فصلنامه علمی
رویکردهای نو در مدیریت دولتی
The scientific quarterly of
New Approaches in Public Administration
JNAPA

# Emerging Technologies and Proactive Protection of Law Enforcement Personnel[1]

Mohammad Musa Khorshidi
Research Assistant Professor, Faraja Center for Strategic Studies (Corresponding Author)
ORCID: 0009-0007-9274-6457
m.khorshidi59@gmail.com

Hadi Ansari
Master of Laws, Applied Research Office, Border Guard Command, Bushehr Province
ORCID: 0009-0001-1588-4035
hadiansari13606@gmail.com

**Received: 2025/03/09| Revised: 2025/07/20| Accepted: 2025/07/26**

## Abstract

Pre-event protection of law enforcement personnel is of particular importance as a preventive approach to ensuring the health and safety of human resources in the security and law enforcement fields. This review article, with the aim of examining the role of new technologies in promoting security and preventing crime in law enforcement forces, has conducted an extensive review of research conducted in this field. Among the key findings of this research, the following can be mentioned: Machine learning algorithms and artificial neural networks are able to identify and predict criminal behavior patterns by analyzing a huge amount of data. This allows law enforcement forces to take preventive action and prevent crime from occurring. By connecting different devices to each other, the Internet of Things allows the collection of a large amount of data that can be used to monitor the environment and identify potential threats. By creating a distributed, immutable ledger, blockchain can help improve transparency, security, and traceability in criminal cases. In addition to the benefits mentioned, this research also addresses the challenges in implementing these technologies. These include privacy concerns, algorithmic bias, and more. Overall, this research shows that new technologies can be used as a powerful tool for crime prevention and proactive protection.

**Keywords:** Emerging technologies, artificial intelligence, blockchain, proactive protection, surveillance

[1] https://sanad.iau.ir/Journal/napa/Article/1201546

فصلنامه علمی
رویکردهای نو در مدیریت دولتی
The scientific quarterly of
New Approaches in Public Administration
JNAPA

# Extended Abstract

## Emerging Technologies and Proactive Protection of Law Enforcement Personnel

### Introduction

In today's world, where scientific and technological advancements are rapidly transforming lifestyles and social interactions, law enforcement agencies face new challenges and opportunities in maintaining public order and security. On one hand, offenders are leveraging advanced technologies to develop more sophisticated methods of committing crimes. On the other hand, strengthening the proactive protection of law enforcement personnel has become a strategic necessity to prevent crimes and mitigate both internal and external threats (Matlala Ramolobi L.G., 2018).

To prevent potential violations, various methods and techniques based on scientific and logical principles should be employed, ensuring that individuals rationally engage with them, become aware of the consequences of their actions, and understand the potential repercussions. For example, measures such as increasing the difficulty and risks for offenders, intensifying penalties, or implementing preventive strategies can help deter financial crimes within law enforcement agencies (Hassanvand et al., 2021).

Given the complexity of modern crimes, the use of innovative technologies in proactive protection—such as unmanned aerial vehicles, artificial intelligence, analytical information systems, and chatbots—can significantly enhance law enforcement effectiveness and improve responses to security challenges (Tulinov et al., 2022). However, the introduction of these technologies faces obstacles such as budget constraints, legal deficiencies, and methodological limitations, hindering their widespread and effective adoption (Hendrix et al., 2019; Mastrobuoni, 2020).

This review article explores the significance of utilizing modern technologies for the proactive protection of law enforcement personnel, analyzes the challenges associated with their implementation, and proposes practical solutions. The primary objective of this study is to present a framework for the effective use of innovative technologies in crime prevention and the protection of law enforcement personnel against various threats.

### Theoretical Framework

Emerging technologies are technologies whose development or applications have not been fully realized. These technologies are usually new, but they also include older technologies that find new applications. Emerging technologies are often capable of changing the status quo ("Emerging Technologies," 2024). The most prominent impact of these technologies lies in the future and is therefore still somewhat uncertain and ambiguous in the introduction phase (Rotolo et al., 2015). Emerging technologies are dramatically transforming law enforcement practices, increasing efficiency, transparency, and operational capabilities. The integration of artificial intelligence (AI), blockchain, and advanced information systems is reshaping the way law enforcement agencies operate, leading to improved crime prevention and investigation processes.

Pre-event protection is a set of measures and measures that are taken to prevent violations and crimes from occurring among employees of an organization. These measures can include training, awareness-raising, strengthening religious and belief beliefs, and improving the livelihood and psychological conditions of employees.

Strong surveillance systems reduce the occurrence of crime by increasing the likelihood of detection and punishment (Eck and Clarke, 2019, p. 1). Situational crime prevention (SCP) theory focuses on environmental factors affecting the occurrence of crime and attempts to prevent crime by reducing criminal opportunities rather than focusing on the individual characteristics of criminals. This approach has a significant impact on the prevention of economic crimes, especially emerging threats

such as online fraud and cybercrime. The following sections examine key aspects of SCP and its relevance to the prevention of economic crimes.

SCP categorizes criminal opportunities using the "effort, risk, reward, provocation, excuses" framework, which helps identify and mitigate the conditions conducive to crime (Stones and Tilley, 2022). Techniques such as target hardening, surveillance, and access control have been effectively applied to a variety of crimes, including economic crimes such as fraud (Eck and Clarke, 2019, p. 1). International implementation of SCP, particularly in Latin American regions, has shown positive results in crime reduction and has demonstrated the adaptability of the approach to different contexts (Benito and Tejera, 2020). Rapid technological advancements pose challenges for SCP and increase the need for continuous adaptation to address new forms of economic crime (Johnson, 2024).

## Methodology

This systematic review used a comprehensive search strategy to identify relevant studies published in reputable databases such as Google Scholar, Science Direct, Elmnet, IranDoc, Normags, and Civilica. Search terms focused on technology, law enforcement, and crime prevention. In total, 66 articles were included in the analysis. Data extraction was performed to identify key themes such as types of technologies used, applications, and challenges encountered.

## Discussion and Results

The integration of modern technologies, particularly artificial intelligence (AI), into surveillance and law enforcement systems has revolutionized crime prevention. AI enhances traditional methods by introducing new approaches such as crime prediction, real-time monitoring, and advanced criminal analytics, helping law enforcement agencies track criminal activities more effectively and respond swiftly (Fatih & Bekir, 2015). Tools like facial recognition, voice analysis, and social media monitoring improve threat assessment and optimize resource allocation, allowing police forces to be more effective in high-risk areas and prevent crimes before they occur (Kobets, 2024).

However, AI also raises ethical and legal concerns. Issues such as privacy violations, potential biases in data, and the risk of misuse necessitate appropriate legal frameworks to manage this technology responsibly (Lunhol & Torhalo, 2024). In combating cybercrime, AI plays a crucial role in tracking threats and analyzing digital data. By processing vast datasets, AI can detect unusual behaviors and enable security teams to take preventive measures (Fomin & Luk'janova, 2023). Additionally, predictive policing models help law enforcement identify crime patterns and allocate resources more efficiently (Kahla, 2024).

Overall, AI is a key player in improving police efficiency and crime prevention. However, to ensure its effective and responsible use, regulatory and ethical policies must be developed to maximize security benefits while mitigating potential risks (Sukhodolov & Bychkova, 2018).

The Internet of Things (IoT) refers to interconnected devices equipped with sensors, processors, and communication technologies that facilitate data exchange through networks (Dey et al., 2017). Integrating IoT and Artificial Intelligence (AI) has revolutionized crime prevention and law enforcement by enhancing surveillance, cybersecurity, and data analysis. These technologies enable proactive security measures through early threat detection and behavioral pattern recognition.

IoT-based biometric tracking improves offender supervision, reducing the need for constant physical presence. For instance, IoT devices continuously monitor an individual's location and movement, ensuring compliance with legal restrictions, which enhances public safety and reduces police resource burdens (Dlodlo et al., 2015). Additionally, IoT sensors in workplaces detect potential threats and monitor employee activities in real time, preventing offenses and workplace violations (Alinejad, 2024).

AI-powered IoT systems analyze vast datasets using complex algorithms, offering real-time monitoring and predictive analytics. For example, AI algorithms process IoT sensor data to identify suspicious behavior, supporting preventive policing (Kahla, 2024; Saini et al., 2023; Singh & Ramdeo, 2023). Furthermore, big data and IoT integration address limitations of traditional Crime Prevention Through Environmental Design (CPTED). These smart systems automatically alert individuals in high-risk areas, preventing crimes before they occur (Jeon & Jeong, 2016).

In summary, AI and IoT enhance surveillance efficiency and law enforcement effectiveness by providing continuous data collection and analysis. These technologies enable proactive policing strategies, increasing public trust and safety measures.

## Conclusion

The integration of modern technologies into law enforcement offers significant potential for improving public security and enhancing the efficiency of police operations. Technologies such as artificial intelligence, body-worn cameras, the Internet of Things, and blockchain can bring about transformative changes in surveillance, data analysis, and crime prediction. However, the adoption of these technologies must take into account ethical implications, privacy concerns, and potential biases. To ensure their responsible and effective use, it is essential to establish clear legal frameworks and develop robust governance mechanisms.

## Contribution of authors

All authors have participated in this research in equal proportion.

## Ethical approval

Choose an item.

