A PARADIGM SHIFT IN TRADITIONAL INVESTIGATION METHODS: INTRODUCTION OF AI IN DIGITAL FORENSICS

Dr. Sufiya Ahmed, Associate Professor, Department of Law,
Babasaheb Bhimrao Ambedkar University, Lucknow

Nikhil Kumar, LLM, Department of Law,
Babasaheb Bhimrao Ambedkar University, Lucknow

ABSTRACT

Digital forensics offers a scientific method of acquisition, analysis, and preservation of data contained in digital media whose information and contents can be used as evidence in a court of law. This form of investigation is done for the search of digital evidence so that it can be produced before the court and made admissible. Given the complexity and ever-evolving nature of digital threats, it is suggested that a paradigm shift in the way that cyber forensics investigations are conducted is required. Artificial intelligence holds great promise for criminal investigations, especially in the areas of information extraction, data analysis, and decision-making support. It can also help with data gathering and processing, criminal activity identification, prediction, and classification. Artificial intelligence can improve law enforcement agencies' operations by lowering the need for extra human resources, expediting investigations, and minimising human mistakes. AI can bring a boom in cybercrime detection and investigation, DNA analysis, e-document detection, and any literature finding through meta-analysis of vast, complex data available from various sources in a very short period of time. This paper offers a critical insight into the current challenges faced by our criminal justice system and proposes to apply AI technology for ensuring speedy justice.

Keywords: criminal investigation, cyber forensics, digital forensics, AI

Introduction

"Justice" has always been the essential component of life and liberty, and the hatred around a miscarriage of justice is the root cause of all wars. To discover the truth and avoid an injustice being committed is the goal of any criminal investigation and trial. [1] Building a just society and ensuring responsive governance are based on the "Justice, Truth, and Evidence" triangle. In essence, the "truth" behind a fact helps the court carry out its justice-administration duties. But truth and justice are abstract concepts, and "evidence" as a tangible object helps establish the truth and ensures a fair trial. Therefore, strong scientific evidence stands for the victory of truth, which brings about justice. [2] The ultimate objective of the criminal justice system is to protect or restore social control by means of a specific division or amalgamation of processes, bodies, and organizations, or, in other words, an intended or systematic type of response in which a community would have reacted to an action or individuals that it finds odd or challenging, unpleasant, frightening, or otherwise objectionable. [3] Both in the interest of the public and the accused, it is required to conduct an investigation into crimes, including violent and serious ones, in a fair and reasonable time, as it otherwise frustrates the very objective of the penal laws. [4] The Supreme Court, also acknowledging the very requirement, held speedy trial as a fundamental right to the accused [5] which begins with the arrest of the accused and continues to all phases of investigation and trial, even including appeals and revisions. [6] Disposing of the case as soon as possible so as to ensure the justice delivery system becomes more efficient and trustworthy.

In India, police have been assigned the primary role in the scheme of criminal investigation and prevention. [7] The police serve a crucial role in maintaining the rule of law, promoting life, liberty, equality, and fraternity among state subjects, and preserving the security and protection of human rights in a democratic system of government. Apart from this, identifying offenders and conducting investigations into crimes constitutes a crucial role. Criminal investigation, is

[1] Zahira Habibulla H. Sheikh v. State of Gujarat, (2004) 4 SCC 158, and Mohd. Hussain v. State (NCT of Delhi), (2012) 9 SCC 408.
[2] Bhumika Indulia, "Spreading Wings of Forensic Science," *SCC Times*, 2024, 04, *available at*: https://www.scconline.com/blog/post/2024/01/16/spreading-wings-of-forensic-science/ (last visited April 27, 2024).
[3] Reema Bhattacharya and Aqueeda Khan, "Use of Science in Law: An International Review of Criminal Justice System" 9 *Jour* 01-02 (2022).
[4] Law Commission of India, "239 Report on Expeditious Investigation and Trial of Criminal Cases Against Influential Public Personalities" 01-03 (March, 2012)
[5] *Hussainara Khatoon* v. *Home Secretary, State of Bihar*, 1979 AIR 1369
[6] *Kartar Singh* v. *State of Punjab*, 1994 SCC (3) 569
[7] K.N. Chandrasekharan Pillai (ed.), *Criminal Procedure* 22 (Eastern Book Company, Lucknow, 6th edn., 2014).

one of the prime duties of police, does not meet satisfactory standards. The whole burden of collecting the evidence with due process and efficiency is assigned to the police, which generally serves as the first point of contact if someone is victimised. But the data suggests some other picture. They lacked efficiency and time precision in the process. If we take the statistics of 2016 into consideration, the available data reflects that by the end of 2016, thirty percent (30%) of all cases submitted were still pending for investigation. This means that getting justice in India might take a very lengthy time, especially when combined with the backlog of cases in the courts for trial. [8] It was only for this reason that Dr. Justice V. S. Malimath report suggested the separation of the investigative wing from the wing responsible for maintaining law and order. [9] After failing by states to implement these recommendations over years, the Supreme Court came with judgement in the landmark case of *Prakash Singh vs Union of India,* [10] in 2006, in which it issued a guideline (one of the several guidelines for police reform) to, "Separate investigating police from law & order police, starting with towns/ urban areas having population of ten lakhs or more, and gradually extend to smaller towns/urban areas." The State sponsored conventional criminal investigation process (earlier) had been conducted in mainly three ways First, specific criminal investigations (detective departments); Second, specialist squads are formed in response to particular problems, e.g. anti-theft squads; and Third, major inquiry teams are set up to investigate specific incidents or events. All three organisational frameworks worked independently of forensic science (except for specialist scenes).[11]

