisions distributed by the legislator in criminal procedural law, in respect of criminal legal legitimacy. Actions such as apprehension, search, hearing, and detention are all investigative procedures of a purely legal nature that cannot be carried out without a legal provision authorizing them.**

However, predictive policing is exceedingly preemptive to the investigation stage and contradicts the principle of criminal legal legitimacy, especially concerning the querying of personal data, as the constitutional principle asserts the presumption of innocence.

In cases where individuals are detained based on predictive policing and heard, there must be unequivocal evidence and data, leaving no room for error before the individual is removed from the category of suspects. Additionally, the bias observed in some countries' use of this data to detain a specific category, especially those with dark skin, diverges from the intended goal.

Considering the two previous systems, we find that the investigatory system is closer to the precautionary system. However, both are subsequent to the commission of the crime, while predictive policing constitutes actions preceding the crime, merely consisting of inquiries about potential occurrences and predictions of crimes, making its legal framework closer to **administrative and regulatory nature**.

3. The Administrative Nature of Crime Prediction:

The administrative nature of crime prediction becomes apparent when considering two elements:

Firstly, referring to the authority responsible for data inquiry and analysis, there exists a specialized agency empowered by a legal framework that protects its actions. One such example is the intelligence agency operating at the level of police directorates, which has effectively shifted the paradigm from merely investigating crimes to preemptively eradicating them. This proactive approach aims to create a safer and more secure future.

On the other hand, the administrative nature of predictive policing is evident in the tools used, which transcend the judicial realm or any other jurisdiction through the utilization of artificial intelligence technologies. For instance, facial recognition technology supported by artificial intelligence aids in identifying the whereabouts of wanted individuals, leading to their apprehension before they become aware of being under surveillance. Artificial intelligence systems have also succeeded in developing preemptive

strategies and effective measures to combat various criminal networks, such as monitoring communication channels, decrypting encrypted messages, and identifying voices and biometric data to apprehend criminals involved in illegal activities.

Furthermore, inspection procedures conducted through scanning devices to prevent the flow of contraband across borders and apprehend smugglers fall within the framework of maintaining public order and security. Thus, the functional criterion defines the administrative nature of using artificial intelligence algorithms in crime prediction.

The Second Axis: Techniques of Predictive Policing and Their Legitimacy:

The introduction of artificial intelligence into the realm of data analysis is one of the most discussed topics globally and scientifically, particularly in various fields such as industry, commerce, medicine, environment, and notably, security. However, in the legal domain, the authorization to use these applications must be legally regulated to uphold the principle of legal legitimacy.

Access to artificial intelligence applications must be accompanied by legal security to protect users from violating the constitutional principle that safeguards individual freedom and data from intrusion.

However, the question that arises in this context concerns the validity of these technologies when facing suspects who have not yet committed a crime and cannot be prosecuted for actions they might have been inclined to commit or may change their intentions.

Firstly, an Overview of Predictive Policing Techniques:

Various technological methods are employed by law enforcement agencies in the era of artificial intelligence for crime prediction, akin to forecasting earthquakes, weather forecasts, and epidemic predictions, all relying on a systematic approach serving all platforms equipped with such intelligent applications. However, beyond the realm of technology and the necessity of globalization across all fields, discussing these techniques and their legality from a legal perspective and their respect for the constitution and personal freedoms is imperative (El-Masri, 2023).

01. Utilizing Artificial Intelligence Algorithms:

The sequence of steps or studies following a sequential method, relying on previous data in a precise sequence, as introduced by the Persian mathematician Muhammad ibn Musa al-Khwarizmi for analyzing and predicting a specific phenomenon. Artificial intelligence algorithms used by applications in law enforcement agencies for crime prediction and identification of criminals follow pre-established steps and previous statistics. These algorithms are integrated into programs where crime rates in specific areas and the number of criminals are analyzed over a specific period of time, providing undeniable results in discovering new crimes (Al-Eissawi, 2020).

02. Feeding Artificial Intelligence with Pre-existing Data:

Feeding artificial intelligence applications with massive amounts of data and inputting new information, similar to the growth of the human mind and its nourishment with qualitative information that increases human awareness and shapes thinking and inference. This facilitates law enforcement agencies in providing clear and accurate results, with high accuracy rates. These data have reliable sources, including administrative programs such as hospitals that determine the proportions of victims of assault and battery crimes, as well as prison management, which determines crime rates and the number of detainees for each

crime and their areas of commission. Similarly, data obtained from courts, the number and types of criminal cases, vary from one area to another, such as cases of substance abuse, as well as data acquired from sensor devices such as radar and location tracking devices, for example, for traffic violations.

Additionally, another type of source is pertinent for cybercrimes, as the entry and exit of individuals from websites through searching for specific items confirm the inclinations of suspects to commit a certain crime (Khan, 2019, pp. 100–112).

Criminal behavior and its danger rely on the analysis conducted by artificial intelligence on the data, as is the case in studying the behavior of criminals who frequent suspicious websites and pages or target victims from specific groups, such as those seeking legal migration or engaging in prostitution.

Based on the foregoing, it can be said that the fuel for algorithms is accurate data, which we input into artificial intelligence applications to obtain accurate results and predict crimes with very high accuracy. Predicting a robbery in a specific area by a suspected individual is based on algorithms fed with data about their daily activities at different times, as well as through investigations and their personal and social data, and their activities on social media (Lababili, 2020).

