JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

ARTIFICIAL INTELLIGENCE: CRIME BEYOND IMAGINATION

Guide: Dr. Niti Nipuna Saxena
Author: Geeta Prajapati
Student of Sage University, Indore
Institute of law and legal studies

Abstract

"*The next world war be a code war instead of a cold war"*. 21st century's most revolutionary technologies, artificial intelligence (AI) has permeated every aspect of daily life and numerous sectors, including healthcare and finance. Although AI offers enormous advantages, its potential for abuse by criminals has created new and sophisticated threats that are frequently referred to as *"crime beyond imagination"* since they put current legal and investigative frameworks to the test. AI makes this issue crucial, although it provides strong tools for law enforcement, when abused it poses unbelievable risks to societal stability and international security. AI is a double -edged sword when it comes to crime it makes it possible for new, complex forms of crime, but it also gives security and law enforcement strong tools and easy solutions to identify, stop and look into illegal behavior. AI has a wide range of applications in the context of crime, including both the use of AI by law enforcement for investigative purposes and its use by criminals for new and improved types of illegal activities. Increasing worries that previously unthinkable new and sophisticated forms of criminal conduct are being made possible by artificial intelligence. Law enforcement is facing serious issues as AI lowers the cost to entry for criminals and increases the scope and sophistication of attacks. AI is a power full tool that criminals are quickly using to commit large-scale crimes while also giving law enforcement previously un heard of capabilities for crime investigation and prevention. Most jurisdictions, including India, currently lack explicit, dedicated legislation to oversee crimes related to AI. Rather, current legislation is being modified to deal with AI abuse, mainly by concentrating on the human creators, operators, or users involved, The Information Technology (IT) Act of 2000, Bharatiya Nyaya Sanhita of 2023, and The Digital Personal Data Protection Act (DPDP) of 2023 are jus a few of the statutes that are used by main legal requirements.

Keywords: Artificial, Intelligence, Sophisticated, Digital.

Introduction

The contemporary period has seen a rise in the complexity of crime, as new forms and methods of criminal behavior have emerged due to the rapid improvements in communication, technology, and social structures. Even though they are crucial, traditional law enforcement methods frequently fails to handle these changing issues. These constraints have brought attention to the need for creative solutions that may effectively and proactively combat crime. Artificial intelligence has the potential to significantly increase the frequency of criminal activity. In order to determine if India's current legal framework is sufficient to combat cybercrime in the context of AI technology, this research will assess the usage and abuse of AI in connection to cybercrimes. *"I dream of a Digital India where cyber security becomes an integral part of our national security"* by Prime Minister Narendra Modi. Over 86% of households are now connected to the interest. Cybersecurity incidents in India rose from 10.29 lakh in 2022 to 22.68 lakh in 2024.[1] With predictive policing, investigate the revolutionary potential of AI in law enforcement. It proactively prevents crime by using AI algorithms to analyze massive amounts of data for real -time insights and hotspot identification.

[1] Curbing cyber frauds in digital India, Press Note Department, Oct 08 2025 12:01 pm https://www.Pib.gov.in/PressNoteDetails.aspx?NoteId=155384&ModuleId=3&reg=3&lang=2.

Objective decision-making and resource efficiency are benefits. In order to adopt AI responsibly and create safer communities, ethical issues must be addressed. Discover the future of crime prevention with predictive policing driven by AI. The purpose of this study is to analyze the perceived roles, difficulties, and coping strategies associated with development of AI in law enforcement across the globe, which is rapidly undergoing digital changes. The government approach to tackle cybercrime the "Cyber Swachhta Kendra" (Botnet Cleaning and Malware Analysis Centre), Sanchar Saathi (for blocking lost phones/reporting fraud), National Cybercrime Reporting Portal (NCRP) for complaints, and Cyber Commandos for specialized law enforcement. Government made infrastructure & coordination units CEIR (Central Equipment Identity Register), NCCC (National Cyber Coordination Centre), CFMC Cyber Fraud Mitigation Centre and Samana Vay platform. Multimodal generation this could allow criminals to produce synthetic content for deception and impersonation, including in settings involving dynamic interaction with a victim. Advanced planning and reasoning: which can be combined with web search to help design and adapt sophisticated attack strategies. AI Agents: AI systems which can take actions on their own may enable persistent large-scale criminal activity without the need for human oversight or intervention. In addition to these capabilities, widespread consumer market adoption could create new attack surfaces and reduce barriers to criminal use. For example, companies are using compression techniques to develop (and sometimes open source) models that are small enough to be run on lightweight devices like smartphones. As these consumer applications continue to grow, it is likely that criminal exploitation will grow too. Our approach, Broadly, we split our work into three areas: risk modelling, technical research, and interventions to address these challenges.[2]

Artificial Intelligence: Challenges Combating Crime

Law enforcement is changing from a reactive to a proactive paradigm thanks to artificial intelligence (AI), which provides strong tools to fight crime while starting a "arms race" against criminals utilizing similar technologies. In order to improve public safety, AI is being used for financial crime detection, real-time surveillance, and predictive policing.

