Integrating Artificial Intelligence into Cybercrime Investigation: Challenges and Future Directions

Yogita Gautam[1], Dr. Renu[2]

[1]LL.M. (Master of Laws), University Institute of Legal Studies, Chandigarh University, Mohali (Punjab)
[2]Professor, University Institute of Legal Studies, Chandigarh University, Mohali (Punjab)

Abstract

Computer and social networking whereby criminals use the Internet to propagate criminal activities are some of the major challenges faced by existing policing strategies. Modern-day crimes include hacking into computer systems and stealing money from consumers, ransomware, identity theft cases, and hacking, all of which use the dark web and encryption. In this regard, artificial intelligence (AI) is the most efficient solution for improving the manner of cybercrime investigation. This paper also analyses how AI technologies such as machine learning natural language processing, and deep learning can be incorporated in cybercrime investigations and how they can assist in dealing with difficulties concerning data volume, complexity, and encryption. The advantages of utilizing AI are numerous from pattern recognition to repetitive tasks cutting down the investigation time. However, the paper recognizes that applying AI in business brings legal, technical, and ethical concerns including; privacy, bias, and legal constrictions. This research analyses existing legal frameworks of India, the EU, and the United States while looking at how it would be possible to incorporate AI into cybercrime investigations without violating the rights of a citizen. Further, it reveals infringement and possible bias, as well as unlawful use for violations, and recounts drawbacks related to the lack of resources and expertise that police departments confront. In the final section of the paper, directions for future research focusing on the use of AI in the fight against cybercrime are given in addition to that, the practice of cooperation with different countries, legal regulation of such activities, protection of ethical issues, and training of personnel are described. They are useful in making sure that the levels of artificial intelligence benefits are achieved fully without compromising security and the basic rights of an individual.

Keywords: Artificial Intelligence, Cybercrime Investigation, Cybercrime.

1. NTRODUCTION

Cybercrime has emerged and grown stiff through the enhancement of information technology and the enhanced popularity of the internet and this has facilitated crimes such as financial fraud and cyber theft, identity theft, ransomware attacks, hacking, and cyber espionage. These threats have advanced greatly in terms of their usage of the dark web, cryptocurrencies, and conjunction and mastering concealment mechanisms, which is why the traditional approach to law enforcement could not potentially chase them. Another strategy that has come to light in the process of supporting the performance of conventional police functions in the fight against cyber criminality is Artificial Intelligence (AI). Advanced AI technologies, including machine learning, natural language processing, and deep learning, can search datasets containing large volumes of information, identify outliers, and find patterns that may be hard even for detectives to notice. Therefore, to curb incidences of cybercrime and the procedures involved AI becomes a crucial tool in handling digital evidence, especially in cases where data is encrypted. The main research question in this study is, what are the issues of incorporating Artificial Intelligence in cybercriminal investigations in the future, especially within the Indian context? The usage of AI in such a domain has both benefits and risks including the following concerning the existing privacy laws[1] and due process rights as expressed by the seven-judge bench of the Supreme Court of India in the case of *Justice K.S. Puttaswamy (Retd.) v. Union of India*[2]. The involvement of AI in cybercrime investigation, issues associated with its implementation, and ways to make its usage legal and ethical will be investigated. Thus, the current legal regimes in India, the US, and the EU will be compared to determine the current state of regulation alongside the implementation of AI without underestimating the fundamental rights.

2. UNDERSTANDING CYBER CRIMES AND INVESTIGATIVE NEEDS

Computer crime, or cybercrime, as it is more commonly known, is a criminal act that employs the computer or uses it as an object or goal. The increase in the use of technology has made cybercrimes expand into different categories and now offer different activities like hacking, identity theft, phishing, and ransomware. Virulent computer crimes, for example, hacking, entail breaking into computer systems to acquire, alter, or manipulate information. This form of cybercrime is therefore a real concern to people and organizations, as the *S.S. Lotus, France v. Turkey*[3] Showed that when an organization's data is hacked, it stands to lose a lot of money. Likewise, identity theft, which is a situation where somebody embezzles personal information like credit card details or social security details, is still a major concern for the police.