## Conflict of interest

No conflicts of interest are declared by the authors

پژوهشگاه علوم انسانی و مطالعات فرهنگی
پرتال جامع علوم انسانی

فصلنامه علمی
رویکردهای نو در مدیریت دولتی
The scientific quarterly of
New Approaches in Public Administration
JNAPA

# فناوری‌های نوین و صیانت پیش‌کنشی کارکنان محیط انتظامی

**تاریخ دریافت: ۱۴۰۳/۱۲/۱۹ تاریخ ویرایش: ۱۴۰۴/۰۴/۲۹ تاریخ پذیرش: ۱۴۰۴/۰۵/۰۴**

**محمدموسی خورشیدی**
**استادیار پژوهشی مرکز مطالعات راهبردی فراجا (نویسنده مسئول)**
ORCID: 0009-0007-9274-6457
m.khorshidi59@gmail.com

**هادی انصاری**
**کارشناسی ارشد حقوق، دفتر تحقیقات کاربردی فرماندهی مرزبانی استان بوشهر**
ORCID: 0009-0001-1588-4035
آدرس ایمیل: hadiansari13606@gmail.com

## چکیده

صیانت پیش‌رویدادی از کارکنان انتظامی به‌عنوان یک رویکرد پیشگیرانه در تأمین سلامت و ایمنی نیروی انسانی در حوزه‌های امنیتی و انتظامی اهمیت ویژه‌ای دارد. این مقاله مروری، با هدف بررسی نقش فناوری‌های نوین در ارتقای امنیت و پیشگیری از جرم در نیروهای انتظامی، به بررسی گسترده‌ای از پژوهش‌های انجام شده در این حوزه پرداخته است. از جمله یافته‌های کلیدی این پژوهش، می‌توان به موارد زیر اشاره کرد:

الگوریتم‌های یادگیری ماشین و شبکه‌های عصبی مصنوعی قادرند با تحلیل حجم عظیمی از داده‌ها، الگوهای رفتاری مجرمانه را شناسایی کرده و پیش‌بینی کنند. این امر به نیروهای انتظامی امکان می‌دهد تا به صورت پیشگیرانه اقدام کرده و از وقوع جرم جلوگیری کنند. با اتصال دستگاه‌های مختلف به یکدیگر، اینترنت اشیا امکان جمع‌آوری داده‌های فراوانی را فراهم می‌کند که می‌توان از آن‌ها برای نظارت بر محیط و شناسایی تهدیدات بالقوه استفاده کرد. با ایجاد یک دفتر کل توزیع شده و غیرقابل تغییر، بلاکچین می‌تواند به بهبود شفافیت، امنیت و ردیابی شواهد در پرونده‌های جنایی کمک کند. علاوه بر مزایای ذکر شده، این پژوهش به چالش‌های موجود در پیاده‌سازی این فناوری‌ها نیز پرداخته است. از جمله این چالش‌ها می‌توان به نگرانی‌های مربوط به حریم خصوصی، سوگیری الگوریتم‌ها اشاره کرد.

در مجموع، این پژوهش نشان می‌دهد که فناوری‌های نوین می‌توانند به عنوان ابزاری قدرتمند برای مقابله با جرم و صیانت پیش‌کنشی مورد استفاده قرار گیرند.

**کلمات کلیدی:** فناوری‌های نوین، هوش مصنوعی، بلاک‌چین، صیانت پیش‌کنشی، نظارت

## ۱– مقدمه

در دنیای امروزی که پیشرفت‌های علمی و فناوری با سرعت فزاینده‌ای در حال تغییر شیوه‌های زندگی و تعاملات اجتماعی است، نیروی انتظامی نیز به‌عنوان نهادی مهم و مسئول در برقراری نظم و امنیت جامعه، با چالش‌ها و فرصت‌های جدیدی روبه‌رو است. از یک‌سو، متخلفان با استفاده از فناوری‌های نوین به ابزارها و روش‌های پیچیده‌تری برای ارتکاب جرایم دست

یافته‌اند، و از سوی دیگر، تقویت صیانت پیش‌کنشی از کارکنان نیروی انتظامی به‌عنوان یک راهکار استراتژیک جهت پیشگیری از وقوع جرایم و آسیب‌های داخلی و خارجی ضرورت یافته است (Matlala Ramolobi L.G., 2018).

در راستای پیشگیری از تخلفات احتمالی، باید از روش‌ها و تکنیک‌های گوناگونی که مبتنی بر اصول علمی و منطقی هستند بهره گرفت تا افراد به شکل منطقی با آن‌ها مواجه شده و نسبت به نتایج اعمال خود هوشیار شوند و بدانند چه پیامدهایی در انتظارشان است. برای نمونه، می‌توان از اقداماتی مانند افزایش دشواری‌ها و خطرات برای مرتکبان، تشدید مجازات‌ها، یا مزایا و اقدامات پیشگیرانه‌ای بهره برد که مانع ارتکاب جرائم مالی در ناجا شود (Hassanvand et al., 1400).

با توجه به پیچیدگی جرایم مدرن، استفاده از فناوری‌های نوآورانه در صیانت پیش‌کنشی از کارکنان نیروی انتظامی، از قبیل وسایل پرنده بدون سرنشین، هوش مصنوعی، سیستم‌های اطلاعاتی-تحلیلی و چت‌بات‌ها، می‌تواند در ارتقای اثربخشی این نیرو و بهبود روند مقابله با چالش‌های امنیتی نقش اساسی ایفا کند (Tulinov et al., 2022). با این حال، معرفی این فناوری‌ها با موانعی نظیر کمبود بودجه، نقص‌های قانونی و محدودیت‌های روش‌شناختی همراه است که مانع از به‌کارگیری گسترده و مؤثر آن‌ها شده است (Hendrix et al., 2019; Mastrobuoni, 2020).

در این مقاله مروری، ضمن بررسی اهمیت استفاده از فناوری‌های نوین در زمینه صیانت پیش‌کنشی از کارکنان نیروی انتظامی، به تحلیل چالش‌ها و مشکلات پیش روی پیاده‌سازی این فناوری‌ها و ارائه راهکارهای عملی پرداخته می‌شود. هدف اصلی این مقاله، ارائه چارچوبی برای استفاده مؤثر از فناوری‌های نوآورانه در جهت پیشگیری از جرایم و حفاظت از کارکنان نیروی انتظامی در برابر تهدیدهای مختلف است.

## ۲- ادبیات تحقیق

### فناوری‌های نوین[1]

فناوری‌های نوین، فناوری‌هایی هستند که توسعه و یا کاربردهای آن‌ها تا حد زیادی تحقق نیافته‌اند. این فناوری‌ها معمولاً جدید هستند، اما شامل فناوری‌های قدیمی که کاربردهای جدیدی پیدا می‌کنند، نیز می‌شوند. فناوری‌های نوین اغلب قادر به تغییر وضعیت موجود هستند (“Emerging Technologies,” 2024). برجسته‌ترین تأثیر این فناوری‌ها در آینده نهفته است و بنابراین در مرحله معرفی هنوز تا حدودی نامشخص و مبهم است(Rotolo et al., 2015) .

فناوری‌های نوین در حال تحول چشمگیر در شیوه‌های انتظامی هستند و کارایی، شفافیت و قابلیت‌های عملیاتی را افزایش می‌دهند. ادغام هوش مصنوعی[2]، بلاک چین[3] و سیستم‌های اطلاعاتی پیشرفته در حال تغییر شکل نحوه عملکرد سازمان‌های انتظامی است و منجر به بهبود فرآیندهای پیشگیری و تحقیقات جنایی می‌شود.

### صیانت پیش‌کنشی

صیانت پیش‌کنشی به مجموعه‌ای از اقدامات و تدابیر گفته می‌شود که به منظور پیشگیری از وقوع تخلفات و جرایم در میان کارکنان یک سازمان انجام می‌شود. این اقدامات می‌توانند شامل آموزش، آگاه‌سازی، تقویت باورهای دینی و اعتقادی، و بهبود شرایط معیشتی و روانی کارکنان باشند.

**نظریه پیشگیری وضعی[4]**: سیستم‌های نظارتی قوی با افزایش احتمال شناسایی و مجازات، وقوع جرم را کاهش می‌دهند (Eck and Clarke, 2019, p. 1).

[1] Emerging technologies
[2] Artificial Intelligence
[3] Blockchain
[4] Situational Crime Prevention

نظریه پیشگیری از جرم وضعی بر عوامل محیطی مؤثر بر وقوع جرم تمرکز دارد و تلاش می‌کند با کاهش فرصت‌های مجرمانه به جای تمرکز بر ویژگی‌های فردی مجرمان، از وقوع جرم جلوگیری کند. این رویکرد در پیشگیری از جرایم اقتصادی، به‌ویژه تهدیدات نوظهور مانند کلاهبرداری آنلاین و جرایم سایبری، تأثیر قابل‌توجهی دارد. بخش‌های زیر جنبه‌های کلیدی پیشگیری از جرم وضعی و ارتباط آن با پیشگیری از جرایم اقتصادی را بررسی می‌کند.

پیشگیری از جرم وضعی فرصت‌های مجرمانه را با استفاده از چارچوب "تلاش، ریسک، پاداش، تحریک، بهانه‌ها"[1] طبقه‌بندی می‌کند، که به شناسایی و کاهش شرایط مساعد برای جرم کمک می‌کند (Stones and Tilley, 2022).

تکنیک‌هایی مانند مقاوم‌سازی هدف[2]، نظارت[3]، و کنترل دسترسی[4] به‌طور مؤثری در انواع جرایم، از جمله جرایم اقتصادی نظیر کلاهبرداری، به کار گرفته شده‌اند (Eck and Clarke, 2019, p. 1).

اجرای بین‌المللی پیشگیری از جرم وضعی، به‌ویژه در مناطق آمریکای لاتین، نتایج مثبتی در کاهش جرم نشان داده و سازگاری این رویکرد با زمینه‌های مختلف را به اثبات رسانده است (Benito and Tejera, 2020).

پیشرفت سریع فناوری چالش‌هایی برای پیشگیری از جرم وضعی ایجاد می‌کند و نیاز به انطباق مستمر برای مقابله با اشکال جدید جرایم اقتصادی را افزایش می‌دهد (Johnson, 2024).

## ۳– روش تحقیق

این مرور نظام‌مند از استراتژی جستجوی جامعی برای شناسایی مطالعات مرتبط منتشر شده در پایگاه‌های معتبر مانند گوگل اسکالر، ساینس دایرکت، علمنت، ایران‌داک، نورمگز و سیویلیکا استفاده کرده است. اصطلاحات جستجو بر فناوری، نیروهای انتظامی، و پیشگیری از جرم تمرکز داشتند. معیارهای ورود و خروج شامل مقالات پژوهشی منتشرشده به زبان‌های فارسی و انگلیسی با دسترسی به متن کامل بود. پروپوزال‌ها، مقالات غیر مرتبط، بدون داوری و متون غیرعلمی (گزارش خبری، وب‌سایت) حذف شدند. در مجموع، از میان ۱۸۸ عنوان اولیه، ۶۸ مقاله در بازه زمانی ۲۰۱۶ تا ۲۰۲۴ در تحلیل گنجانده شدند. که ۴۰ مقاله آن در بازه ۳ سال پایانی انجام شده است. همچین در جهت بسط مبانی و تعاریف از تحقیق‌های قدیمی‌تر نیز استفاده شد. استخراج داده‌ها برای شناسایی موضوعات کلیدی مانند انواع فناوری‌های استفاده‌شده، کاربردها و چالش‌های موجود انجام شد.