Legal system

- **Liability and Accountability:** Such as biased algorithmic decisions or failed robotic surgeries can happen. But assigning liability is complex, involving developers, manufacturers, users, and sometimes third-party data providers.
- **Data privacy and Security:** AI system often require large datasets for training, raising concerns about personal data privacy and misuse.
- **Ethical Concerns and Algorithmic Bias:** Algorithmic bias can lead to discrimination in hiring, lending, legal judgements, and more. The lack of transparency is Black box problem.
- **Intellectual Property (IP) and Deepfakes:** Like Indian Copyright Act is struggling to keep pace, and legal reform is underway to update definitions and enforcement mechanisms.[3]

Advanced Technology

- **Low Accuracy in Real-World Situation:** Low quality CCTV footage frequently causes facial recognition System (FRT) in India to have significant false-positive rates.
- **Black Box Problem:** Due to the lack of transparency in many AI system police officers find it challenging to explain how a machine reached a particular conclusion, which poses problems for trail evidentiary standards.
- **Language and Context Barriers:** When assessing social media for risks, NLP (Natural Language Processing) technologies are less successful since they frequently miss regional language, dialects and slang.

Police Training

- **Infrastructure and Resources:** Many police academies, excepting Sardar Vallabhbhai National Police Academy, Hyderabad which trains Indian Police Service (IPS) officers, face significant challenges due to inadequate training facilities, which often include limited classroom space, uncomfortable dormitory accommodations, and outdated technological resources. This lack of modern equipment hampers the training effectiveness, leaving recruits ill-equipped for contemporary policing demands. Additionally, insufficient funding restricts access to essential training materials

[2] How will AI enable the crimes of the future, AI Security Institute, Jul 3,2025 https://www.aisi.gov.uk/blog/how-will-ai-enable#:~:text=This%20could%20allow%20%criminals520to,Risk%20Modelling.

[3] Legal challenges of Artificial Intelligence in India, CSIA Law Associates, Aug 18, 2025 https://csialawassociates.co.in/know-your-law/f/legal-challenges-of-artificial-intelligence-in-india

and professional trainers, further compromising the quality of education. Variability in training standards across different states and regions exacerbates the issue, creating inconsistent preparedness among officers nationwide.

- **Curriculum and Training Methods:** Many training programmes utilize outdated curricula that overlook pressing contemporary issues like crowd control, handling sectarian and communal violence, cybercrime, crypto crime, and terrorism, hindering law enforcement's effectiveness. There's insufficient emphasis on community policing, cultural sensitivity, and human rights, which are crucial for building trust with communities. Additionally, these programmes often fail to incorporate the latest technology, leaving officers unprepared for tech-driven crimes, and neglect mental health training, vital for managing stress and supporting those in crises. Practical scenario-based exercises are often missing, and disaster management training is inadequate. Lastly, a limited focus on forensic science can undermine officers' investigative capabilities. Hence, a comprehensive upgrade is essential.
- **Recruitment and Selection Process:** The recruitment process at many places suffers from inefficiencies and potential corruption, resulting in the selection of less qualified candidates, which diminishes workforce effectiveness. Additionally, varying training syllabus across the country lead to performance issues, while insufficient psychological training leaves officers unprepared for stress, impacting their well-being and job performance. Gender bias in recruitment practices further underrepresents women and fosters discrimination, undermining diversity. Lastly, training often emphasizes technical skills over essential soft skills like communication and conflict resolution, limiting recruit success in collaborative, real-world scenarios. Addressing these issues is vital for a more effective and equitable police force.[4]

People Awareness

- **Inadequate Informed Consent:** Individuals’ right to privacy is frequently violated when surveillance occurs in public areas without their knowledge or consent.
- **Fatigue with consent and digital illiteracy:** A large percentage of people in less educated areas are ignorant of how their data is gathered or utilized due to widespread digital surveillance and complicated, frequently English-based consent forms.
- **Absence of Transparency:** The public’s trust in AI surveillance systems is diminished by the absence of public disclosure about the types of data that are gathered, why they are collected, and how long they are kept.