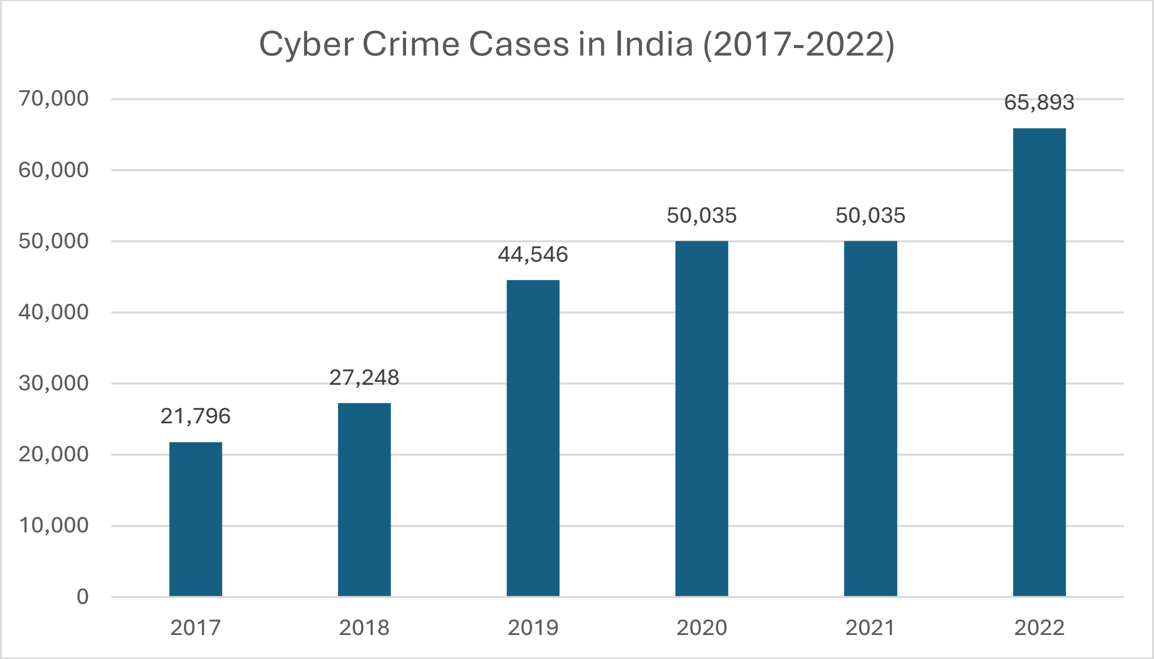


Fig 2: Year-wise Trend of Cyber Crime Cases in India (2017-2022)[4]

[1] Data Protection Laws in India, available at: https://blog.ipleaders.in/data-protection-laws-in-india-3/ (last visited on October 1, 2024).
[2] AIR 2017 SC 4161.
[3] 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7).
[4] Crime in India, available at: https://www.ncrb.gov.in/crime-in-india.html (last visited on October 1, 2024).

Phishing is also a very popular type of cybercrime, where attackers attempt to deceive individuals by accessing the personal and organizational information of a user through ordinary email or fake websites. Ransomware—malware that encrypts a victim's files and demands a ransom for the release of the files—is also on the rise. The most recent and large-scale manifestation of this type of cybercrime is described by the WannaCry ransomware attack in the year 2017, which impacted hundreds of thousands of organizations across the world, inclusive of healthcare services, making a clear manifestation of key infrastructure ill-prepared for this type of cyber threat.[5]

The range of possible cybercrimes is vast, and it requires a particular approach to investigation, mainly because of the different types of obfuscation used by the criminals. These crimes are mostly transnational, which poses problems in determining the accuracy of jurisdiction and common coordination between various agencies. In the process, traditional forms of detective work often fail to work because, as new technologies are developed, so are new strategies, schemes, and tactics by the wrongdoers. This has made it necessary to deploy newer forms of technology, such as artificial intelligence (AI), to handle the modern challenges of efficient cybercriminal investigations. [6].

3. CHALLENGES IN TRADITIONAL CYBERCRIME INVESTIGATION

The primary problem with traditional cybercrime investigation approaches is that they contain numerous difficulties, especially about the constantly growing number and level of complexity of cyber threats. Another drawback of using manual approaches for threat assessment is the impossibility of tracking rapid and multiple threats simultaneously. Due to the large amount of information that can be collected during a cybercrime investigation, including a fairly large amount of information from different sources, the analysis takes a lot of time, and it is practically impossible to be conducted by humans without using technical means. For instance, when analyzing the recent high-profile hacking case where investigators look for the source of the data leak, it might take weeks or even months to search through terabytes of data, which has a high probability of giving incorrect results.[7]

A second challenge is that there is no current protocol for retrieving and analyzing digital evidence. Digital data can be tampered with easily, and this is especially important for a prosecution where digital evidence forms the premise of the case. In addition, such heinous crimes know no bounds and are ever-evolving, creating a need for law enforcement agencies to adapt to effectively deal with the ever-evolving threats, a thing that the legal and procedural mechanisms are unable to do, hence the ineffectiveness of traditional investigation as a method of dealing with cybercrime. Section 65B of the Indian Evidence Act of 1872, which deals with electronic records, talks about proper procedures needed, and the procedure of handling the records still presents some challenges because where manual methods are used, they are not efficient and reliable.

The issue of ample volumes of data in law enforcement agencies is the second major challenge identified below. Criminal activities online include the examination of logs, metadata, encrypted communications, and other evidence forms that need technical prowess or tools to understand. In cross-border

[5] M. Satheesh Kumar, J. Ben-Othman, and K. G. Srinivasagan, "An Investigation on Wannacry Ransomware and its Detection," 33 *IEEE Symposium on Computers and Communications* 1-6 (2018).

[6] Cybercrime Investigation Tools and Techniques You Must Know!, available at: https://cybertalents.com/blog/cyber-crime-investigation (last visited on October 1, 2024).