NEED OF CYBER FORENSIC

India has the third biggest number of people using the internet in the world, after the United States and China; the number climbed substantially between 2012 and 2017, with an annualized growth rate of 44%, and India was ranked among the top five countries to be affected by cybercrime, according to a 22 October report by online security firm "Symantec Corp." To combat this exponentially growing and evolving threat to society, the government of India has taken initiatives against them. From establishing national cyber forensic laboratories, which provide early stages of digital forensic assistance to the investigating agencies in both online

[8] Sriharsha Devulapalli and Vishnu Padmanabhan, "India's Police Force Among the World's Weakest", *Live Mint*, June 19, 2019, *available at*: https://www.livemint.com/news/india/ (last visited on May 3, 2024).
[9] Government of India, "Committee on Reforms of Criminal Justice System" 92 (Ministry of Home Affairs, 2003)
[10] Writ Petition (Civil) 310 of 1996
[11] Jane Monckton-Smith, Tony Adams, *et.al., Introducing Forensic and Criminal Investigations* 05 (Sage, New Delhi, 2013)

and off-line modes, to legislating the Information Technology Act, 2000, which is a comprehensive statute addressing various aspects of digital transactions and cyber crimes (that includes definition, punishment, investigation, power of agencies, etc.),. The national cyber security policy provides for a secure and strong cyberspace environment and national cybercrime. The reporting portal provides a platform for the public report and provide information about cyber incidents pertaining to all types of crime. It also collects data and statistics, which help in evolving and effectively making policies. Even though the rate of unsuccessful investigations is increasing with time. [12]

These crimes occur in cyberspace, which is a notional or virtual world, unlike the traditional vulnerabilities that happen in the real world. As it is always said, to combat any challenge, there are two major steps; first, a cure, and second, prevention. In context of cyber challenges, prevention is cyber security and cure is proper and effective investigation in order to collect evidence and make the perpetrator pay for his deed. The internet is universally available and thus borderless. The issue of how to handle technological crimes has emerged as a result of this borderless technology. The primary issue with these types of crimes is with law enforcement and investigation. One of the most difficult problems India's law enforcement organisations deal with is cybercrime. [13]

Considering a cyber-investigation, for it to be an effective and impactful investigation, it must reflect and contribute to the increased percentage of convictions of offenders, and for that, it must collect evidence that can be produced before court and made admissible. [14] Digital forensics offers a scientific method of acquisition, analysis, and preservation of data contained in digital media whose information and contents can be used as evidence in a court of law. The digital evidence collected through cyber forensics must be authentic (that is, it must relate to the incident), complete, reliable (the chain of seizure procedure becomes crucial), and believable (the document and reports should be in understandable language and must develop trust among the jury and judges), as some essential conditions must be fulfilled to be admissible. [15] Due to this reason, probably the trickiest and most intricate aspect of the

[12] Anupriya Chatterjee, "Why are cybercrime convictions low in India? 'Weak forensics, dark net, & cross-border attacks," the Print, April 24, 2024.
[13] Prakash, Pranav Raj. "Cybercrime Investigation and Enforcement of Law in India." *IAHRW* 02 (2015)
[14] Hunker, Jeffrey. Cyber War and Cyber Power: Issues for NATO Doctrine. NATO Defense College,. *JSTOR*, 01, (2010)
[15] Anthony Reyes and Kevin O'Shea, *et.at., Cyber Crime Investigations*, 225 (Syngress Publishing, Inc., Rockland, MA, 2007)

cybercrime investigation process is digital forensics. It is complicated as well as complex, but at the same time, it will also be the source from which the strongest evidence will come. [16] The traditional digital forensics approach involved physical seizure of computers and related systems, then, image and data copying bit by bit in a forensically sound manner, which was time consuming and less efficient (as the data to be preserved were large in size) and resulted in major investigations being either unsuccessful, incomplete, or inadmissible evidence. [17] relying on the National Crime Records Bureau report (NCRB) released by the Union Home Ministry of five years of statistics that cover the years 2017 to 2021. Of the chargesheets submitted in 5,180 cases throughout all states and Union Territories (UTs), only 152 resulted in convictions in 2017. Just over 490 of the 7,000 cases in which chargesheets were submitted in 2018 resulted in convictions. Chargesheets were submitted in 9,000 cases in 2019; of those, 360 resulted in convictions; and in 14,087 cases in 2020, there were almost 1,109 convictions. The figures dropped to 490 convictions in over 18,000 cases where chargesheets were submitted in 2021. [18] The primary goal of any cyber forensic specialist employing cyber forensics technology is a speedier investigation procedure with reliable outcomes. Cyberforensics technology is incredibly important in today's highly developed and modern world. Cyberforensics aids professionals in computing forensics by providing vital digital or electronic evidence that is needed to locate the criminal offender. [19] It is therefore required to shift the traditional approach to crime investigation, and there is a need for a paradigm shift to application of some scientific techniques in cyber investigation.