Artificial Intelligence Advantages to Control Crime in India

India’s law enforcement is changing from a reactive to a proactive paradigm thanks to artificial intelligence (AI), which offers major benefits in terms of resource allocation, crime prevention, and investigative effectiveness. Predictive policing, facial recognition, and the investigation of large, dispersed datasets are important applications.

Legal Framework

- **AI in FIR Filing and Judicial Proceeding:** AI-driven speech-to-text tools assist in real time FIR filing and case documentation. AI is improving witness testimony analysis and courtroom evidence evaluation.
- **Data-Driven Crime Tracking and Intelligence System:** AI enhances Crime and Criminal Tracking Network Systems (CCTNS). Integration with e-prisons and e-Forensics databases.
- **Predictive policing:** AI models analyze crime patterns, high-risk areas, and criminal behavior enabling law enforcement to take proactive measures.[5]

[4] Md. Imran Wahab, Police Training in India: Navigating the Challenges and Forging the Future, legal service India, https://www.legalserviceindia.com/legal/article-19065-police-training-in-india-navigating-the-challenges-and-forging-the-future.html

[5] Digital Transformation of Justice: Integrating AI in India’s Judiciary and Law Enforcement, Ministry of Law and Justice, Feb 25, 2025 8;22PM https://www.pib.gov.in/PressReleasePage.aspx?PRID=2106239&reg=3&lang=2#:~:text=Conclusion-,Artificial%20Intelligence%20is%20%transforming%20India’s%20judiciary%20and%20law%209enforcement%20by,and%20transparent%20for%20all%20citizens.

Technology Tools

- **Using Predictive Policing:** To find “hot spots,” AI systems examine past crime statistics, meteorological trends, and geographic information.
- **Social Media surveillance:** To identify potential terrorist activities, illegal internet marketplaces, and security risks, digital forensic tools can examine social media.
- **(ALPR) Automatic license Plate Readers:** These devices identify stolen cars or suspects in criminal investigations by scanning and recording license plates.

Effective Police Force

- There are many different ways that AI can be used in policing strategies. One way is through predictive policing. Predictive policing uses data and analytics to predict where and when a crime is likely to occur. This information can then be used by police officers to prevent crimes from happening in the first place.[6]
- Officers can swiftly sift through hours of CCTV footage to identify suspects or missing people thanks to training in AI-powered face recognition (FRT) and video analytics.
- AI training shortens the period between a crime and identification of a suspect by enhancing the speed at which police can evaluate vast volumes of data.

Literate people

- By encouraging proactive community engagement, building trust, and simplifying the adoption of preventive solutions, public knowledge of artificial intelligence (AI) serves as a force multiplier in the fight against crime.
- People may better defend themselves, report suspicious activities more successfully, and assist law enforcement in implementing security measures rather than opposing them when they are aware of how AI tools operate.
- Increase Cybersecurity Awareness: Raising public awareness reduces the likelihood of AI-driven crimes like phishing and deepfake frauds. People can “Think before they act,” preventing financial crime, by being aware that scammers can imitate voices or faces.
- By educating the public about the repercussions of disseminating false threats or unintentionally participating in cybercrime, awareness efforts like “Think Before you Post” lessen the strain on police resources and stop crime from getting worse.

Government Tool to Detect Crime

The National Cyber Crime Reporting Portal (NCRP) cybercrime.gov.in, which is run by the Indian Cybercrime Coordination Centre (ICCC) of the Ministry of Home Affairs (MHA), is India’s main government platform for identifying and reporting cybercrime. It enables citizens to report a variety of cybercrime, particularly those that target women and children, and provides resources for financial fraud reporting (155260) and cybersecurity awareness. The Cyber Swachhta Kendra, which offers free security tools, and the Sanchar Saathi portal, which reports fraudulent communications, are two other important projects.

Key Platforms and Initiatives:

- National Cyber Crime Reporting Portal (NCRP)

Purpose: Is to provide a single location for citizens to report online fraud, identify theft, hacking, and cyberbullying.

Features: Include the ability to file complaints online, add evidence track cases, and provide cyber safety advice.

Focus: Special measures for offences against women and children are the main focus.[7]

- Indian Cybercrime Coordination Centre (I4C)

Role: The main point of contract for law enforcement agencies (LEAs) to coordinate cybercrime investigations.