[7] C. Horan and H. Saiedian, "Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions", 1 *Journal of Cybersecurity and Privacy* 580-596 (2021).

investigations, there are basic issues of jurisdiction and cooperation with other agencies, further compounding the difficulty of the process. Realizing the drawbacks of the conventional approaches and the growing complexity of the cyber threat landscape, different technological approaches have been considered more suitable for contemporary investigating practices, and AI is selected as one of the viable approaches to assist cybercrime investigators.

3.1 AI as a Solution for Cybercrime Investigation

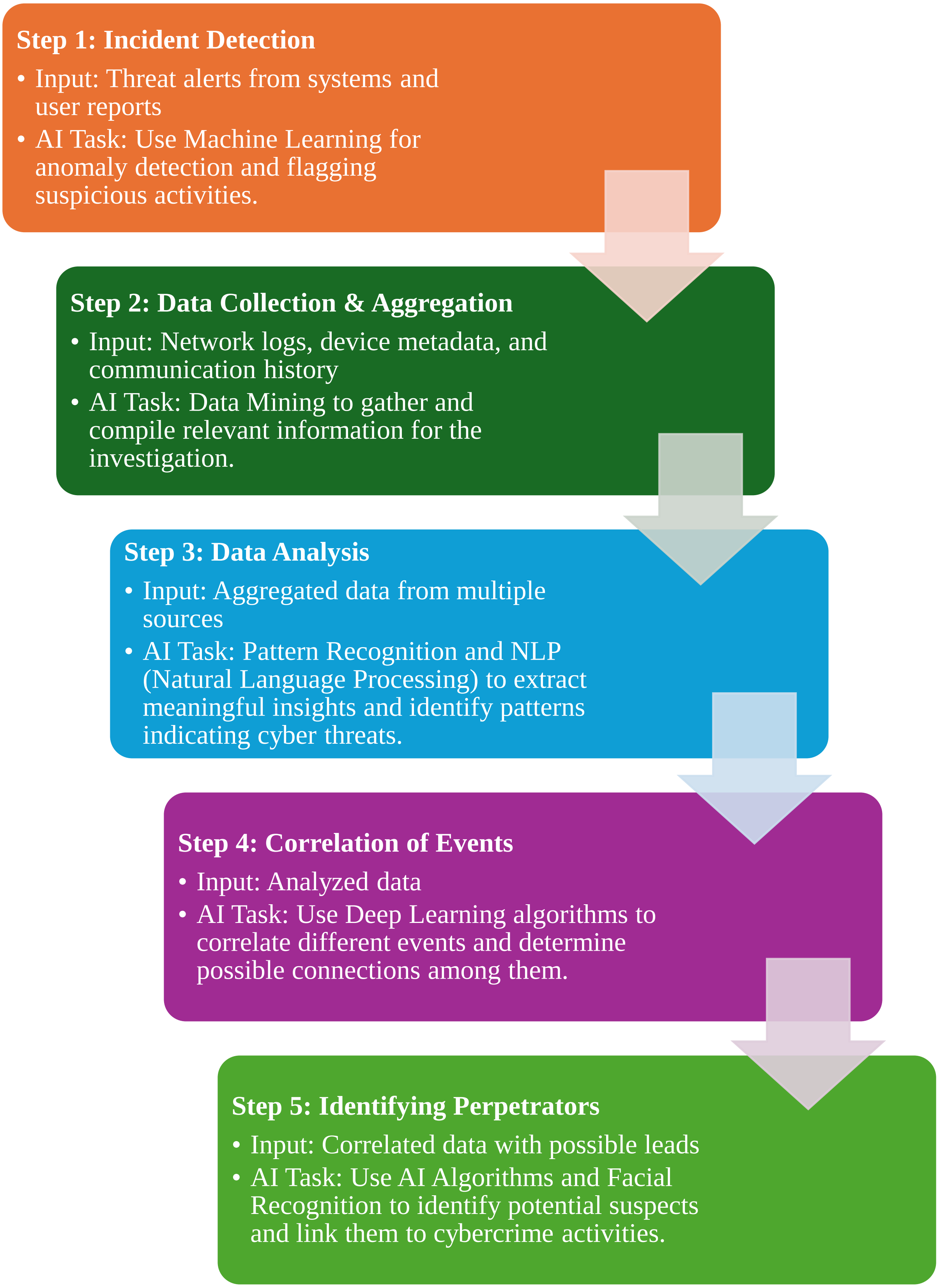
AI provides an effective approach to solving the issues encountered in ordinary cyberspace crime investigations. Thus, the strong and diverse areas of AI, which can include the analysis of large volumes of data as well as pattern recognition and automation capabilities, provide a revolutionary step change in how cybercrime may be identified and combatted. Where manual investigations fail due to the slow pace and possible inaccuracies that come with sifting through a myriad of papers, records, and electronic data, AI enhances investigations by making quick work of the same due to its capabilities to sort through and analyze large amounts of data in a relatively short period. Through the use of machine learning, large databases can be scanned, weaknesses detected, and possibly future threats assessed, thus enabling the investigators to concentrate on certain areas.[8]Pattern recognition is another important function carried out by artificial intelligence to identify cyber-crimes. AI systems can be taught to identify the manners of operation of known hackers, so once such hackers engage in similar activities in different networks and systems, they can be nabbed by law enforcement. For instance, it is possible to pick the phishing emails and analyze the linguistic feature or structure similarity of the email message before using it in an attack. These advanced features are further expanded by deep learning, a subfield of AI: the recognition of faces and voices, as well as chain connections linking various data containing the specifications of cybercriminals.[9]