## ۴– یافته‌ها

### جرائم کارکنان

پیشرفت‌های دیجیتال، زمینه‌ساز شکل‌گیری سوءرفتارهای نوین در سازمان‌ها شده است؛ مانند خرابکاری سایبری و همکاری کارکنان با مجرمان خارجی. خرابکاری سایبری شامل آسیب عمدی به زیرساخت‌های دیجیتال با هدف ایجاد اختلال یا دسترسی به اطلاعات حساس است. همدستی نیز به مشارکت کارکنان در جرایمی مانند تقلب یا سرقت اشاره دارد. برای مقابله با این تهدیدات، سازمان‌ها می‌توانند از ارزیابی ریسک پرسنلی بهره بگیرند. یکی از ابزارهای مؤثر در این زمینه، Reid Background Check Plus است که شاخص‌های رفتار پرخطر را شناسایی و هشدارهای امنیتی ارائه می‌دهد (Cunningham et al., 2018).

جرم پلیسی به رفتارهای مجرمانه مأموران پلیس مانند خشونت، سوءمصرف مواد و تخلفات مالی اطلاق می‌شود. به دلیل کمبود داده‌های رسمی، تحلیل دقیق آن دشوار است. مطالعات نشان می‌دهند که این جرائم گسترده بوده و شامل سوءاستفاده

---

[1] effort, risk, reward, provocation, excuses
[2] target hardening
[3] surveillance
[4] access control

جنسی، نقض قوانین مواد مخدر، و فساد مالی هستند؛ به‌طور مثال، در یک پژوهش، ۱۳۹۶ افسر از ۷۸۲ نهاد در ۴۷ ایالت آمریکا مرتکب جرائم مالی شده‌اند (Idy, 2022; Stinson, 2015; Stinson et al., 2016, 2018).

در ایران، پژوهش‌های مختلفی به بررسی جرائم در میان نیروهای انتظامی پرداخته‌اند. برخی بر ارائه راهکارهای قانونی و رفتاری تمرکز داشته‌اند، برخی دیگر دیدگاه‌های دینی و حقوقی درباره جاسوسی را بررسی کرده‌اند. همچنین با بهره‌گیری از داده‌کاوی، مدلی برای پیش‌بینی تخلفات براساس ویژگی‌های شخصیتی ارائه شده است. عوامل محیطی نیز به‌عنوان مؤلفه‌های تأثیرگذار بر عملکرد کارکنان شناسایی شده‌اند (Afshani, 2020; Sharifi, 2020).

در عین حال، برداشت عمومی از رفتار پلیس نقش مهمی در تصویر اجتماعی آن دارد. پژوهش‌ها نشان می‌دهند که رفتارهای کلامی و غیرکلامی پلیس بر این تصویر اثرگذارند. برای مثال، تنظیم واقعی احساسات (کار عاطفی) می‌تواند انحرافات رفتاری را کاهش داده و تعهد شغلی افسران را افزایش دهد (Aghaei et al., 2020; Rahimi and Abbasi Rostami, 2021).

جرائم پلیسی با انگیزه مالی نیز از اهمیت ویژه‌ای برخوردارند، زیرا شامل سوءاستفاده کارکنان از موقعیت شغلی برای کسب منافع مالی می‌شوند. این جرائم به سه دسته تقسیم می‌شوند: جرائم سارقانه که اغلب شامل سرقت یا اخاذی هستند؛ جرائم مبتنی بر بازار که به بهره‌برداری از بازارهای غیرقانونی مانند قاچاق مواد مخدر مرتبط‌اند؛ و جرائم تجاری که از منابع نیروی انتظامی برای منافع مالی استفاده می‌کنند (Lemos & Minzner, 2014; Naylor, 2003).

همچنین، برخی پژوهش‌ها در ایران به جرائم اقتصادی و سوءرفتار در میان نیروهای انتظامی و کارکنان دولتی پرداخته‌اند. نتایج نشان می‌دهد که عواملی مانند بیکاری، تورم، نرخ ارز و مداخلات دولتی در اقتصاد، زمینه‌ساز افزایش فساد و تخلفات اداری هستند. این یافته‌ها بر ضرورت اصلاح ساختارهای اقتصادی و حاکمیتی برای پیشگیری از جرم تأکید دارند (Poya et al., 2020).

در مجموع، این پیشرفت‌ها در مطالعات جرم‌شناسی و همچنین ارزیابی رفتارهای کارکنان، به سازمان‌ها و نهادهای انتظامی کمک می‌کنند تا با شناخت بهتر از الگوها و رفتارهای پرخطر، راهکارهای مؤثری برای مقابله با تهدیدات داخلی و خارجی اتخاذ کنند و به بهبود امنیت و کاهش جرائم دست یابند.

**فناوری‌های نوین در صیانت پیش‌کنشی**

ترکیب فناوری‌های نوین، به‌ویژه هوش مصنوعی، تحولی در پیشگیری از جرم و ارتقای عملکرد نهادهای انتظامی ایجاد کرده است. هوش مصنوعی با قابلیت‌هایی مانند پیش‌بینی جرم، نظارت بلادرنگ و تحلیل داده‌های جنایی، به شناسایی تهدیدات و تحلیل دقیق‌تر شواهد کمک می‌کند. همچنین ابزارهایی چون تشخیص چهره، صدا و پایش شبکه‌های اجتماعی، امکان جمع‌آوری اطلاعات لحظه‌ای از مظنونان و شبکه‌های مجرمانه را فراهم می‌سازند (Fatih & Bekir, 2015).

پلیس پیش‌بینی‌کننده با بهره‌گیری از الگوریتم‌های هوش مصنوعی، داده‌های گذشته را تحلیل کرده و الگوهای جرم را شناسایی می‌کند. این رویکرد به تخصیص هوشمند منابع و استقرار نیروها در مناطق پرخطر کمک می‌کند. همچنین، فناوری‌هایی مانند تشخیص چهره و نظارت خودکار، نظارت لحظه‌ای را تقویت کرده و امکان واکنش سریع به جرایم را فراهم می‌سازند. هوش مصنوعی با تسریع تطبیق DNA و تحلیل شواهد دیجیتال، به حل مؤثرتر پرونده‌ها نیز کمک می‌کند. با این حال، استفاده از این فناوری‌ها مستلزم توجه به مسائل اخلاقی و تدوین قوانین مناسب است تا ضمن بهره‌گیری از مزایای آن، خطراتی مانند نقض حریم خصوصی یا سوءاستفاده کاهش یابد (Kobets, 2024; Sukhodolov & Bychkova, 2018).

هوش مصنوعی در جنبه‌هایی مانند پیش‌بینی جرم، تشخیص چهره و تحلیل داده به پلیس کمک می‌کند که الگوهای جرم را شناسایی کرده و منابع خود را بهینه‌تر توزیع کند. هرچند همچنان نگرانی‌هایی در مورد حفظ حریم خصوصی و احتمال سوگیری در این سیستم‌ها وجود دارد (Lunhol & Torhalo, 2024).

نیروهای انتظامی، برای مقابله با جرایمی که به کمک فناوری‌های اطلاعات و ارتباطات انجام می‌شوند، در حال به‌روزرسانی استراتژی‌های خود هستند. این مسئله به‌ویژه در حوزه‌هایی مانند حمل‌ونقل اهمیت بیشتری دارد، چراکه مجرمان معمولاً از شبکه‌های ارتباطی و کانال‌های دیجیتال برای هماهنگی عملیات قاچاق، پنهان کردن تراکنش‌های مالی و دور زدن سیستم‌های شناسایی استفاده می‌کنند (Fomin & Luk'janova, 2023).

نهادهای انتظامی با استفاده از فناوری‌های نظارت پیشرفته و ابزارهای شنود، توانایی بیشتری در ردیابی این شبکه‌ها و شناسایی فعالیت‌های مشکوک دارند و می‌توانند قبل از گسترش اقدامات غیرقانونی، آن‌ها را متوقف کنند. این نظارت دقیق همچنین احتمال همکاری‌های مجرمانه درون سازمان‌های انتظامی را کاهش می‌دهد.

**هوش مصنوعی**

هوش مصنوعی به توانایی ماشین‌ها در درک محیط، یادگیری و اقدام هدفمند گفته می‌شود (Russell & Norvig, 2016). در سال‌های اخیر، این فناوری به ابزاری کلیدی در حوزه امنیت و پلیس تبدیل شده است. هوش مصنوعی با تحلیل داده‌ها و شناسایی رفتارهای ناهنجار، اقدامات پیشگیرانه را پیشنهاد می‌دهد. همچنین، سیستم‌های مدیریت اطلاعات با تحلیل الگوهای جرمی، نقش مؤثری در پیشگیری از جرایم به‌ویژه در حوزه سایبری ایفا می‌کنند (Rajabi Taj Amir et al., 2022).

پژوهش‌های اخیر نشان می‌دهد که پیشرفت سریع هوش مصنوعی و یادگیری ماشین تأثیر قابل‌توجهی بر حکمرانی عمومی گذاشته است. این فناوری‌ها با افزایش دقت تصمیم‌گیری، بهینه‌سازی تخصیص منابع و ارتقای شفافیت، می‌توانند کارایی نظام‌های حکمرانی را بهبود بخشند. بااین‌حال، چالش‌هایی همچون مسائل اخلاقی، نظارتی و حقوقی نیز در این مسیر مطرح است. Sadeghian (۲۰۲۵) در مطالعه‌ای فراتحلیلی بر اساس بررسی ۳۱ پژوهش کلیدی بین سال‌های ۲۰۱۵ تا ۲۰۲۳، مدلی سه‌بعدی از حکمرانی هوش مصنوعی ارائه کرده که شامل ابعاد فنی، حقوقی ـ اخلاقی و سیاست‌گذاری عمومی است. نتایج این تحقیق بر لزوم ایجاد چارچوب‌های قانونی شفاف، تقویت سازوکارهای نظارتی و توسعه رویکردهای مسئولانه در بهره‌گیری از هوش مصنوعی در نظام‌های حکمرانی تأکید دارد.