Services: Offers a framework for handling cyber threats and oversees the NCRP.[8]

[6] Iron Yun, How AI Can Improve Local Policing Strategies, VAIDIO, Feb 14,2024 https://www.vaidio.ai/blog/how-ai-can-improve-local-policing-strategies#:~:text=There%20are%20many%20different%20ways,happening%20in%20the%20first%20place

[7] Ministry of Home Affairs, National Cyber Crime Reporting Portal, https://cybercrime.gov.in/webform/Accept.aspx

[8] Ministry of home affairs, Indian Cybercrime Coordination Centre (I4C), https://i4c.mha.gov.in/ncrp.aspx

- Citizen Financial Cyber Fraud Reporting System

Role: As a vital conduit in India, allowing people to promptly report financial cybercrimes (such as phishing and internet scams).
Services: Report online financial fraud at the national cybercrime helpline number1930.[9]

- Sanchar Saathi Portal

Role: Enables reporting suspected fraudulent communications (spam/scam) so that telecom authorities can take appropriate action.
Services: The Department of telecommunications (DoT), Government of India, created a mobile application to boost security, empower mobile users, and fight telecom-related fraud.[10]

- Cyber Swachhta Kendra

Role: Plays a vital role in establishing a secure digital India by identifying botnet infections, alerting users, offering free tools (such as bot removal software) and instruction to clean infected devices, collaborating with ISPs and antivirus companies to secure systems and encourage cyber hygiene under the MeitY's Digital India initiative.
Service: Provides India's Malware Analysis Centre and Botnet Cleaning.[11]

Discussion

The use of artificial intelligence (AI) into criminal activities is quickly transitioning from a theoretical worry to a practical, high-stakes reality. AI-enabled crime (AIC) takes advantages of machine learning's speed, scalability, and intelligence to automate, scale and enhance illicit behaviors, posing previously unimaginable threats. Despite the popularity of the "autonomous malicious agent" story, fraudsters can also pose as CEOs or family members to approve large-scale fraudulent transactions. "Dark LLMs" and Automated Malware jailbroken Large Language Models (LLMs) are being used by criminals to produce sophisticated malware, phishing emails, and scam script. They frequently get beyond safety controls to produce "uncensored" tools. Businesses, society, and law enforcement will all be significantly and immediately impacted by the use of these AI tools AI's independent behavior undermines legal liability by obfuscating accountability. The "black box" nature of AI makes it challenging to track how a decision was reached, making it challenging to assign blame to the developer, the user, or the AI itself. Overcoming Conventional Security Adaptive AI malware, which modifies its behavior to evade detection, is beyond the reach of traditional cybersecurity (signature-based detection). Indeed, the consequence are significant and are already being felt Loss of Trust in Media the widespread use of deepfakes is undermining public confidence in digital media, which makes it more difficult for judges to accept video evidence. The "Arms race" in cybersecurity refers to the ongoing, intensifying conflict between automated attackers and defenders as security corporations are compelled to use AI to combat AI. In order to combat this, experts stress the necessity of "glass box" interpretable AI, stringent regulatory frameworks, and AI-driven defense systems to keep up with these changing dangers.

Conclusion

Artificial intelligence (AI) is ushering in a new era of criminality that defines conventional wisdom, transitioning from human-driven behaviors to automated, hyper-sophisticated, and autonomous threats. While AI is an effective tool for law enforcement, its potential for abuse ranges from "crime-as-a-service" platforms and AI-authored fake news to the weaponization of autonomous drones and vehicles. The incorporation of Artificial intelligence (AI) into the judiciary marks a watershed moment, expanding beyond traditional legal processes to combat "crimes beyond imagination," such as complex cybercrimes, deepfakes, and AI-enabled fraud. This transformation needs a new judicial approach that combines technical adoption with ethical monitoring, as discussed at the planned 2026 national Conference on "Reimagining Crime and Criminal Justice System in the era of AI & ML. Artificial intelligence is transitionally moving from a reactive investigative tool to a proactive force in crime prevention, with future applications aimed at combating crime through predictive analytics, autonomous surveillance, and enhanced digital forensics, While AI is increasingly being used to detect fraud and identify criminals, its true promise lies in "anticipating" crimes before they occur.

[9] Ministry of home affairs, National Cyber Crime Reporting Portal, https://cybercrime.gov.in/webform/Crime_NodalGrivanceList.aspx

[10] Ministry of Communications, Department of Telecommunications, http://sancharsaathi.gov.in/sfc/

[11] Ministry of Electronics and Information Technology Government of India, Cyber Swachhta Kendra http://www.csk.gov.in/