[16] Ibid
[17] Martin Novak; Jonathan Grier; Daniel Gonzales, "New Approaches to Digital Evidence Acquisition and Analysis," 2018, *Available at:* nij.ojp.gov:(Last visited on april 23, 2024.)
[18] Anupriya Chatterjee, "Why are cybercrime convictions low in India? 'Weak forensics, dark net, & cross-border attacks," the Print, April 24, 2024.
[19]Timothy M. Mackenzi colonel (air university), *Available at :* https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF (Accessed April 21, 2024.)

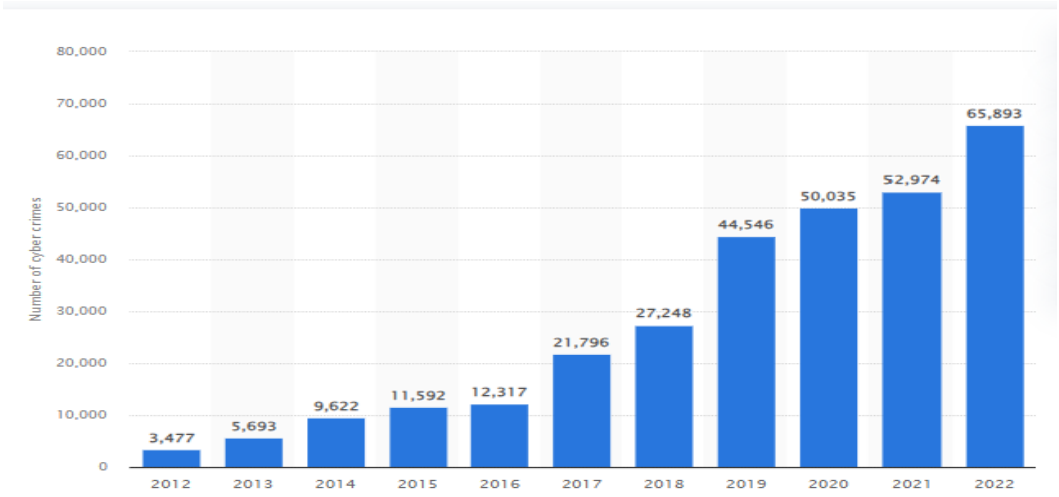

Chart: Number of cybercrimes vs. time (years). source: stastica [20]

Cybercrimes against people, property, and the government are the three main categories. Email harassment, stalking, defamation, unauthorized access to computer systems, indecent exposures, email spoofing, fraud, cheating, and pornography are examples of cybercrimes against people or individuals. Computer vandalism, virus propagation, denial of service attacks, unauthorized access to computer systems, infringements on intellectual property rights, Internet time theft, and the selling of illicit goods are examples of crimes against property related to computers. Cyberterrorism, online gambling, forgeries, trafficking in financial schemes, distributing pirated software, exposing minors to inappropriate content, and information possession are examples of cybercrimes against the state or society. [21]

There are many ways to exploit vulnerabilities or launch a cyberattack. [22] For example, according to the US Department of Defense [23], cyber attacks can be passive cyber attacks (they termed it computer network exploitation) or disruptive cyber attacks (they termed it computer network attack). A passive cyber attack generally involves copying and removing data without interrupting systems, or a disruptive cyber attack involves corrupting or modifying data, impacting system or network services, or refusing or restricting usage of systems or networks. Disruptive cyber attacks might be motivated by greed, vandalism, revenge, or extortion. They

[20] Statista, Available at : https://www.statista.com/statistics/report-content/statistic/309435 (accessed April 22, 2024.)
[21] Shantanu Kemkar (ed.), *Criminology & Penology with Victimology* 143-155 (Central law Publication, allahabad, Fifteenth Edition.)
[22] Hunker, Jeffrey. *Cyber War and Cyber Power: Issues for NATO Doctrine*. NATO Defense College, 2010. *JSTOR*, http://www.jstor.org/stable/resrep10354. (Accessed April 22, 2024.)
[23] Timothy M. Mackenzi colonel (air university), *Available at:* https://media.defense.gov/2017/Nov/20/2001846608/-1/-1/0/CPP_0004_MCKENZIE_CYBER_DETERRENCE.PDF (Accessed April 23, 2024.)

can also be carried out by terrorists, non-state actors, or states. Cyberwarfare and state-sponsored attacks: are now becoming serious threats as critical infrastructure and confidential government data are becoming more vulnerable to cyberespionage and state-sponsored cyberattacks, which pose a threat to developing countries like India. Disruptive cyber attacks can have major physical, social, and economic consequences. These can be any of electrical power systems, rail systems, nuclear power, military vulnerabilities, and other economic infrastructure. They are sophisticated yet critical for the political and social welfare and well being of citizens. Advanced Cyber Attacks: Cybercriminals are becoming more and more skilled at targeting people and businesses with sophisticated methods like ransomware, zero-day exploits, and social engineering.