مدل‌های هوش مصنوعی برای پیشگیری از جرایم سایبری: مدل‌های هوش مصنوعی با تحلیل حجم عظیمی از داده‌ها به شناسایی الگوهایی که ممکن است نشان‌دهنده تهدیدات امنیتی باشند کمک می‌کنند. این الگوها می‌توانند شامل رفتارهای غیرمعمول در ورود، انتقال‌های غیرمنتظره داده‌ها یا دسترسی‌های غیرمجاز به سیستم‌ها باشند که همگی از نشانه‌های ابتدایی حملات سایبری محسوب می‌شوند. تشخیص سریع این الگوها به تیم‌های امنیتی امکان می‌دهد پیش از وقوع تهدیدات جدی، اقدامات مناسب را انجام دهند (Awasthi et al., 2023).

پلیس پیش‌بینی‌کننده و تحلیل جرم: استفاده از داده‌های تاریخی، جمعیت‌شناسی و ویژگی‌های محله‌ای به پلیس این امکان را می‌دهد که با تخصیص بهتر منابع و تمرکز بر مناطق یا افراد با ریسک بالا، به‌شکل پیشگیرانه وارد عمل شود. به‌طور مثال، با استفاده از داده‌های مکانی و زمانی، مناطق داغ جرم شناسایی شده و نیروهای پلیس به‌شکل کارآمدتری در این مناطق مستقر می‌شوند. این روش که به "پلیس پیش‌بینی‌کننده" معروف است، توانسته به کاهش جرم و بهبود امنیت عمومی کمک شایانی کند (Kahla, 2024).

نقشه‌برداری جرم و تخصیص بهینه منابع: در این روش، داده‌های جغرافیایی و جمعیتی با استفاده از رنگ‌ها و نمادهای خاص برای نمایش مناطق پرخطر به‌کار می‌روند. به این ترتیب، پیچیدگی داده‌های جرم به‌صورت تصویری ساده‌تر قابل درک شده و تصمیم‌گیری در تخصیص منابع برای جلوگیری از جرایم بهینه می‌شود (Kolodyazhny, 2020). الگوریتم‌های یادگیری ماشین در این زمینه با تحلیل داده‌های حجیم، الگوها و پیش‌بینی‌های دقیقی از رفتارهای مجرمانه ارائه می‌دهند. این فرایند به سازمان‌های نظامی کمک می‌کند تا به‌طور پیشگیرانه عمل کرده و از وقوع جرم پیشگیری کنند (Kahla, 2024).

رویکردهای پیشرفته هوش مصنوعی در امنیت سایبری: الگوریتم‌های هوش مصنوعی با شناسایی الگوهای شبکه‌ای غیرمعمول به تشخیص تهدیدات امنیتی کمک می‌کنند. این روند شامل تحلیل ترافیک شبکه و شناسایی انحرافات از فعالیت‌های عادی است که در صورت مشاهده، به‌طور خودکار علامت‌گذاری شده و برای بررسی بیشتر ارسال می‌شود (Sharma et al., 2024). در برخی موارد، سیستم‌های هوش مصنوعی حتی قابلیت پاسخ‌دهی خودکار دارند؛ برای مثال، می‌توانند در صورت شناسایی ناهنجاری، دستگاه یا سیستم آلوده را ایزوله کرده و از گسترش تهدید جلوگیری کنند (Awasthi et al., 2023).

نمایه‌سازی رفتاری و شناسایی نیت‌های مجرمانه: این فناوری با شناسایی الگوهای رفتاری غیرمعمول در افراد می‌تواند به‌صورت پیشگیرانه نشانه‌های نیت‌های مجرمانه را شناسایی کند. برای مثال، رفتارهایی همچون خریدهای غیرمعمول یا فعالیت‌های تکراری مشکوک می‌توانند نشانه‌ای از برنامه‌ریزی یک جرم احتمالی باشند. نمایه‌سازی رفتاری بر اساس داده‌های جمع‌آوری‌شده، به سازمان‌های امنیتی کمک می‌کند تا پیش از وقوع جرم، اقدامات پیشگیرانه انجام دهند (Kahla, 2024; Mena, 2011).

پیشرفت‌های جدید در مدل‌های یادگیری ماشین: پژوهش‌ها نشان می‌دهند مدل‌هایی مانند جنگل‌های تصادفی و درختان تصمیم‌گیری با تحلیل داده‌های فضایی-زمانی، انواع جرم را پیش‌بینی می‌کنند و در مناطق پرخطر به تمرکز منابع و کاهش جرم کمک کرده‌اند. همچنین، تکنیک‌های متوازن‌سازی داده و یادگیری بدون نظارت، دقت پیش‌بینی و تحلیل روندهای مجرمانه را افزایش می‌دهند و تخصیص بهینه منابع را ممکن می‌سازند (Sardana et al., 2021; Shama, 2017).

این رویکردها و ابزارهای نوین در هوش مصنوعی به سازمان‌های امنیتی کمک می‌کنند تا تحلیل دقیق‌تری از داده‌ها ارائه دهند و از طریق بینش‌های مبتنی بر داده و تصمیم‌گیری فعالانه، امنیت عمومی را ارتقا بخشیده و منابع را به بهترین شکل تخصیص دهند (Dharsan et al., 2023).

**نگرانی‌ها از هوش مصنوعی**

استفاده گسترده از هوش مصنوعی در پیشگیری از جرم و اجرای قانون، نگرانی‌های اخلاقی و حقوقی مانند تبعیض، ناعادلانه بودن نتایج و فقدان شفافیت را به دنبال داشته است؛ چرا که داده‌های آموزشی ممکن است سوگیری داشته باشند. بنابراین، تدوین چارچوب‌های اخلاقی و قانونی برای تضمین احترام به حقوق افراد ضروری است (Dimovski & Grujić, 2024; Sukhodolov & Bychkova, 2018).

هوش مصنوعی همچنین خطرات جدیدی مانند جرایم سایبری و سوءاستفاده از سیستم‌های نظارتی را ایجاد کرده است که نیازمند قوانین و پروتکل‌های امنیتی سختگیرانه است (Kobets, 2024). حفاظت از اطلاعات شخصی نیز اهمیت یافته و رویکردهایی مانند رمزنگاری و آموزش عمومی برای افزایش آگاهی درباره حفظ حریم خصوصی لازم است (Tsvyk & Tsvyk, 2023).

چالش‌های استفاده از هوش مصنوعی در قانون را می‌توان به مشکلات فنی (دقت، امنیت سایبری) و ملاحظات ذهنی (اعتماد عمومی، اخلاق) تقسیم کرد که به قوانین شفاف و پاسخگو نیاز دارد تا هم منافع امنیتی و هم حقوق فردی حفظ شوند(Tulinov et al., 2022).

در نهایت، نظارت با هوش مصنوعی ممکن است باعث استرس و کاهش رضایت شغلی کارکنان شود، بنابراین باید بین نیازهای نظارتی و حفظ حریم خصوصی تعادل برقرار کرد و سیاست‌های روشن و احترام به حقوق کارکنان را رعایت کرد (Kot, 2021).

**فناوری بلاک‌چین**

بلاکچین یک سیستم ذخیره‌سازی دیجیتال اطلاعات است که داده‌ها را در قالب بلوک‌هایی به هم پیوسته ذخیره می‌کند. هر بلوک شامل کد منحصر به فرد، زمان ثبت و جزئیات تراکنش‌ها است و به بلوک قبلی متصل می‌شود، به‌طوری که تغییر اطلاعات بسیار دشوار است و امنیت بالایی دارد (Iansiti & Lakhani, 2017).

ویژگی‌های بلاکچین مانند شفافیت، امنیت و تغییرناپذیری، آن را به ابزاری مؤثر در بهبود عملکرد نهادهای انتظامی و قضایی تبدیل کرده است. به‌عنوان مثال، پلیس دهلی از بلاکچین برای ردیابی و مدیریت شواهد استفاده می‌کند که از تغییر یا سوءاستفاده جلوگیری کرده و تخلفات مالی را کاهش می‌دهد (Feltovic, 2024; Rukinov, 2020).

Ghajari (۲۰۲۵) در پژوهشی مروری درباره کاربرد فناوری بلاک‌چین در فرایندهای اداری نشان می‌دهد که این فناوری با ارتقای شفافیت، کارایی و اعتماد می‌تواند موجب تحول چشمگیر در نظام اداری شود. نتایج تحقیق بر اهمیت بررسی چالش‌های فنی، حقوقی، امنیتی و حکمرانی در مسیر پذیرش این فناوری تأکید دارد. همچنین چارچوبی برای اجرای مؤثر بلاک‌چین پیشنهاد شده که بر امنیت داده‌ها، حفظ حریم خصوصی و طراحی نظام نظارتی کارآمد تمرکز دارد. به‌رغم محدودیت‌هایی مانند کمبود منابع نظری و تحولات سریع فناوری، این پژوهش تصویری روشن از ظرفیت‌ها و ریسک‌های به‌کارگیری بلاک‌چین در بهبود کارایی و شفافیت فرایندهای سازمانی ارائه می‌دهد.

همچنین، قراردادهای هوشمند در بلاکچین فرآیندهای مالی و اداری مانند پرداخت‌ها و مدیریت مزایا را به‌صورت خودکار و امن انجام می‌دهند و احتمال تخلف را کاهش می‌دهند. بلاکچین ابزار مؤثری برای مقابله با جرایم سایبری و پولشویی است، زیرا امکان پیگیری دقیق تراکنش‌ها و شناسایی فعالیت‌های مشکوک را فراهم می‌کند (Mousavi Barangi et al., 2020 ; et al., 2022).

یکی دیگر از کاربردهای بلاک‌چین، ایجاد مدلی برای حفاظت از شواهد است. مدل زنجیره شواهد[1] با بهره‌گیری از فناوری "دفترکل توزیع‌شده[2]" به شهروندان اجازه می‌دهد که شواهد را به‌صورت ناشناس و ایمن بارگذاری کنند. این مدل، به‌ویژه در کشورهایی که سیستم‌های قضایی و انتظامی ممکن است دچار فساد باشند، اطمینان می‌دهد که شواهد به‌صورت یکپارچه و غیرقابل تغییر حفظ شوند، که این امر به کاهش بی‌اعتمادی و ترس شهروندان کمک می‌کند (Shahaab et al., 2021).