Automation also has its contribution to improving the effectiveness of cybercrime investigations. Cognitive automation tools in AI can do simple, tedious work like scanning logs, obtaining digital evidence, and preparing reports, thus easing work for human investigators. This in turn makes it possible for police officers to focus on more core and constructive tasks in any investigation.[10]AI also plays a role in improving the aspects of digital investigation, which is an important factor in the collection of proofs in cybercrime-related court trials. Data may be either deleted, and forensic tools created using AI are capable of searching for it, encrypted, or encrypted in such a way that the AI-based instrument used in the cybercriminal's case is also capable of breaking the encryption. On the other hand, it is important that all use of AI is legal and has regard to relevant protected rights, such as the contemporary right to privacy.

[8] Ramanpreet Kaur, D. Gabrijelčič, and T. Klobučar, "Artificial intelligence for cybersecurity: Literature review and future research directions", 97 *Information Fusion* 101804 (2023).

[9] A. Shalaginov, I. Kotsiuba, and A. Iqbal, "Cybercrime Investigations in the Era of Smart Applications: Way Forward Through Big Data," 2019 *IEEE International Conference on Big Data* 4309-4314 (2019).

[10] Horan C, Saiedian H, "Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions", 1 *Journal of Cybersecurity and Privacy* 580-596 (2021).



Step 1: Incident Detection

- Input: Threat alerts from systems and user reports
- AI Task: Use Machine Learning for anomaly detection and flagging suspicious activities.

Step 2: Data Collection & Aggregation

- Input: Network logs, device metadata, and communication history
- AI Task: Data Mining to gather and compile relevant information for the investigation.

Step 3: Data Analysis

- Input: Aggregated data from multiple sources
- AI Task: Pattern Recognition and NLP (Natural Language Processing) to extract meaningful insights and identify patterns indicating cyber threats.

Step 4: Correlation of Events

- Input: Analyzed data
- AI Task: Use Deep Learning algorithms to correlate different events and determine possible connections among them.

Step 5: Identifying Perpetrators

- Input: Correlated data with possible leads
- AI Task: Use AI Algorithms and Facial Recognition to identify potential suspects and link them to cybercrime activities.

Fig 1. AI Integration in Cybercrime Investigation: A Step-by-Step Approach[11]

[11] L. S. Awasthi, A. K. Rai, K. S. Awasthi, S. Kumar, A. K. Bajpai, and H. Pathak, "Cyber Crime Prevention Model Using Artificial Intelligence", 13 *Journal of Chemical Health Risks* 814-822 (2023).

4. ROLE OF ARTIFICIAL INTELLIGENCE IN CYBER CRIME INVESTIGATION

AI can adopt different technologies in its process of supporting law enforcement agencies to fight cyber-crimes for the following reasons: Currently, one of the most used AI technologies in cyber investigations is machine learning. First, it is the ability to analyze huge amounts of data, identify already existing patterns, and learn new ones—an essential function for fighting cybercrime. These algorithms are capable of detecting anomalies, raising an alarm, or even outlining possible cyberattacks using prior data.[12]

Another important AI technology applied in cyber investigation is natural language processing (NLP). NLP is useful in making reflections and translations of textual communications, and that is how it can be used by investigators to decode messages from coded and distinct types and recognize disguised threats in communicated messages. They are particularly useful in surveillance of social media, email, and instant messengers for signs of a cybercriminal. For instance, in a phishing ring, NLPs were used to help the investigators make a discovery on the most used linguistic features in emails, hence leading to the arrest of the ring leaders. Another important nugget of AI is that the predictive analytics ability assists the law enforcement agency in avoiding cybercrimes. The relative analysis of trends and patterns in previous cyber-attacks is useful in the development of models of predicted future threats and possible countermeasures.

The subcategory of ML is known as deep learning and is used to make a model that can work for comprehending intricate representations such as images, audio, or video streams. This technology is helpful when it comes to some jobs, such as the identification of criminals (Hackers) through a camera or an image captured during an investigation, such as facial recognition. He also learned that deep learning models have powered efforts to crack codes used by criminals through an encryption system, something that has been used in cases of ransomware attacks in which AI makes it possible to identify the key encryption patterns. Altogether, these AI technologies form a set of tools that can be used effectively for a variety of tasks important for a law enforcement agency to effectively confront diverse and challenging aspects of modern computer crime investigation.