A NEED FOR PARADISM SHIFT IN APPROACH OF INVESTIGATION

Cybercrime has very serious ramifications in today's high-tech society, as computer-run technologies are being utilised more and more in everything from basic door security systems to nuclear power plants. [24] The below table represents an interconnection between the sophistication of the attack and time in years. The chat clearly shows that in the late 90's and early 2000s, cyber attacks were primarily based on basic weapons like malicious codes, hacking,etc, But later, they grew uncontrolled, advancing the weapons of cyberattack like advanced worms, cyber espionages, and warfare, etc.

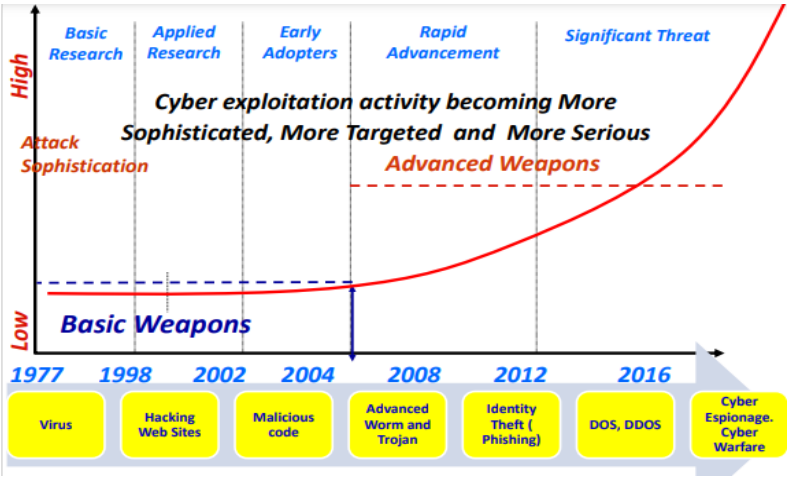

Chart: Attack Sophistication v. time (years) source: Niti Ayog [25]

[24] Narinder Singh and Moirangmayum Sanjeev Singh. "CHALLENGES OF CYBER CRIME IN INDIA." *International Journal of Social Science and Interdisciplinary Research* 3 (2015)

[25] Dr. V.K. Saraswat, Cybersecurity Conclave at Vigyan Bhavani, *Available at:* https://www.niti.gov.in/sites/default/files (Accessed 22 Apr. 2024.)

On the other hand, the subject matter of cyber forensics is totally backed by informational technology, which is ever evolving and changing, unlike traditional forensic science, where the core matter does not changes so rapidly. A fingerprint may change and evolve, but it does it gradually over the lifespan of an individual. However, it is said that operating system changes nearly in every five years. The storage devices and drives continues to grow larger and larger (improving the magnetic data density) while decreasing in volumes. It is therefore required to evolve the traditional practices, procedures and techniques of cyber investigation to obtain digital evidences as the technology is evolving and developing continuously. [26]

Cyber forensics, or digital forensics, offers a combination of computer science and legal science. This form of investigation is done for the search of digital evidence so that it can be produced before the court and made admissible. Digital foresic essentially involves three major steps Seizing the media, Acquiring the media, and Analysing the forensic image of the original media. [27] (1) Device Identification (involving seizure): The initial step is to identify any electronic devices or storage media that may contain data, metadata, or other digital artefacts related to the investigation. These electronic gadgets are gathered and preserved in a forensics lab or similar secure location to ensure successful data retrieval. (2) Data preservation (involving acquiring): Forensic professionals generate an image, or a bit-by-bit copy, of the information that needs to be stored and maintained. They then securely store both the image and the original to prevent them from being modified or damaged. Experts collect two types of data: persistent data (stored on a device's local hard disk drive) and volatile data, which must be treated with caution because it is fleeting and can be lost if the device shuts down or loses power. For example, data placed in memory or in transit, such as cache, and RAM (random access memory),. (3) Forensic analysis: Forensics experts then examine the image in search of any relevant digital data. Files, web browser history, emails, and other items may have been erased intentionally or unintentionally. Investigators use specialized techniques such as live analysis, which evaluates still-running systems for volatile data, and reverse steganography, which exposes data hidden by using steganography, a technique for concealing sensitive information within ordinary-looking messages, to uncover "hidden" data or metadata. (4) Reporting: Finally, forensic professionals prepare a formal report summarizing their analysis

[26] Anthony Reyes and Kevin O'Shea, *et.at.,* Cyber Crime Investigations, 221 (Syngress Publishing, Inc., Rockland, MA, 2007)

[27] National Institute of Justice funding opportunity, "New Approaches to Digital Evidence Processing and Storage," Grants.gov announcement number NIJ-2014-3727, (2014.)

and disclosing the investigation findings. Reports vary from case to case and are frequently used in court to present digital evidence.