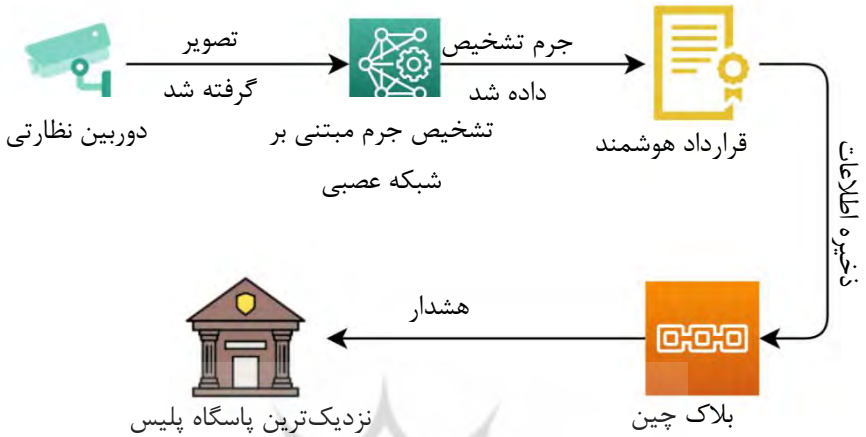
بلاک‌چین با ترکیب با فناوری‌های هوش مصنوعی، امکان تشخیص خودکار جرم را فراهم می‌کند. به‌عنوان نمونه، مدل بلوک جرم از طریق تحلیل داده‌ها و شناسایی الگوهای مشکوک، می‌تواند به‌صورت بلادرنگ فعالیت‌های مجرمانه را شناسایی و به ایمنی عمومی کمک کند. همچنین، ذخیره‌سازی امن داده‌های صحنه جرم و اطلاعات حساس در بلاک‌چین می‌تواند از دستکاری آن‌ها جلوگیری کند و به یکپارچگی سوابق صحنه جرم اطمینان ببخشد (Patel et al., 2022).

مراکز هوشمند مبارزه با جرم با ادغام فناوری‌ها و داده‌ها، به پلیس در شناسایی و واکنش مؤثرتر به جرم کمک می‌کنند. مطالعه‌ای توسط Arietti، (2024) نشان داد که این فناوری‌ها در شیکاگو نرخ رسیدگی به پرونده‌های خشونت‌آمیز و جرایم دارایی را بهبود بخشیده و حل پرونده‌ها را افزایش داده‌اند.

شکل ۱ کارکرد سیستم پیشنهادی بلوک جرم را نشان می‌دهد. این مدل شامل تجهیزات نظارتی شهری است که در مکان‌های با نیاز به امنیت بالا نصب می‌شوند. این سیستم‌ها تصاویر ویدئویی را به‌طور مداوم ضبط کرده و به یک «معماری شبکه عصبی پیچشی آموزش‌دیده» ارسال می‌کنند تا تهدیدها و رفتارهای مجرمانه را شناسایی کند. در صورت شناسایی فعالیت مشکوک، هشدار صادر شده و قرارداد هوشمند مبتنی بر بلاک‌چین فعال می‌شود. این قرارداد محل وقوع جرم را ذخیره و نزدیک‌ترین ایستگاه پلیس را شناسایی کرده و از طریق کانال امن اطلاع‌رسانی می‌کند تا پلیس سریعاً وارد عمل شود (Patel et al., 2022).

[1] EvidenceChain
[2] DLT

بلاک‌چین همچنین برای ذخیره‌سازی امن داده‌های مربوط به صحنه جرم نیز مورد استفاده قرار می‌گیرد. این فناوری امکان ذخیره‌سازی دائمی و دسترسی آسان به داده‌های حساس را برای نهادهای قانونی فراهم می‌کند و از دستکاری آن‌ها جلوگیری می‌نماید. چنین سیستم‌هایی موجب حفظ اصالت سوابق صحنه جرم می‌شوند و به کاهش فساد کمک می‌کنند (Ghazi Nejad et al., 2024).




**تصویرشماره (۱): مدل سیستم بلوک جرم (Patel et al., 2022)**

فناوری بلاک‌چین با شفافیت و تغییرناپذیری خود می‌تواند در کاهش جرایم شرکتی مؤثر باشد، زیرا از تخلفات مالی جلوگیری کرده و انطباق با قوانین را تسهیل می‌کند. این فناوری امکان نظارت مداوم بر فعالیت‌های غیرمجاز و شناسایی سریع تراکنش‌های مشکوک را فراهم می‌کند و رویکردی فعالانه برای پیشگیری از جرایم شرکتی ایجاد می‌کند (Kabiru et al., 2024).

علاوه بر این، بلاک‌چین با ارتقای امنیت سایبری، تضمین یکپارچگی و اصالت داده‌ها، به بهبود روش‌های انتظامی کمک می‌کند. سیستم‌هایی مانند CRAB که از بلاک‌چین برای ذخیره و حفاظت از سوابق جنایی استفاده می‌کنند، فساد را کاهش داده و مدیریت سوابق را بهبود می‌بخشند. این فناوری‌ها با افزایش امنیت و شفافیت، پلیس را در پاسخ به نیازهای امنیتی عمومی یاری می‌رسانند (Kesarkar, 2024; Tasnim et al., 2018).

**اینترنت اشیاء**

اینترنت اشیا[1] به دستگاه‌هایی گفته می‌شود که با حسگرها و فناوری‌های ارتباطی، قادر به اتصال و تبادل داده با دیگر سیستم‌ها هستند(Dey et al., 2017). ادغام اینترنت اشیا و هوش مصنوعی، تحول چشمگیری در پیشگیری از جرم و اجرای قانون ایجاد کرده است؛ این فناوری‌ها با نظارت پیشرفته، امنیت سایبری و تحلیل داده‌های دقیق، به شناسایی زودهنگام تهدیدها کمک می‌کنند.

از طریق اینترنت اشیا و داده‌های بیومتریک، امکان ردیابی و نظارت بر افراد مشروط فراهم شده که باعث افزایش کارایی پلیس و کاهش نیاز به حضور فیزیکی می‌شود (Dlodlo et al., 2015). همچنین، حسگرهای اینترنت اشیا می‌توانند خطرات محیطی را شناسایی و به پیشگیری از جرایم کمک کنند (Alinejad, 1403).

[1] Internet of Things

هوش مصنوعی با تحلیل داده‌های بلادرنگ از دوربین‌ها و حسگرها، پاسخ سریع‌تر و دقیق‌تری به حوادث ارائه می‌دهد و رفتارهای مجرمانه را شناسایی می‌کند (Kahla, 2024; Saini et al., 2023; Singh & Ramdeo, 2023).

این هم‌گرایی فناوری‌ها، محدودیت روش‌های سنتی پیشگیری از جرم را کاهش داده و امکان هشدار خودکار در مناطق پرخطر را فراهم می‌کند (Jeon & Jeong, 2016).

در کل، ترکیب اینترنت اشیا و هوش مصنوعی با تحلیل مداوم داده‌ها، کارایی نظارت و ایمنی عمومی را بهبود بخشیده و رویکردی فعالانه در پیشگیری از جرم به سازمان‌های انتظامی می‌دهد.

**سیستم‌های نظارت تصویری مبتنی بر هوش مصنوعی**

سیستم‌های نظارت تصویری که با هوش مصنوعی تقویت شده‌اند، توانایی‌های نظارتی و شناسایی ناهنجاری‌ها در لحظه را افزایش می‌دهند و برای شناسایی رفتارهای مشکوک در مکان‌های مختلف اهمیت دارند (Kahla, 2024). این سیستم‌ها با تجزیه و تحلیل جریان‌های ویدیویی و استفاده از فناوری تشخیص چهره، حجم زیادی از داده‌ها را پردازش کرده و به طور مؤثری از پیش‌بینی و پیشگیری از جرم پشتیبانی می‌کنند(Sukhodolov & Bychkova, 2018) . در این راستا، چین به عنوان یکی از پیشتازان استفاده از فناوری نظارت تصویری مبتنی بر هوش مصنوعی شناخته می‌شود (Kolodyazhny, 2020). این سیستم‌ها با فراهم کردن تحلیل‌های پیوسته و زنده به نیروهای انتظامی کمک می‌کنند تا بتوانند به سرعت به تهدیدات امنیتی احتمالی واکنش نشان دهند.

Vafaei, Daneshfard, and Mousakhani (۲۰۲۵) در پژوهشی به طراحی الگویی برای نظارت بر اثربخشی خط‌مشی‌های عمومی در عصر دیجیتال پرداختند. در این مطالعه، بعد فناوری و نوآوری در نظارت را یکی حوزه‌های اصلی شناسایی کرده است. نتایج نشان می‌دهد که استقرار نظام نظارتی کارآمد می‌تواند به ارتقای کیفیت اجرا و بهبود مستمر خط‌مشی‌های عمومی کمک کند.

تحلیل ویدیویی مبتنی بر هوش مصنوعی، امکان نظارت و شناسایی مستمر رفتارهای مشکوک را فراهم می‌کند و با افزایش کارایی نظارت، به کاهش وقوع جرم کمک می‌کند. این سیستم‌ها قادرند رفتارهای غیرعادی را در لحظه شناسایی کرده و به نیروهای انتظامی هشدار دهند و این امکان را فراهم کنند تا به تهدیدات احتمالی سریع‌تر واکنش نشان دهند (Kahla, 2024; Ninoria et al., 2023).

دوربین‌های مداربسته پیشرفته با هوش مصنوعی، به‌ویژه در مناطق شهری پرجرم، نظارت و شناسایی خودکار اشیاء را تسریع و واکنش به تهدیدات را بهبود می‌بخشند(Kolodyazhny, 2020).

فناوری‌های نوآورانه مانند رباتیک، پهپادها و نقشه جرم نیز در کنار نظارت هوشمند به اجرای قانون کمک می‌کنند؛ مثلاً پهپادها مناطق وسیع را پوشش می‌دهند و ابزارهای نقشه جرم با تحلیل داده‌ها، مناطق جرم‌خیز را شناسایی و تخصیص بهینه منابع را ممکن می‌سازند (Tulinov et al., 2022).