4.1 Applications of AI in Investigation

There is a myriad of ways in which AI is currently used in the context of cybercrime investigation, from malware detection to behavioral analysis and automated data mining. One of the main uses is the identification of viruses, with which hackers break into Internet resources and steal information. Traditional antivirus programs are not able to cope with the dynamic growth of malware while using behavior-based techniques, AI-based systems can react to new types of malware.

Another crucial area that can benefit from AI in the combating of cybercrime includes the identification of fraud. Scams and cyber theft on financial accounts have been on the rise, with the common ones being credit card fraud and identity theft, and through learning transaction patterns and tendencies of customers, AI can detect the fakes in real time. Using AI technology has become the norm in banks and other financial institutions since it can be used to recognize fraudulent transactions and alert the management before great loss occurs. Another crucial approach is based on behavioral analysis, the work of which is aimed at assessing user actions and applying the results to identify cyber threats. AI can easily detect anomalous trends, which, if unusual in normal usage, could be a sign of violation, thus allowing investigators to act quickly towards threats.[13]

[12] Selma Dilek, Hüseyin Çakır, and Mustafa Aydın, "Applications of Artificial Intelligence Techniques to Combating Cyber Crimes: A Review", 6 *International Journal of Artificial Intelligence & Applications* 1-19 (2015).

[13] B. Custers, "AI in Criminal Law: An Overview of AI Applications in Substantive and Procedural Criminal Law", in B.

Data mining is one of the most important applications of artificial intelligence, and this is an excellent feature for increasing the efficiency of the investigation of cybercrimes. The police require retrieving information from digital storage media, including mobile phones, computers, or servers, to prosecute individuals suspected of cybercrime. When the process is handled manually, it can at times be a tiresome and very time-consuming affair. Data mining using artificial intelligence makes it easy and fast to search through large data packages to look for evidence and sort the data into bins for further examination. For instance, in the arrest of a hacking group that specializes in attacking financial institutions, AI systems could be used to interpret data obtained from gadgets seized from the group members to unravel the communication threads and the core members of the group.[14]

5. LEGAL FRAMEWORK FOR AI IN CYBER CRIME INVESTIGATION

Technology advancements concerning artificial intelligence AI in cybercrime investigations reflect a research duality of AI applications and the laws that regulate them. National and global legal systems affecting data privacy place constraints on the use of AI in these investigations. At the international level, the EU's General Data Protection Regulation, or GDPR, acts as a reference regulation with strict conditions governing data processing, privacy, and consent, among others. GPDR continues to be a significant law for AI-driven cyber investigations with strict detail on the legal and authorized process to be followed when processing any personal data. According to the GDPR, DPIAs are required before implementing an artificial intelligence process on data, which are considered special categories of personal data, and this increases the accountability of law enforcement agencies utilizing artificial intelligence tools in combating cyber-crimes. This regulation acts as a model that has an impact on other legislation in other countries outside the EU.[15]

Another and especially relevant international instrument is the Budapest Convention on Cybercrime, or more officially, the Convention on Cybercrime is the first of its kind treaty designed on internet and computer crime by pulling together national laws, improving investigation tools, and increasing international cooperation. The Convention brings a focus to human rights and freedoms—again, when it comes to AI used in cyber investigations, privacy and other human rights have to be protected. While India has not ratified the Budapest Convention, it has displayed a positive approach towards accustoming the nation's laws to international standards, leaning specifically towards the Budapest Convention in areas of cybercrime and data protection.[16]

Nationally, the Digital Personal Data Protection Act, 2023 (DPDP Act) in India is for legal regulation of data protection[17]. This intends to control the handling of personal information by government and private players through setting standards in the collection, storage, and processing of data. The DPDP Act has consequences for the use of AI in the investigation of cybercrimes since police forces will be expected to guarantee compliance with data minimization and purpose limitation principles in the utilization of AI. It

Custers and E. Fosch-Villaronga (eds.), Law and Artificial Intelligence, Information Technology and Law Series, vol 35, T.M.C. Asser Press, The Hague, 2022.

[14] M. Abouzari, "Application of artificial intelligence in criminal investigations", 3 *ModernTechnologies Law* 1-13 (2022).

[15] Camouflage of AI in Cyber Crimes Vis-a-Vis Legal Issues and Challenges, available at: https://woxsen.edu.in/woxsen-law-review/wlr-papers/camouflage-of-AI-in-cyber-crimes-vis-a-vis-legal-issues-and-challenges/ (last visited on October 3, 2024).

[16] Ayşe Okutan and Yalçın Çebi, "A Framework for Cyber Crime Investigation", 158 *Procedia Computer Science* 287-294 (2019).

[17] India: Decrypting critical concepts under India's Digital Personal Data Protection Act, 2023 and comparison with GDPR and PIPL, available at: https://www.ijlt.in/post/india-decrypting-critical-concepts-under-india-s-digital-personal-data-protection-act-2023-and-com (last visited on October 2, 2024).

also lays rules on data localization that may hamper cross-border investigations involving any artificial intelligence technologies. Also, Section 69 of the Information Technology Act of 2000 provides the power to any authorities to intercept, monitor, or decrypt information in the interest of the sovereignty and integrity of India and the security of the state.[18] However, the application of such power has to be contingent on privacy compliance, and in the case of applying AI for surveillance mechanisms, there has to be legal backing explaining why and how it is applied to prevent bad actors from exploiting such platforms.