Given the complexity and ever-evolving nature of digital threats, it is clear that a paradigm shift in the way that cyber forensics investigations are conducted is required. As we have already seen above that how conventional approaches frequently find it difficult to keep up with the quick advances in technology. By encouraging investigators to foresee and counter possible dangers before they manifest, paradism's proactive investigative method boosts the overall resilience of cyber ecosystems. [28]We will try to analyse various possible approaches that can be applied in the cyber forensics investigation against these cyber challenges to compact the cyber challenges effectively and adequately.

Advancing Automation in Digital Forensic Investigations Using Machine Learning Forensics:

In the last few years, every piece of data, be it a book, video, medical information, genetic information, etc., has been transformed into digital formats. As a result of this transformation, this information has become an easy target for cyber perpetrators. [29] As we know, digital forensics helps in the extraction of deleted, hidden, or encrypted files from the suspect's system or device, but the existing investigation process or method requires more human involvement, which unfortunately makes it a slow process. Therefore, the current manpower and infrastructure of governmental agencies involved in investigations find themselves insufficient to tackle these challenges. Machine learning, a subset of artificial intelligence technology [30], may prove itself as a novel approach to tackle this challenge. This advanced technology has the capability of automation, and its algorithms are so programmed and trained that they express themselves in a way like human's activity and behaviour. [31] For example, AUDIT [32], which is an automated disc investigation toolkit, offers a way to investigate targeted images and data in a disc even with a non professional, non expert or person with minimal knowledge

[28] A.C.Tapia, and La Porta, *et al.*, Paradism: A New Paradigm for Cybersecurity Investigation, *Journal of Digital Forensics, Security and Law*, 37-52.(2020)
[29] Iqbal, Salman, and Soltan Abed Alharbi. "Advancing Automation in Digital Forensic Investigations Using Machine Learning Forensics." *Digital Forensic Science* (2019): n. pag.
[30] Artificial intelligence versus machine learning, *Available at* https://cloud.google.com/learn/artificial-intelligence-vs-machine-learning (Last visited on March 28, 2024.)
[31] Machine learning, *Available at :* https://www.ibm.com/topics/machine-learning (Last visited on March 28, 2024.)
[32] Umit Karabiyik, *Building an Intelligent Assistant for Digital Forensics* (2015) (Unpublished Ph.D. thesis, Florida State University College of Arts and Sciences).

of technology. The toolkit, based upon the physical and logical structure of discs, examines the target source in a holistic design.

Application of Artificial Intelligence in the Field of Criminal Investigation.

Al is evolving into a global catalyst for change in industries, communities, and governmental systems as a result of his acknowledged strength as a transformative force. The law and the criminal justice system also did not remain untouched by its influence. Our honourable courts initially showed strong opposition to its incorporation into the Indian justice system, but they have gradually softened their position. We can see a lot of development in artificial intelligence being introduced in our justice systems. Consultation of Punjab and Haryana High Court in *Jaswinder Singh versus State of Punjab* [33] for broader aspects of bail jurisprudence around the world where cruelty is a factor in deciding bail; however, the court clarified that it is not an expression of the merits of the case. The increased use of this technology is expected to increase efficiency and productivity. At the (rescent) Indo-Singapore Judicial Conference, the honorable chief justice of India, commenting on the incorporation of AI in the Indian justice system (either in legal practice or judicial decision making) said AI in court presents both opportunities and challenges. To quote him, "We cannot avoid the question of using AI in court adjudication. The integration of AI in modern processes, including court proceedings, raises complex ethical, legal, and practical considerations that demand a thorough examination. The use of AI in court adjudication presents both opportunities and challenges that warrant nuanced deliberation,"[34] He embraced the incorporation of technology but also cautioned about the high risks, like indirect discrimination and unexplained bias. This opinion, however, shows that, gradually, the judiciary is also open to accepting modern technology, but with some caution. [35]

Artificial intelligence (AI) holds great promise for criminal investigations, especially in the areas of information extraction, data analysis, and decision-making support. As a logical extension of the progress of digitalization and algorithmization in criminal investigations,

[33] 2024: PHHC : 014669

[34] The Hindu,"AI presents both challenges and opportunities for courts, says CJI" *available at:* https://www.thehindu.com/news/national/ai-presents-both-challenges-and-opportunities-for-courts-says-cji/article68062517.ece (last accessed on 15 april,2024)

[35] Anmol Kaur Bawa,"Use Of AI In Court Adjudication Presents Both Opportunities & Challenges : CJI DY Chandrachud" *available at :* https://www.livelaw.in/top-stories/use-of-ai-in-court-adjudication-presents-both-opportunities-challenges-cji-dy-chandrachud (last accessed on april15, 2024)

artificial intelligence is actively being used in criminalistics.[36] Artificial Intelligence (AI) systems can help with data gathering and processing, criminal activity identification, prediction, and classification. Automation in criminal investigations has scopes from exploring the evidences at crime scene to AFIS (automated fingerprint identification system), [37] pattern recognition in financial transactions to audio video analysis , facial recognition to advanced crime scene reconstruction [38] However, as AI's capacity for decision-making can be interpreted as having "malicious intent," its application to criminal law poses concerns about accountability and punishment. If any error occurs or on any malfunction, who or how a computer can be held accountable (Mahardhika, 2023) [39] or other legal aspects in practical application.