پلیس پیش‌بینی‌کننده با بهره‌گیری از الگوریتم‌های هوش مصنوعی داده‌های جرم را تحلیل کرده و نقاط احتمالی وقوع جرم را شناسایی می‌کند که این امر در تخصیص بهتر منابع پلیس بسیار مؤثر است (Bag et al., 2024; Kahla, 2024). مطالعات نشان داده‌اند که این روش به کاهش چشمگیر نرخ جرم و تخلف منجر شده است؛ به‌طوری‌که در یک مطالعه، ۴۳ درصد از تغییرات نرخ جرم به تحلیل‌های مبتنی بر هوش مصنوعی نسبت داده شده است (Eran & Hasranizam, 2024).

مدل‌های هوش مصنوعی مانند MobileNet V2 و YOLO در سیستم‌های نظارتی برای بهبود پردازش ویدیویی استفاده می‌شوند. MobileNet V2 به‌خاطر سرعت اجرا در موبایل و YOLO به‌خاطر تشخیص سریع اشیاء، امکان شناسایی

دقیق و فوری فعالیت‌های غیرقانونی، سلاح‌ها و رفتارهای مشکوک را فراهم می‌کنند و کارایی سیستم‌های نظارت را افزایش می‌دهند (Zhadan et al., 2024).

**دوربین‌های بدن‌پوش پلیس**

دوربین‌های بدن‌پوش پلیس ابزار مهمی برای افزایش شفافیت و پاسخگویی در تعاملات نیروهای انتظامی با شهروندان هستند. این دوربین‌ها با ضبط صدا و تصویر، شواهد بی‌طرفانه‌ای ارائه می‌دهند که می‌تواند در حل اختلافات و کاهش تنش‌ها مؤثر باشد (Milidragovic & Milić, 2024).

همچنین، این دوربین‌ها امنیت افسران را افزایش داده و رفتار محترمانه‌تر در تعاملات را ایجاب می‌کنند (Douglas, 2021) (Jones, 2016).

با این حال، تأثیر آنها بر کاهش تخلفات و استفاده از زور هنوز مورد بحث است و برخی معتقدند مشکلات ساختاری عمیق‌تر پلیس نیازمند اصلاحات گسترده‌تر است. دوربین‌ها باید در کنار آموزش، ارزیابی روان‌شناختی و حمایت‌های دیگر به کار گرفته شوند تا نتیجه بهتری داشته باشند (Rai، ۲۰۱۹؛ Peterson و Lawrence، ۲۰۱۹).

از سوی دیگر، دوربین‌های بدن‌پوش نقش مهمی در فرآیندهای قضایی دارند و شواهد تصویری آنها معتبرتر از اظهارات شفاهی است. اما نگرانی‌هایی درباره حفظ حریم خصوصی و مدیریت داده‌های ضبط شده وجود دارد که نیازمند تدوین سیاست‌های شفاف و امنیتی است (Milidragovic & Milić, 2024).

در مجموع، این دوربین‌ها می‌توانند اعتماد بین پلیس و جامعه را تقویت کنند، اما برای اثربخشی بیشتر باید جزئی از برنامه جامع اصلاحات پلیسی همراه با رعایت مسائل حریم خصوصی و حمایت‌های قانونی باشند.

## ۵–بحث و نتیجه‌گیری

ادغام فناوری‌های نوین در نیروهای انتظامی، ظرفیت قابل‌توجهی برای ارتقای امنیت عمومی و بهبود کارایی عملیات پلیس ارائه می‌دهد. فناوری‌هایی مانند هوش مصنوعی، دوربین‌های بدن‌پوش، اینترنت اشیا و بلاکچین می‌توانند در زمینه نظارت، تحلیل داده‌ها و پیش‌بینی جرم تحولات شگرفی ایجاد کنند. یافته‌ها حاکی از آن است که در بعضی از موارد استفاده از فناوری-های نوین تا ۴۰ درصد باعث کاهش تخلف شده است. در ادامه، چند کاربرد و مسیر آینده این فناوری‌ها در این حوزه آمده است:

با گسترش دستگاه‌های متصل، داده‌های اینترنت اشیا می‌توانند به عنوان شواهد ارزشمند به‌کار روند. فناوری‌های هوش مصنوعی و داده‌های بزرگ می‌توانند حجم زیادی از داده‌های دیجیتال مثل ایمیل‌ها، پست‌های شبکه‌های اجتماعی و سوابق ارتباطی را برای کشف الگوها، ارتباطات و شواهد بررسی کنند.

الگوریتم‌های هوش مصنوعی می‌توانند با تحلیل داده‌های تاریخی مانند سوابق کیفری، عوامل اقتصادی-اجتماعی، ارزیابی دقیق‌تری از ریسک ارائه دهند.

با استفاده از دستگاه‌های اینترنت اشیا و الگوریتم‌های هوش مصنوعی می‌توان تراکنش‌های مالی را تحلیل کرده، الگوهای مشکوک را شناسایی و علائم تقلب یا جرایم مالی را کشف کرد. این کار می‌تواند به پلیس و نهادهای مالی در پیشگیری و پیگیری چنین جرایمی کمک کند.

ویژگی غیرقابل تغییر بلاک‌چین می‌تواند امنیت ثبت رویدادها را تضمین کند و زمینه تبعات قانونی ناشی از دستکاری شواهد را به‌طور قابل توجهی کاهش دهد. با فراهم شدن دید کامل و خطی از تمامی مراحل، نهادهای قضایی و انتظامی می‌توانند در هر لحظه به سوابق دسترسی پیدا کرده و فرایند ممیزی را تسهیل کنند. پیاده‌سازی این فناوری‌ها، ضمن کاهش هزینه‌های بلندمدت ناشی از اختلافات قضایی، بار مالی حکومت در حوزه ایمنی عمومی و دادرسی را کاهش می‌دهد.

پیشنهاد می‌شود یک مدل مرجع بلاک‌چین شامل تعریفی از ساختار داده‌ها و مکانیسم افزودن بلاک جدید طراحی شود. همچنین قوانین خودکار برای تأیید هر مرحله از انتقال شواهد، هش‌گذاری توافقی و اطلاع‌رسانی بی‌درنگ نوشته شود و داشبوردی برای نمایش زنجیره شواهد و ابزارهای جستجو و گزارش‌گیری اجرا شود. باید درنظر داشت که نقش ناظر مستقل (بازرس قضایی) در تعیین سیاست‌های کنترلی مشخص گردد. استانداردهای امنیت اطلاعات (ISO/IEC) به‌طور اجباری در اجرا لحاظ شود.

با توجه سودمندی‌های ذکر شده باید در نظر داشت که پذیرش این فناوری‌ها باید با در نظر گرفتن پیامدهای اخلاقی، نگرانی‌های حریم خصوصی و احتمال سوگیری‌ها همراه باشد. برای استفاده مسئولانه و مؤثر از این فناوری‌ها، ضروری است که چارچوب‌های قانونی مشخصی ایجاد شده و مکانیزم‌های حاکمیتی قوی توسعه یابند.

مطالعات پیشین نیز بر اهمیت بهره‌گیری از فناوری‌های پیشرفته در پیشگیری از جرم و ارتقای اثربخشی نیروهای انتظامی تأکید کرده‌اند. یافته‌های این پژوهش با این مطالعات هم‌راستا است؛ برای مثال، مشخص شد الگوریتم‌های یادگیری ماشین و شبکه‌های عصبی مصنوعی می‌توانند با تحلیل حجم عظیمی از داده‌ها الگوهای جرم را پیش‌بینی کنند و بدین ترتیب امکان اقدام پیشگیرانه را فراهم سازند. همچنین، همان‌طور که منابع پژوهشی قبلی نشان داده‌اند (Dlodlo et al., 2015; Kahla, 2024; Alinejad, 1403)، اتصال دستگاه‌های اینترنت اشیا داده‌های محیطی فراوانی را در اختیار می‌گذارد که برای شناسایی تهدیدات بالقوه کاربرد دارد.

یافته‌های این تحقیق بر نوآوری تلفیق چند فناوری نوظهور (هوش مصنوعی، بلاک‌چین، اینترنت اشیا و سیستم‌های نظارتی هوشمند) در چارچوب پیشگیری پیش‌کنشی تأکید می‌کنند و بدین ترتیب به غنای دانش موجود افزوده‌اند. بطور خاص، با وجود تحقیقات متعدد در حوزه بلاک‌چین و زنجیره نگهداری شواهد دیجیتال (Arietti, 2024; Feltovic, 2024; Mousavi et al., 2022)، این پژوهش با بررسی نوین کاربرد بلاک‌چین در مدیریت و حفظ یکپارچگی شواهد فیزیکی جنایی، خلأ قابل‌توجهی را شناسایی کرده است. افزون بر این، با اشاره به محدودیت‌ها و چالش‌های پیاده‌سازی (نظیر ملاحظات حریم خصوصی و مداخله عناصر ناهشیار الگوریتم‌ها)، این تحقیق چشم‌انداز روشن‌تری نسبت به نیازهای پژوهشی و کاربردی آینده ارائه می‌دهد.

این مطالعه، مانند بسیاری از مرورهای نظام‌مند، با محدودیت‌هایی مواجه است. اولاً، دسترسی به منابع علمی محدود به مقالات فارسی و انگلیسی دارای متن کامل بوده و احتمالاً برخی از مطالعات مرتبط (به‌ویژه گزارش‌ها و متون غیرایندکس‌شده) از قلم افتاده است. ثانیاً، بسیاری از یافته‌ها بر اساس داده‌های ثانویه و تحلیل کیفی گزارش‌هاست و آزمایش‌ها یا پیاده‌سازی‌های میدانی جدید را شامل نمی‌شود. علاوه بر این، همان‌گونه که پژوهش‌های دیگر نشان داده‌اند، محدودیت‌های قانونی، مشکلات فنی و ملاحظات بودجه‌ای می‌تواند مانع به‌کارگیری کامل فناوری‌های نوین شود.

مثلاً ضعف استانداردهای فنی یا کمبود زیرساخت‌های ارتباطی ممکن است باعث کاهش دقت سیستم‌های مبتنی بر هوش مصنوعی شود. نگرانی‌های اخلاقی و مسأله سوگیری الگوریتم‌ها نیز نباید نادیده گرفته شوند؛ پژوهش‌ها بر نیاز به چارچوب‌های شفاف حقوقی و اخلاقی برای تضمین عدالت و حفظ حقوق شهروندان تأکید کرده‌اند.