5.1 Challenges with Legal Compliance

The incorporation of AI in cybercrime investigation is a complex process in terms of compliance with the existing law regarding data acquisition, retention, and processing. The first is the issue of processing the data timely while dealing with requirements provided under current applicable privacy laws. Artificial intelligence technologies use data feeds for their teaching and operation, and data feeds usually entail information concerning individuals. However, provincial or national legislation like the DPDP Act in India and the GDPR in Europe sets certain standard requirements for the collection, storage, and use of the data. Police agencies and forces need to tread on these legal issues very carefully because if there is a violation by the police, then all the evidence gathered can be thrown out of court.

Another huge task is the management of the collected data during cybercrime investigations in a way that minimizes the risk of it being accessed by anyone who has no business with it. Given that AI models are applied in investigations, the data on which they are trained must be relevant, adequate, and do not exceed the data necessary for its processing. It corresponds to the concepts of data minimization and purpose limitation contained in data protection statutes. Nevertheless, the ways of adhering to these principles are not always clear, as cybercriminal activity investigations presuppose the accumulation of a great deal of information that can be irrelevant at first sight.[19]

Furthermore, cross-border data transfers have a concern of legalities enhanced by cross-border electronic crime investigations, which require the exchange of data between jurisdictions. The GDPR has put barriers to the transfer of data to non-EU countries, and India's proposed data localization standards pose legal and procedural challenges to effectively implementing AI in transnational cybercrime analytics. It, however, means that efficient and effective AI-based investigations need to be carried out while, at the same time, compliance with such regulations is achieved through the negotiation of international data-sharing agreements and other legal compliance measures. Noncompliance with these requirements results in legal responsibilities, inability to investigate, and infringement of the legal rights of individuals.

5.2 Ethical Considerations in Using AI

The application of artificial intelligence in cybercrime investigations also brings out several ethical issues, especially about the conflict between the Privacy Act and the Crime Prevention Act. On the one hand, AI technologies bring much value in improving the speed and quality of cyber investigations; on the other hand, they are concerning for personal data privacy. Hyping alarm concerns regarding the state’s extent of intrusive powers, surveillance, and data gathering. AI systems are capable of amassing substantial amounts of personal data.

The second one is that bias is very likely to show up in AI algorithms. Like all human creations, AI systems are designed by humans with the use of specific sets of data, and if this set of data has pre-existing

[18] Suhrith Parthasarathy, "Surveillance and its privacy pitfalls" *The Hindu*, December 22, 2023.

[19] K. Quezada-Tavárez, P. Vogiatzoglou, and S. Royer, "Legal challenges in bringing AI evidence to the criminal courtroom", 12 *New Journal of European Criminal Law* 531-551 (2021).

prejudice, then the AI systems themselves will too. In the course of employing AI in investigations of cybercrime, prejudiced AI means it becomes noble to target certain groups, thus contravening provisions of the Indian Constitution on equality and non-discrimination.[20]

The last analyzed ethical issue about the application of AI in cybercrime investigations is accountability. AI systems, especially when they are based on intensified machine learning algorithms, have black-box syntax, that is, their decision-making possibilities are not easily interpretable by the human mind. The lack of explaining or justifying the various choices made by AI increases concern over responsibility of action, particularly when the system is wrong in something such as identifying a suspect or repudiating a ticket. Therefore, introducing proper guidelines for the actions taken by AI-controlled apparatuses demands a certain number of decisions must be made by a person to include the protection of an individual's rights and to create a legal way to seek correction in case of an error. Currently in India, the legislation regulating the accountability of AI is in its infancy; therefore, it requires a proper set of regulations that would define responsibilities whether on the side of enforcement agencies, developers, or any other party that may be using AI systems for tackling cybercrimes.

6. CHALLENGES IN INTEGRATING AI INTO CYBER CRIMES INVESTIGATION

The implementation of AI in cybercrime investigations is faced with a set of technical issues that need to be met for AI technologies to effectively be applied. Some of them are technical and concerned with the problems of data quality and availability for AI model training. A further requirement is the fact that AI algorithms, especially those referred to as machine learning algorithms, need a great deal of data of good quality. However, in the case of cybercrime investigations, the extraction of such data is another problem because there are legal concerns about privacy, decentralized information systems, and the fact that the data collected in most cases is often sensitive. Some of the challenges posed by the data gathered from such cyber-crimes include the possibility of sparsity, noise, or even bias, which raises questions about the capability of AI models to recognize cyber threats. Also, there's the question of possession and utilization of personal data for AI training.[21]

There is also another technical issue in applying AI in analyzing cybercrime investigations; this is the issue of encryption. Encryption is a popular cyberspace tool that is widely used by cybercriminals to disguise their actions. AI systems are troubled by problems of decryption, especially where the systems in use are equipped with one of the most difficult-to-crack sets of algorithms. While there are recent developments in more advanced AI models, such as those based on deep learning routines, the activity is computationally heavy and can take a relatively long time to sort out the pattern to make inferences that might assist in the decryption of some forms of data. Regarding ransomware attacks where the criminals use complex encryption to keep the victims away from their systems, AI's capacity to decrypt the information or even to identify the decryption key is strait-jacketed by the algorithm used by the criminals. This technical restriction becomes a massive challenge in the utilization of AI in solving cybercrime since the absence of such inherent knowledge can slow an investigation.