POSSIBLE APPLICATIONS OF ARTIFICIAL INTELLIGENCE IN CRIMINAL INVESTIGATION (POTENTIAL PROSPECTIVE)

1.FORENSIC ODONTOLOGY

Forensic odontology is mainly concerned with the identification of individuals. It becomes more important when dental evidence is the only evidence for the crime. Dental hard tissues are known to be resistant to pressure, humidity, and high-temperature changes, which in the identification process makes them a very reliable source.[40] Forensic odontology involves the examination, evaluation, management, and presentation of dental evidence in criminal or civil proceedings, all in the interest of justice.[41] The most effective tool for storing, analyzing, and applying product data gathered for forensic evidence in court cases is artificial intelligence. For digital forensic and evidentiary investigations, it can establish and supply a repository. [42] For this purpose, a variety of algorithmic models can be developed and adjusted to allow all

[36] Sebyakin, Aleksey. "Artificial Intelligence in Criminalistics: System of Decision-Making Support." *Baikal Research Journal* 10 (2019)
[37] Al-Wajih, Yousif Ahmed, Waleed M. Hamanah, Mohammad Ali Abido, Fouad Al-Sunni and Fakhraddin Alwajih. "Finger Type Classification with Deep Convolution Neural Networks." *International Conference on Informatics in Control, Automation and Robotics* (2022).
[38] Liao, Guan-Lung. "A Novel Plan for Crime Scene Reconstruction." (2015).
[39] Mahardhika, Vita, Pudji Astuti and Aminuddin Mustaffa. "Could Artificial Intelligence be the Subject of Criminal Law?" *Yustisia Jurnal Hukum* (2023)
[40] José Luis Fereira 1, Angela Espina de Fereira, Ana Isabel Ortega, Methods for the analysis of hard dental tissues exposed to high temperatures, *available at :* https://pubmed.ncbi.nlm.nih.gov/ (last visited on mar.22, 2024)
[41] Sylvie Louise Avon, Forensic odontology: the roles and responsibilities of the dentist, *available at :* https://pubmed.ncbi.nlm.nih.gov/ (last visited on mar.21, 2024)
[42]J. Pathak and Niharika Swan, *et al.*, "Role of various stakeholders in application of artificial intelligence to forensic odontology - a potential prospective 09 *Annals of dental speciality* 51 (2021)

relevant stakeholders to make the best possible contributions to the field of forensic odontology. Most importantly, AI can be beneficial in forensic odontology if all stakeholders integrate interdisciplinary approaches.

2. DNA ANALYSIS

Another field in which this modern technology (AI) can play a huge role is in the analysis of DNA (deoxyribonucleic acid) in solving the puzzles of crime. Because of a number of fixed variations between people, the analysis of DNA of forensic interest is able to identify each person uniquely based on their genetic profile. This identification can be done by matching the profile of the human remains to profiles that are already known or by determining whether or not they are compatible with the DNA that their relatives inherited. [43] It is done through DNA sequencing. DNA sequencing establishes the four bases of the DNA nucleotide's sequence adenine (A), thymine (T), guanine (G), and cytosine (C). The rapid expansion of DNA grouping information brought about by the development of sequencing technology has pushed the study of DNA successions into a stream of massive data. [44]

3. IDENTIFICATION OF PERSON

Artificial intelligence (AI) plays a crucial role in the identification of individuals, particularly in real-time scenarios. An extensive review of machine learning approaches used in people detection and identification, such as the principal component analysis and support vector machines is provided by person identification using video-based detection and recognition or group picture identification. [45] Images of people in custody and image mining from social media or CCTV footage are now possible in real time through the application of deep learning. Appreciation for the development of deep learning and the construction of neural network programs, which have resulted in the automation of Internet of Things (IoT) [46] devices and technology, which has yielded good results. [47] IoT is an intelligent system programmed for the

[43] Álvarez, Ángel Carracedo. "DNA rewriting our memory: Recovering missing people through their genetic profile" (2019). March 21

[44] Goswami, Siddharth and Sachin Sharma. "DNA Sequencing using Artificial Intelligence." *2022 International Conference on Edge Computing and Applications (ICECAA)* (2022): 1033-1037.

[45] Priyanka, Ms., G. Patil and Dr. Manasi R. Dixit. "Person Identification in Group Photographs with Artificial Intelligence." (2021).

[46] IoT devices are pieces of hardware, such as sensors, actuators, gadgets, appliances, or machines, that are programmed for certain applications and can transmit data over the internet or other networks.

[47] Diallo, Chérif. "An Intelligent System for Detecting People from Images and Videos Provided by IoT Devices." *2021 International Conference on Computational Science and Computational Intelligence (CSCI)* (2021): 1721-1727.

detection of people and their identification.