بر اساس مرور نظام‌مند ادبیات، مشخص شد که تحقیقات اندکی به کاربرد بلاک‌چین و قراردادهای هوشمند برای افزایش اطمینان از صحت و یکپارچگی زنجیره دلایل فیزیکی پرداخته‌اند. این کمبود، فرصت مهمی برای پژوهشگران ایجاد می‌کند تا ضمن تعمیم الزامات کلان زنجیره حفاظتی به هر دو حوزه دیجیتال و فیزیکی، چارچوب‌های مبتنی بر بلاک‌چین را طراحی و ارزیابی کنند. به‌ویژه، پژوهش‌های آینده باید به بررسی محدودیت‌های فنی، چالش‌های حقوقی و اقتصادی، و سنجش عملیاتی مدل‌های پیشنهادی در محیط‌های واقعی بپردازند.

پژوهش‌های تجربی میدانی برای ارزیابی کارایی چارچوب در حوزه‌های مختلف ضروری است. همچنین، همکاری دانشگاه، صنعت و نهادهای قانونی می‌تواند به توسعه و آزمون نمونه‌های واقعی کمک کند. سرمایه‌گذاری در کارگاه‌ها و سمینارهای آموزشی برای انتقال دانش فنی و ارتقای توانمندی کارکنان قضایی و انتظامی پیشنهاد می‌شود.

توصیه‌ها شامل موارد زیر می‌شود:

راهنمایی‌های اخلاقی: تدوین راهنمایی‌های جامع اخلاقی برای استفاده از فناوری‌های نوظهور در نیروهای انتظامی با پرداختن به مسائلی مانند حریم خصوصی، سوگیری و مسئولیت‌پذیری.

حریم خصوصی داده‌ها: اجرای اقدامات قوی حفاظت از داده‌ها برای حفاظت از اطلاعات حساس و اطمینان از انطباق با مقررات مربوط به حریم خصوصی.

رویکرد انسان‌محور: تلاش برای اجرای رویکردی انسان‌محور در پیاده‌سازی فناوری، تأکید بر اهمیت قضاوت انسانی و نظارت در فرآیندهای تصمیم‌گیری.

آموزش مداوم: ارائه آموزش مداوم به نیروهای انتظامی برای اطمینان از استفاده مؤثر و درک صحیح این فناوری‌ها.

همکاری: تقویت همکاری بین نهادهای انتظامی، شرکت‌های فناوری و دانشگاه‌ها برای تسهیل تبادل دانش و توسعه راه‌حل‌های نوآورانه.

مشارکت عمومی: تعامل با عموم مردم برای ایجاد اعتماد و شفافیت در استفاده از این فناوری‌ها، پرداختن به نگرانی‌های مربوط به نظارت و حریم خصوصی.

این تدابیر در کنار سیاست‌گذاری‌های کلان (مانند تخصیص بودجه برای تحقیق و توسعه فناوری در سازمان‌های انتظامی و تدوین استانداردهای الزامی امنیت اطلاعات) می‌تواند زمینه را برای استفاده مؤثر و مسئولانه از فناوری‌های نوین در صیانت پیش‌کنشی از کارکنان و مردم فراهم آورد.

## References

Afshani, A. R. G. (2020). Obstacles and Limitations of Effective Intervention of Police Staff in Dealing with Visible Crimes (Case Study of Fateb Eleventh Police Station). https://api.semanticscholar.org/CorpusID:226057696 [In Persian].

Aghaei, A., Jahedi, P., & Karami, H. (2020). The social construction of desirable behavior of police officers from the perspective of students. https://api.semanticscholar.org/CorpusID:226024940 [In Persian].

Alinejad, M. (1403). The Impact of Technology on Crime Prevention and Detection: Challenges and Opportunities. 10th International and National Conference on Management, Accounting and Law Studies. https://civilica.com/doc/2042286 [In Persian].

Arietti, R. (2024). Do real-time crime centers improve case clearance? An examination of Chicago's strategic decision support centers. Journal of Criminal Justice, 90, 102145. https://doi.org/10.1016/j.jcrimjus.2023.102145

Awasthi, L. S., Rai, A. K., Awasthi, K. S., Kumar, S., Bajpai, A. K., & Pathak, H. (2023). Cyber Crime Prevention Model Using Artificial Intelligence. Journal of Chemical Health Risks, 13(4s), Article 4s. https://doi.org/10.52783/jchr.v13.i4s.1660

Bag, A., Roy, S., & Pandey, A. (2024). Harnessing the Power of Artificial Intelligence in Law Enforcement: A Comprehensive Review of Opportunities and Ethical Challenges. In A. Ara & A. Ara (Eds.), Advances in Computational Intelligence and Robotics (pp. 121–145). IGI Global. https://doi.org/10.4018/979-8-3693-1565-1.ch008

Barangi, H., Raji, F., & Khaseh, A. A. (2020). Analysis of Security and Privacy Research in the Field of Blockchain: A Scientometric Study. Journal of Soft Computing, undefined(undefined). https://civilica.com/doc/1487151 [In Persian].

Benito, R. C., & Tejera, Y. S. (2020). Experiencia internacional de la aplicación de la prevención situacional como estrategia para la reducción de los delitos. Boletín ONBC. Revista Abogacía, 64.

Cunningham, M. R., Jones, J. W., & Dreschler, B. W. (2018). Personnel risk management assessment for newly emerging forms of employee crimes. International Journal of Selection and Assessment, 26(1), 5–16. https://doi.org/10.1111/ijsa.12202

Dey, N., Hassanien, A. E., Bhatt, C., Ashour, A. S., & Satapathy, S. C. (2017). Internet of Things and Big Data Analytics Toward Next-Generation Intelligence. Springer International Publishing. https://books.google.com/books?id=2fwwDwAAQBAJ

Dharsan, R., Krishanthini, M., Traveena, C., Anubama, L., Hansika, M. M. D. J. T., & Chandrasiri, S. (2023). The Future of Crime Prevention: Police Case Analysis Using Machine Learning. 2023 5th International Conference on Advancements in Computing (ICAC), 454–459.

Dimovski, D., & Grujić, Z. (2024). Possibilities of using artificial intelligence in crime prevention. Bezbednost, Beograd. https://api.semanticscholar.org/CorpusID:271315276

Dlodlo, N., Mbecke, P., Mofolo, M. R. O., & Mhlanga, M. (2015). The Internet of Things in Community Safety and Crime Prevention for South Africa. https://api.semanticscholar.org/CorpusID:53139524

Douglas, S. (2021). The Effects of Body-Worn Cameras on Violent Police Victimization. Policing: A Journal of Policy and Practice, 15(2), 1399–1416. https://doi.org/10.1093/police/paaa032

Eck, J. E., & Clarke, R. V. (2019). Situational Crime Prevention: Theory, Practice and Evidence. In M. D. Krohn, N. Hendrix, G. Penly Hall, & A. J. Lizotte (Eds.), Handbook on Crime and Deviance (pp. 355–376). Springer International Publishing. https://doi.org/10.1007/978-3-030-20779-3_18

Emerging technologies. (2024). In Wikipedia. https://en.wikipedia.org/w/index.php?title=Emerging_technologies&oldid=1253844555#cite_note-1

Eran, M. S., & Hasranizam, H. (2024). The Effectiveness of Crime Prevention Using GIS Technology and CCTV Application for Smart City. In R. N. Yadava & M. U. Ujang (Eds.), Advances in Geoinformatics Technologies (pp. 59–75). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-50848-6_4

Fatih, T., & Bekir, C. (2015). POLICE USE OF TECHNOLOGY TO FIGHT AGAINST CRIME. European Scientific Journal, ESJ, 11. https://api.semanticscholar.org/CorpusID:54086329

Feltovic, M. (2024). Utilizing Blockchain Technology to Modernize Police Operations: Ensuring Security, Transparency, and Efficiency. Eximia, 13, 661–672. https://doi.org/10.47577/eximia.v13i1.493

Fomin, V., & Luk'janova, E. (2023). SOME ASPECTS OF THE ACTIVITIES OF THE INTERNAL AFFAIRS BODIES IN TRANSPORT TO COUNTERACT CRIMES COMMITTED USING INFORMATION AND TELECOMMUNICATION TECHNOLOGIES. Man: Crime and Punishment. https://api.semanticscholar.org/CorpusID:268863613

Gazinejad, S., Darvish, H., & Mahmoudi Meymand, M. (2024). Designing a Futures Model of Bank Employees' Attitudes Regarding Job Security in the Face of Blockchain in the Horizon of 2031. Asset Management and Financing, 12(3), 1–22. https://doi.org/10.22108/amf.2024.139968.1844 [In Persian].

Ghajari, somaye. 2025. "The Impact of Blockchain Technology on Administrative Processes with emphasised on Enhancing Transparency, Efficiency, and Trust." New Approaches in Public Administration (1):88–109. doi:10.71815/jnapa.2025.1194698 [In Persian].

Hassanvand, A., Rahmati, D., & Abedi, Y. (2014). Factors affecting the commission of financial crimes by NAJA employees and strategies to combat them. NAJA Human Resources Quarterly, 15(64), 9–32 [In Persian].

Hendrix, J. A., Taniguchi, T., Strom, K. J., Aagaard, B., & Johnson, N. (2019). Strategic policing philosophy and the acquisition of technology: Findings from a nationally representative survey of law enforcement. Policing and Society, 29(6), 727–743. https://doi.org/10.1080/10439463.2017.1322966

Iansiti, M., & Lakhani, K. R. (2017). The Truth About Blockchain. Harvard Business Review. https://hbr.org/2017/01/the-truth-about-blockchain

Idy, M. Y. (2022). Law Enforcement Against Members of The Indonesian National Police Commit Crimes. Substantive Justice International Journal of Law. https://api.semanticscholar.org/CorpusID:253059791

Jeon, J., & Jeong, S. R. (2016). Designing a Crime-Prevention System by Converging Big Data and IoT. https://api.semanticscholar.org/CorpusID:114435867

Johnson, S. D. (2024). Identifying and preventing future forms of crimes using situational crime prevention. Security Journal, 37(3), 515–534. https://doi.org/10.1057/s41284-024-00441-5

Jones, H. D. (2016). Body-worn cameras are the cure for the curse of official police misconduct and unlawful use of force complaints.