03. Self-learning of Artificial Intelligence:

Self-learning of artificial intelligence is considered the future of AI, through machine learning from included data, continuous data, and previous experiences. The vast amount of information enhances self-learning and makes crime prediction a tangible reality through criminal statistics to monitor criminal movements, track them, and apprehend them before committing crimes. For instance, financial crimes were mainly attributed to white-collar individuals who extensively used electronic payment cards to defraud their clients. Artificial intelligence technologies detected most of the categories searching for fraud and deceit, hindering their activities before executing any crime (Omar, 2022, pp. 55–70).

Secondly, the Protection of Data from Artificial Intelligence Mediums:

Personal data fuels artificial intelligence algorithms, as after collecting, processing, examining, compiling, recording, storing, merging, transmitting, receiving, circulating, publishing, changing, modifying, retrieving, and analyzing the data using any electronic means, we have a platform capable of predicting any desired information. Algeria, like all countries, has given great priority to protecting individuals in their private lives and safeguarding them from technologies that process and trade their data. Hence, Law 18-07 was issued to address several issues regarding the protection of individuals.

Through this law, the correct framework for entering personal information and the possibility of legally researching, investigating, and monitoring while respecting humanitarian principles, dignity, and the sanctity of private life was established. Predictive policing is regulated by Law 18-07, which also established a national authority to protect data with financial and administrative independence. This authority has various tasks aimed at protecting data (Amer, 2017, p. 82).

However, the predictive policing entity and its early crime inquiry cannot fully comply with this law, as it has exceptions allowing it to access and process data without prior authorization. Still, it must adhere to certain obligations (Sharif, n.d.):

1. Confidentiality of Processing and Inquiry:

The predictive policing entity must take all measures to ensure the complete security of the data from leakage or disclosure to unauthorized parties and maintain professional secrecy according to the rules of public law and special laws even after the completion of its tasks.

2. Integrity of Processing:

Exposing data to any unauthorized use, hacking, damage, or any other use outside the intended purpose exposes the owner to accountability. Therefore, the use of crime detection algorithms may fail if others are allowed access to their information network.

Hence, it can be said that the predictive policing process, which is at the core of state security, stability, and the preservation of public order, through the use of artificial intelligence technologies, is legally regulated to protect others' information from hacking and never conflicts with the principle of legitimacy (Al-Sari, n.d.).

Conclusion:

In conclusion, the integration of artificial intelligence in proactive crime prevention is an inevitable necessity. Transitioning from crime suppression to its prevention is imperative in the face of global criminality. Law enforcement must confront it with methods that mirror the evolutionary intelligence of devices, ensuring a future of security devoid of crime. However, accessing crime prediction through algorithms, analyses, and data mining must be framed within a legal framework. This framework should serve as the basis for criminal prosecution, ushering in a new era of anticipating and apprehending suspects without infringing upon their personal liberties or compromising the presumption of innocence. Today's law faces a new challenge of crime anticipation and suspect apprehension, ensuring the validity of the means used, from circumstantial evidence to conclusive evidence that assigns responsibility to its owners. Among the key findings of this research are:

*** Framing the predictive policing process within a legal system that defines its principles and exceptions.

*** Working towards legal intelligence that mirrors artificial intelligence and the globalization of crime through innovative investigative methods.

References :

- Al-Eissawi, Ibrahim. "Future Studies." Egypt Project, 2020, p. 89.
- Al-Hammadi, Saif. "Predictive Policing: Challenges and Opportunities in Crime Prevention." *Journal of Law and Security Studies*, 2021, vol. 5, no. 3, pp. 215-230.
- Al-Sari, Rashid Mohammed Ahmed. "Security Prediction and Its Role in Crime Prevention: An Analytical Study." Saad Abdullah Academy for Security Sciences Journal, 2nd Edition.
- Amer, Qasim Ahmed. "Prospecting and Security Prediction in Sharjah." *Police Research Center*, 1st Edition, 2017, p. 82.
- Electronic Reference: Qasim Ahmed Amer, "Prospecting and Security Prediction in Sharjah," *Police Research Center*, 1st Edition, 2017, p. 82.
- El-Masri, Omar. "Artificial Intelligence and Crime Trends: A Global Perspective." *Security Journal*, 2023, vol. 36, no. 4, pp. 578-593.

- Ibrahim Al-Eissawi, "Future Studies," *Egypt Project*, 2020, p. 89.
- Khan, Adnan. "Digital Forensics and AI: New Frontiers in Cyber Crime Prevention." *Journal of Digital Crime and Forensics*, 2019, vol. 3, no. 2, pp. 100-112.
- Lababili, Amar Yasser Mohammed Zuhair. "The Role of Artificial Intelligence Systems in Crime Prediction," *Police Thought*, 2020, available at: <https://doi.org/10.12816/0053352>
- Mahmoud Salama Abdel Moneim Sharif, "The Legal Nature of Crime Prediction Using Artificial Intelligence and Its Legitimacy," *Arab Journal of Forensic Sciences and Forensic Medicine*, available online at: <https://journals.nauss.edu.sa/index.php/AJFSFM/article/view...> Naif Arab University for Security Sciences (NAUSS).
- Omar, Hana. "Artificial Intelligence in Law Enforcement: Enhancing Predictive Analysis for Crime Reduction." *International Journal of Criminal Justice Sciences*, 2022, vol. 17, no. 1, pp. 55-70.
- Rashid Mohammed Ahmed Al-Sari, "Security Prediction and Its Role in Crime Prevention: An Analytical Study," *Saad Abdullah Academy for Security Sciences Journal*, Kuwait, 2nd Edition.
- Saud Abdul Qadir Al-Sha'ar, "The Role of Artificial Intelligence in Cyber Crimes: A Comparative Study," *Ajman University College of Law*, 2020.