4. CRIME PREDICTION

In recent years, machine learning techniques have been used to aid in criminal investigations. Similar crimes may be committed by the same criminal organisation or by the same perpetrator in succession. Even some states (like Korea and the US) have already started to apply machine learning for crime pattern detection and follow syndicates and criminal organisations. An ordinary investigation becomes slow when such huge and complex data is to be consumed to fetch and find crime patterns in group crime, as they offer urgency to be tackled. These associations have been reflected in the application of machine learning and network based algorithms by the Korean state police. [48] Considering an illustrative scenario of COMPAS (Corrective Offender Management Profiling for Alternative Sanctions), a recidivism prediction programme (most used risk management programme in the US) utilised in multiple US states. The American business Northpointe has created an artificial intelligence programme that examines a variety of variables, including past criminal activity, familial ties, educational background, and drug usage, to forecast the likelihood of recidivism. However, it has been claimed that the defendants' constitutional rights are violated by the algorithm's output, raising important questions about the algorithm's methodology and the elements taken into account when making a particular conclusion. [49]

5. AFIS (automated fingerprint identification system) [50]

The AFIS is an automated system for fingerprint identification utilising biometric techniques for collection, storage, and analysis of fingerprint data using digital imaging technology. The growing need for security applications to gather demographic data has led to a surge in interest in fingerprint-based security solutions. These systems, which employ a person's fingerprints as a unique biometric, are dependable and extremely secure. The effectiveness of the AFIS in terms of search time and matching speed between fingerprint databases was successfully

[48] Jhee, Jong Ho, Myungjun Kim, Myunggeon Park, Jeongheun Yeon, Yoonshin Kwak and Hyun-Weon Shin. "Fast Prediction for Suspect Candidates from Criminal Networks." *2023 IEEE International Conference on Big Data and Smart Computing (BigComp)* (2023): 353-355.

[49] Rhee, Gina. (2023). Artificial Intelligence Prediction Program in Criminal Justice System: focused on its Biased Algorithm in relation to the Racial Discrimination. Wonkwang University Legal Research Institute. 39. 57-73. (10.22397)

[50] Al-Wajih, Yousif Ahmed, Waleed M. Hamanah, Mohammad Ali Abido, Fouad Al-Sunni and Fakhraddin Alwajih. "Finger Type Classification with Deep Convolution Neural Networks." *International Conference on Informatics in Control, Automation and Robotics* (2022).

improved through the use of deep learning tools. A convolutional neural network (CNN) model was created in order to predict the types of fingerprints and classify them.With both databases, the suggested model demonstrated a high level of validation accuracy, achieving an around 94% overall prediction accuracy for fingerprint types.

CHALLENGES AND ISSUES FACED BY AI IN IMPLEMENTATION

The world is nowadays involved in a great debate on the legality and ethicality (of the standard of right or wrong) of the origin and processing of artificial intelligence. As we know, AI uses vast databases available on the internet, websites, social media, etc., along with almost every material and content of books, articles, editorials, and newspapers. A recent legal proceeding against AI named GPTs (generative pre-trained transformers), which trains itself on a large language model (LLM), is widely in the news, raising questions of its ethical and legal issues. In the case of *The New York Times Company v. Microsoft Corporation and OPENAI* [51] The New York Times accused Microsoft and OPENAI of copyright infringement and unlawful use of their data for training and development of this generative tool. Large Language Models (LLM such as ChatGPT developed by OpenAI) are advanced AI systems designed to understand, generate, and interact with human language in a way that mimics understanding. LLMs are trained on vast datasets compiled from the internet, encompassing everything from books and articles to websites and social media posts. This training enables LLMs to generate responses that are coherent, contextually relevant, and often indistinguishable from those that a human might produce. [52] Most of this contention comes from this side of people (who call it unethical), largely on two fronts: (1) *Copyright infringement* That is, they directly violate their copyrighted materials and contents for the training and development of AI. (2) and *Fair use principle*. Here they are accused of exploiting the contents rather than transforming them for commercial purposes.

It is therefore only the Council of Europe's Commission for the Efficiency of Justice (CEPEJ) that created moral guidelines, which later developed as ethical principles for artificial intelligence in legal systems and their surroundings. First is **respecting fundamental rights,** be they the *right to privacy, the right to equality, or fair treatment*. The underlying theme is

[51] Michael M. Grynbaum and Ryan Mac, "The Times Sues OpenAI and Microsoft Over A.I. Use of Copyrighted Work" *The New York Times, Dec.23, 2023.*