Kabiru, H. S., Jika, A. J., & Mishra, R. (2024). Company Crime Tracking System Using Blockchain. 2024 2nd International Conference on Disruptive Technologies (ICDT), 1434–1438. https://doi.org/10.1109/ICDT61202.2024.10489118

Kahla, L. Z. (2024). Leveraging Artificial Intelligence for Crime Detection and Prevention. INTERANTIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT, 08(05), 1–5. https://doi.org/10.55041/IJSREM34207

Kesarkar, T. (2024). Blockchain Technology in Law Enforcement and Security: Overview. International Journal for Research in Applied Science and Engineering Technology. https://api.semanticscholar.org/CorpusID:270810085

Kobets, P. (2024). The causal complex of the emergence of criminal risks caused by the use of artificial intelligence technologies and preventive measures to prevent them. Юридическая Наука и Практика. https://doi.org/doi: 10.36511/2078-5356-2024-1-80-85

Kot, P. (2021). Psychosocial Aspects of Employee Control with the Use of Modern Technologies. Journal for Perspectives of Economic Political and Social Integration. https://api.semanticscholar.org/CorpusID:247309589

Krezi, A. A., Ahmari, H., & Galvardi, M. K. (2021). Prevention of specific military and police crimes in Iranian criminal policy. https://api.semanticscholar.org/CorpusID:238737817 [In Persian].

Lemos, M. H., & Minzner, M. (2014). For-Profit Public Enforcement. Harvard Law Review.

Lunhol, O., & Torhalo, P. (2024). Artificial Intelligence in Law Enforcement: Current State and Development Prospects. Socratic Lectures 10 - Part II, 120–124. https://doi.org/10.55295/PSL.2024.II12

Mastrobuoni, G. (2020). Crime is Terribly Revealing: Information Technology and Police Productivity. The Review of Economic Studies, 87, 2727–2753. https://doi.org/10.1093/restud/rdaa009

Matlala Ramolobi L.G. (2018). Defining e-policing and smart policing for law enforcement agencies in Gauteng Province. Acta Criminologica : African Journal of Criminology & Victimology, 31(1), 136–148. https://doi.org/10.10520/EJC-11c62342cd

Mena, J. (2011). Machine Learning Forensics for Law Enforcement, Security, and Intelligence. Auerbach Publications. https://doi.org/10.1201/b11026

Milidragovic, D., & Milić, N. (2024). Implementation of body cameras worn by police officers in police organizations: Real need or necessary solution. Bezbednost, Beograd. https://api.semanticscholar.org/CorpusID:268435497

Mokhtari, H., & Jalali, S. (2024). The impact of information and communication technology (ICT) and digital data on crime control and prevention in police stations. Digital and Smart Library Research, 11(No. 2 (41)), 13–28. https://doi.org/10.30473/mrs.2024.71441.1595 [In Persian].

Mousavi, P., Salehan, A., & Yousefi-Zanouz, R. (2022). Identifying and reviewing research areas and trends in blockchain technology. Smart Business Management Studies, 10(39), 127–162. https://doi.org/10.22054/ims.2021.64182.2074 [In Persian].

Naylor, R. (2003). TOWARDS A GENERAL THEORY OF PROFIT-DRIVEN CRIMES. British Journal of Criminology, 43, 81–101.

Ninoria, S., Upadhyay, R., Philip, R. S., Dwivedi, R., Micheal, G., Gupta, A., & Mishra, S. (2023). AI and Crime Prevention With Image and Video Analytics Using IoT: In B. K. Pandey, D. Pandey, R. Anand, D. S. Mane, & V. K. Nassa (Eds.), Advances in Computational Intelligence and Robotics (pp. 96–115). IGI Global. https://doi.org/10.4018/978-1-6684-8618-4.ch007

Patel, D., Sanghvi, H., Jadav, N. K., Gupta, R., Tanwar, S., Florea, B. C., Taralunga, D. D., Altameem, A., Altameem, T., & Sharma, R. (2022). BlockCrime: Blockchain and Deep

Learning-Based Collaborative Intelligence Framework to Detect Malicious Activities for Public Safety. Mathematics, 10(17), 3195. https://doi.org/10.3390/math10173195

Peterson, B. E., & Lawrence, D. S. (2019). Body cameras and policing. Oxford Research Encyclopedia of Criminology and Criminal Justice.

Poya, M. Sh., Malmir, M., & Shadmanfar, M. R. (2020). Iran's Criminal Policy Towards Crimes of Government Employees. https://api.semanticscholar.org/CorpusID:240499858 [In Persian].

Rahimi, A., & Abbasi Rostami, N. (2021). Investigating the relationship between emotional workforce strategies and employees' off-duty behaviors. Military Sciences and Technologies, 16(54), 99–118. https://doi.org/10.22034/qjmst.2021.243873 [In Persian].

Rai, T. S. (2019). Body cameras and police misconduct. Science, 365(6450), 246.5-247. https://doi.org/10.1126/science.365.6450.246-e

Rajabi Taj Amir, A., Abdollahi, S., & Shoaei, M. (2022). The role of information exchange management in the process of preventing cybercrime. Information Management Sciences and Technologies, 8(1), 427–450. https://doi.org/10.22091/stim.2022.7572.1690 [In Persian].

Rotolo, D., Hicks, D., & Martin, B. R. (2015). What is an emerging technology? Research Policy, 44(10), 1827–1843. https://doi.org/10.1016/j.respol.2015.06.006

Rukinov, M. (2020, December 19). Opportunities for blockchain in police investigations. Cointelegraph. https://cointelegraph.com/news/opportunities-for-blockchain-in-police-investigations

Russell, S. J., & Norvig, P. (2016). Artificial intelligence: A modern approach. Pearson.

Amirabbas Sadeghian. (2025). Artificial Intelligence in Governance and the Governance of Artificial Intelligence. New Approaches in Public Administration, 1, 1–36. https://doi.org/10.71815/jnapa.2025.1200094

Saini, H. K., Kussum, & Mandeep. (2023). Artificial Intelligence and Internet of Things: A Boon for the Crime Prevention. 2023 International Conference on Advances in Computation, Communication and Information Technology (ICAICCIT), 7–11.

Sardana, D., Marwaha, S., & Bhatnagar, R. (2021). Supervised and Unsupervised Machine Learning Methodologies for Crime Pattern Analysis. International Journal of Artificial Intelligence & Applications. https://api.semanticscholar.org/CorpusID:234089169

Shahaab, A., Hewage, C., & Khan, I. (2021). Preventing spoliation of evidence with blockchain: A perspective from South Asia. 45–52.

Shama, N. (2017). A machine learning approach to predict crime using time and location data. https://api.semanticscholar.org/CorpusID:113942997

Sharifi, M. (2020). Personality typology of illegal employees and presenting a clustering model and predicting their violations using data mining. https://api.semanticscholar.org/CorpusID:226167077 [In Persian].

Sharma, A., Yaduvanshi, E., Sharma, A., & Saha, P. (2024). Mitigating SAD States and Maladaptive Coping in Law Enforcement: Enhance Emotional Competence. International Journal of Experimental Research and Review, 40, 132–141. https://doi.org/10.52756/ijerr.2024.v40spl.010

Singh, R., & Ramdeo, S. (2023). Employee Motivation in a Changing Environment. In R. Singh & S. Ramdeo (Eds.), Contemporary Perspectives in Human Resource Management and Organizational Behavior: Research Overviews and Gaps to Advance Interrelated

Fields (pp. 191–208). Springer International Publishing. https://doi.org/10.1007/978-3-031-30225-1_11

Stinson, P. M. (2015). Police Crime: The Criminal Behavior of Sworn Law Enforcement Officers. Sociology Compass, 9, 1–13.

Stinson, P. M., Liederbach, J., Buerger, M., & Brewer, S. L. (2018). To protect and collect: A nationwide study of profit-motivated police crime. Criminal Justice Studies, 31, 310–331.

Stinson, P. M., Liederbach, J., Lab, S. P., & Brewer, S. L. (2016). Police Integrity Lost: A Study of Law Enforcement Officers Arrested. https://api.semanticscholar.org/CorpusID:112648472

Stones, E., & Tilley, N. (2022). Situational Crime Prevention. In Encyclopedia of Violence, Peace, & Conflict (pp. 404–412). Elsevier. https://doi.org/10.1016/B978-0-12-820195-4.00291-0

Sukhodolov, A. P., & Bychkova, A. M. (2018). Artificial Intelligence in Crime Counteraction, Prediction, Prevention and Evolution. Всероссийский Криминологический Журнал. https://api.semanticscholar.org/CorpusID:192661875

Talob, A. R., & Asgari, H. (2021). The Relationship Between Key Economic Variables and Crime: A Markov-Switching Approach. https://api.semanticscholar.org/CorpusID:238153672 [In Persian].

Tasnim, M. A., Omar, A. A., Rahman, M. S., & Bhuiyan, M. Z. A. (2018). CRAB: Blockchain Based Criminal Record Management System. International Conference on Security, Privacy, and Anonymity in Computation, Communication, and Storage. https://api.semanticscholar.org/CorpusID:54461198

Tsvyk, V. A., & Tsvyk, I. V. (2023). Personal information security as a social problem. RUDN Journal of Sociology. https://api.semanticscholar.org/CorpusID:264139194

Tulinov, V. S., Bilykh, I., Merdova, O., Volobuieva, O., & Veselov, M. (2022). Activities of Law Enforcement Agencies in the Context of the Introduction of Innovative Technologies (Comparative Legal Aspect). Cuestiones Políticas. https://api.semanticscholar.org/CorpusID:247689972

Vafaei, Amir, Karamollah Daneshfard, and Morteza Mousakhani. 2025. "Developing a Model for Monitoring the Effectiveness of Public Policies in the Banking System in the Digital Age." New Approaches in Public Administration (1):92–116. doi:10.71815/2025/JNAPA.1204102.XML [In Persian].

Zhadan, D. O., Mordvyntsev, M., & Pashniev, D. V. (2024). Tracking illegal activities using video surveillance systems: A review of the current state of research. Law and Safety. https://api.semanticscholar.org/CorpusID:269181013

Kolodyazhny (Колодяжний), M. Г. (2020). Application of modern technologies in the field of crime prevention. Herald of the Association of Criminal Law of Ukraine. https://api.semanticscholar.org/CorpusID:230679192