[20] R. K. Bharati, "Ethical Implications of AI in Criminal Justice: Balancing Efficiency and Due Process", 9 *RESEARCH REVIEW International Journal of Multidisciplinary* 93-105 (2024).

[21] Cyber Crime Investigation and Forensics: Leveraging AI and Big Data for More Effective Solutions, available at: https://www.researchgate.net/profile/Adnan-Ali-56/publication/384327556_Cyber_Crime_Investigation_and_Forensics_Leveraging_AI_and_Big_Data_for_More_Effective_Solutions/links/66f451e9553d245f9e351862/Cyber-Crime-Investigation-and-Forensics-Leveraging-AI-and-Big-Data-for-More-Effective-Solutions.pdf (last visited on October 2, 2024).

6.1 Legal and Regulatory Hurdles

Disregarding the integration of AI into cybercrime investigations is primarily represented by legal and regulatory barriers. The first major concern that is valid concerns the problem of surveillance and the collection of vast amounts of data. Surveillance AI technologies can gather and analyze data, and therefore it profits suspicions that privacy rights could be to some extent invaded. AI applications can be used for most surveillance purposes, and such uses will need legal and ethical regulation. Section 69(1) of the Information Technology Act, of 2000, empowers the government to intercept, monitor, or decrypt any information in the interest of sovereignty, public order, or national security, but this power has to be used sparingly; the usage of AI tools must not infringe the constitutional provision against unreasonable search and seizure.[22]

Another essential regulatory issue remains privacy and data protection law compliance. In India, the Digital Personal Data Protection Act, 2023 (DPDP) relates to collecting, storing, and processing personal data and restricts the use of data by the government and private sector in India. Some of the specific provisions of the DPDP Act include: under the informed consent section, broadcasting organizations face problems in obtaining informed consent that would allow them to access and use the data they require to feed their AI models. The data minimization section provides the same problem for broadcast organizations as they seek to use big datasets to train their models. In addition, data localization is proposed, as specific categories of personal data will have to be processed in India only, and this creates more practical obstacles for international investigations. This means that while implementing the laws that will protect these data and while using AI in the fight against cybercrimes, their agencies must carefully work to strike a balance between the public and their rights.

6.2 Ethical Challenges

The issue of ethics concerning the role of AI in cybercrime investigations is based principally on two facets: bias within AI and discrimination, and misuse of AI tools for unlawful surveillance. It is a fact that the current models learned from historical data, and thus, if this data reflects prejudice, the model will also endorse prejudice. In connection with the fight against cybercrime, unfair machine learning results can be used to bias, for example, the increased attention of law enforcement agencies to certain populations or the targeting of suspicious individuals based on profiling.

Another ethical issue is that AI tools may be used for unlawful monitoring. Most artificially intelligent technologies encompass facial recognition and predictive analytics that can be adapted to pull off mass surveillance, which is clandestine surveillance without the subject's consent. As the above analysis shows, such practices could infringe on privacy rights in a major way and may be applied for reasons apart from policing legitimacy.[23]

6.3 Resource and Skill Constraints

This study has identified other challenges that hinder the efficient implementation of artificial intelligence in criminal investigations, including resource and skill limitations. AI technologies should be integrated into law enforcement agencies; however, professionals who have appropriate skills and knowledge are scarce. A successful implementation of AI in solving cyber crimes requires knowledge of data sciences, machine learning, cyberspace, and digital forensics. But, as it stands, most law enforcement organizations do not have officers who possess the relevant IT background and experience to design effective, deployable, and sustainable AI solutions. Closing this skills deficit, of course, calls for significant

[22] *Supra* Note 20.
[23] *Supra* note 19.

investment in training and capacity-building interventions to impart to law enforcement personnel knowledge and skills essential in containing AI in investigation and enforcement.[24]

Due to the high costs it takes to build an AI infrastructure, it is a big challenge we see. There are high costs associated with the actual development and then the constant running of any AI-based system: investment in computing hardware, data storage, software, and more. Also, the data costs for fetching socio-spatial high-quality datasets that are necessary for training AI solutions may not be easy to afford for most law enforcement agencies, especially when they are working under so many constraints, for instance, inadequate funding. The costs are not limited to acquisition only, but also the cost of maintenance, upgrade, and enhancement of the AI systems calculates the additional cost. In India, police organizations are generally resource-challenged, and obtaining adequate funding to deploy AI applications at a larger level is still a concern. It may, therefore, be necessary to rely on public and private collaborations as well as government funding schemes due to these resource limitations that are hitherto necessary for the extensive use of AI in combating cybercrime.