[52]OpenAI vs. The New York Times: A Pioneering Legal Battle Over AI and Copyright *available at :* https://www.livelaw.in/articles/openai-vs-the-new-york-times-a-pioneering-legal-battle-over-ai-and-copyright-252848?infinitescroll=1 (last visited on march 3, 2024)

that it must comply with basic human rights and ensure transparency and justice. It must comply with the provisions of law simultaneously ensuring independence in the decision making process of judges. At the (rescent) Indo-Singapore Judicial Conference, the honorable chief justice of India said that adopting a hybrid model of AI, i.e., interaction and intervention of both humans and technology, is inevitable and unavoidable in the field of law, but it comes with some challenges, like it might bring with itself inequality. To quote him, [53] "The adoption of AI might accentuate inequality by favouring those with access to advanced technology, and thus AI is a double-edged sword with a capacity to either enhance or undermine the pursuit of justice. Second, the **principle of non discrimination** is one of the first generation human rights and basic fundamental principles recognised in UDHR [54] We cannot deny the possibility of indirect or unexplained happenings of discrimination, as at the end of the day, its response is based on data made available and trained upon. The use of artificial intelligence (AI) tools to anticipate criminal activity does not ensure that prejudice or discrimination resulting from human interaction in the process of choosing the input data for the algorithm won't occur. There have been often claims against the COMPAS which is applied by the US, that the defendants' constitutional rights are violated by the algorithm's output, raising important questions about the algorithm's methodology and the elements taken into account when making a particular conclusion.[55]

In the case of *Jaswinder Singh vs State of Punjab* [56] the court sought the use of chat GPT for considering the broader aspect of Bail jurisprudence in granting bail where cruelty is the factor for decision. The court himself admitted that reference taken for the decision is not influencing the order and is not an expression of the merits of the case. The source of the chat GPT jurisprudence is unknown, and it did not study any legal theory. The basis of its result depends upon randomly mined data. It becomes a question of reliance whether a constitutional court can deprive someone's life and liberty based upon unproven jurisprudence. [57]

---

[53] The hindu,"AI presents both challenges and opportunities for courts, says CJI" *available at:* https://www.thehindu.com/news/national/ai-presents-both-challenges-and-opportunities-for-courts-says-cji/article68062517.ece (last accessed on 15 april,2024)

[54] United Nations," Universal Declaration of Human Rights" *Available at*: https://www.un.org/en/about-us/universal-declaration-of-human-right, Article 2

[55] Rhee, Gina. (2023). Artificial Intelligence Prediction Program in Criminal Justice System: focused on its Biased Algorithm in relation to the Racial Discrimination. Wonkwang University Legal Research Institute. 39. 57-73. (10.22397)

[56] 2024: PHHC : 014669

[57] Dr.Subhradipta Sarkar, "Chat GPT jurisprudence: strengthening justice or delivering injustice *available at* www.timesofindia.com (last accessed on 14 April, 2024)

CONCLUSION

As we conclude the paper, we find that cybercrime is an offense that falls under the purview of economic crime, telecommunications crime, white collar crime, intellectual property infringement, and civil jurisdiction. One common feature is the use of computers and information technology in its execution. Given the complexity and ever-evolving nature of digital threats, it is clear that a paradigm shift in the way that cyber forensics investigations are conducted is required. We have already seen above that how conventional approaches frequently find it difficult to keep up with the quick advances in technology, which makes them ineffective at combating contemporary cybercrimes. With the ongoing efforts of cybercriminals to leverage vulnerabilities and create novel techniques for committing digital offenses, forensic investigators must adopt a more proactive and all-encompassing strategy. With its focus on proactive approaches, applying modern scientific techniques, and flexible thinking, paradisianism offers a novel way of negotiating the complexities of digital investigations in the twenty-first century.

Along with that, examining the legal framework for data portability and secure storage is necessary. Along with this, the two main causes of these challenges are a lack of cybersecurity awareness and an inadequate legal framework. A large number of people and companies in India might not be completely aware of the risks and safeguards related to cybersecurity, which increases their vulnerability to cybercrimes (Lack of Cybersecurity Awareness). Despite India's efforts to address cybercrimes through the establishment of legal frameworks, there might still be gaps and difficulties with properly enforcing laws (inadequate legal framework). Data localization is necessary in order to provide users with the option to permanently delete their data. This can be achieved by tightening up data localization rules and only allowing them to be used in the parent nation. Because of this, the government must comprehend data localization and data security and take appropriate action by passing new legislation, saving Indian residents from having to look for other ways to safeguard their privacy.

"Artificial intelligence is not supposed to replace human intelligence; rather, it is meant to function as software created by humans that may be enhanced in discrete ways." [58] Modern technology is always evolving, bringing with it new levels of experience. Thanks to modern

[58] Baltrūnienė, Jurgita, "Place of artificial intelligence in the detection and investigation of crime the present state and future perspectives" *ojs* vol 26(2022)

technology, which has completely changed the way we communicate and access information, from social media and cloud computing to smartphones and tablets, our lives have become more convenient, easier, and more productive. Artificial intelligence (AI) can improve law enforcement agencies' operations by lowering the need for extra human resources, expediting investigations, and minimising human mistakes. AI can bring a boom in cybercrime detection and investigation, DNA analysis, e-document detection, and any literature finding through meta-analysis of vast, complex data available from various sources in a very short period of time. Researcher groups find it a revolution in the digital world and acknowledge its potential to ease the workload of humans in every field. They are not bothered by the debate about its ethnicity but see its great capability superseding other issues. Also to achieve sustainable growth, improve societal conditions, needs, and demands, and match up the high expectations of the citizens of a country like India, which is the world's fifth-largest economy and second-largest population, must navigate the difficulties and fully utilise the potential of modern technologies and must adopt policies that are in favour of such adoptions.