7. Future Directions for Integrating AI Into Cybercrime Investigation

This research reveals that AI has shown promise in many aspects of cybercrime investigation; however, there are barriers to the technological application of AI, legislation, and morality. For now, the trend has called for a set of specific future directions toward fully tapping into the capabilities of AI in responding to emerging cyber threats. The following guidelines suggest how current drawbacks could be dealt with so that AI in cybercrime investigations could be optimally deployed without violating legal and ethical norms.

1. There should be conflict-free and secure arrangements for sharing information across borders in cybercrime investigations.
2. Establish a process for the collection of a better data set for AI training through synthetic data.
3. Legislate Laws that can be used to regulate the best use of artificial intelligence in cybercriminal justice.
4. Introducing new separate rules for AI into the existing privacy legislation.
5. Establish guidelines that dictate how differently AI ethics policy meets the use of law enforcement.
6. Concentration of bias prevention strategies in AI to reduce the likelihood of the targeted population groups being targeted.
7. Start accrual of additional classes for the police on the topic of artificial intelligence.
8. Promote the collaboration between the public and private sectors to swap AI human capital.
9. The implementation of AI should involve the use of cloud computing and open-source tools to help decrease costs.
10. The state-of-the-art AI models to deal with encryption techniques should be developed.
11. Establish international legal prescriptions that improve the ethical use of AI in the investigation of cross-border cybercrimes.[25]

Possible future developments for the integration of AI in cybercrime investigation entail multi-disciplinary, legal, ethical, and technological changes. Data quality should be improved, extensive legal and ethical requirements should be developed, AI resources should be allocated, capacities within law

[24] Syed Khurram Hassan and Asif Ibrahim, "The role of Artificial Intelligence in Cyber Security and Incident Response", 7 *International Journal for Electronic Crime Investigation 154*-165 (2023).

[25] *Supra* note 7.

enforcement should be increased, and more accountability should be ensured to further use AI to fit into the ever-changing nature of cybercrime. These future steps are important to trigger the thorough fulfillment of AI features contributing to aspects of security against cyber threats as well as the protection of citizens’ rights and legal frameworks.

8. Conclusion

Artificial Intelligence is believed to have a lot of potential in terms of improving the given operational environment, given the availability of intelligent tools applicable to the investigation of cybercrime, something that current methods cannot deal with in terms of their broad scope. Sub-technologies of artificial intelligence belonging to machine learning, natural language processing, and deep learning classes can help detect and investigate cybercrime more effectively since they work with big data and perform data analysis, as well as recognize patterns and automate routine tasks. These capabilities are essential to preventing phishing schemes, ransomware, and other criminal activities, to allow the police to prevent such criminal activities in cyberspace. On the use of artificial intelligence in solving cybercrime: Challenges. Traditional methods prove disadvantageous by addressing the problem of big data and encrypted processes in cyber surveillance. AI though effective comes with some challenges including; privacy, bias, and regulation. The application of AI requires prudential measures to be taken, namely in non-unfair discrimination and the prevention of over-surveillance, which is intrusive of a person’s rights. Furthermore, laws such as the GDPR in the European Union and the DPDP Act in India contain harsh requirements for the use of data, which is needed to protect the citizens’ rights but, at the same time, will allow AI technologies to effectively contribute to investigations. The use of AI in the investigation of cybercrime: the legal systems of countries have crucial importance in the integration of the use of AI in the investigation of cybercrime. This paper emphasizes recognizing certain effective guidelines that would enforce the proper ethical and legal use of AI Technologies. Such regulations should help make the use of AI in the police service easily explainable, and devoid of any prejudice. That is why countries have to join to introduce international conventions and memoranda that can help exchange information on cyber representatives and coordinate their activities. This collaboration will be important in dealing with the transnational character of cybercrimes and ensuring that AI can work properly and to optimum results. Therefore, the following recommendations can be made to improve AI in cybercrime investigations in the future. This is the kind of support governments and law enforcement agencies should direct on the development of various advanced forms of Al models that would handle the encryption or the various other aspects of it so that the utilization of the cloud as well as open source, which they have been advocating as the cost-saving measures, can be stepped up while at the same time improving on the Al’s of investigations so that they are more efficient and faster. Education for law enforcement personnel in terms of the new AI technology as well as issues of public-private partnerships is also essential in developing the necessary stock. In conclusion, AI holds great significant value regarding the solution to those threats that modern cyber security faces, but the incorporation of AI into the processes of investigation of cybercrime has to be done carefully to avoid violation of individuals' and groups' rights to privacy, ethical values, and the overall requirement of community and governmental trust. Policing through artificial means is a great concern for the future as long as it is done in a balanced fashion where the ability to harness AI as a tool for law enforcement will not infringe on such basic rights for citizens. The most important condition for the prevention and further fight against contemporary cyber threats will be the constant progress of the AI technologies used, as well as the existence of an efficient legal and ethical foundation to contrast the cybersecurity threat and fight against cybercrime, while at the same time preserving crucial civil rights and liberties.