Artificial Intelligence an Aid in Detecting Cyber Crimes in India: A Compendium

Ms. Jayati Parsai, Dr. Richa Shrivastava

Associate professor, Sage University

DOI: https://doi.org/10.51244/IJRSI.2025.120500136

Received: 23 March 2025; Accepted: 01 April 2025; Published: 17 June 2025

ABSTRACT

That in this Research Paper the author has postulated an overall scenario of the position and role of artificial intelligence in detecting the cyber-crimes in India. A country where the population to police ratio is extremely disproportionate, in which detecting crimes and solving crime mysteries by providing justice to the victims and catching the perpetrators of crime is a very tedious job which requires heightened caution and meticulous precision, in which the Artificial Intelligence has acted as a wonderful and useful tool to curb, predict and catch the perpetrators of crimes, which has not only made the job of the investigating agencies bit hassle free but has also enhanced the quality and efficiency of their investigation.

The Research Paper has been prepared mainly through referring Secondary Sources, Research Papers and Articles of several legal luminaries and debates of Lok Sabha, for gaining analogical deductions and references thereon.

INTRODUCTION

The Artificial Intelligence (AI) is playing a very pivotal and leading role in enhancing almost the works and services of all the sectors like medical, legal, marketing, corporate, transport, aviation etc. throughout the globe. However, with the growing sphere of Artificial Intelligence and AI-driven Tools, a common man has be to very much cautious and aware regarding the potential threats and complexities which is involved in using of AI practically and prudently on day-to-day basis.

That AI in simple sense refers to a branch of computer science which is enabled and programmed to do a particular task or job through using AI-enabled software in order to act like humans, however AI is primarily an emotionless mechanism which is now being developed with incorporating the human-driven emotions, in order to assist a human being more perfectly and sophisticatedly.

That it has been noticed that, in the last two decades the India has been emerged as a leading hub for Artificial Intelligence and it's implementation in various facets of society is remarkable. That in this periphery the NITI Aayog (National Institution for Transforming India) has released National Program for Artificial Intelligence (NPAI) in year 2018 with an ulterior motive to create awareness among the common public regarding the benefits of artificial intelligence and developing it for public good.

Cyber Crimes in India

That in today's world of cut-throat competition and looking to the pace of growing popularity of cyber space throughout the globe, it is not wrong to term it as a "Digital Era" by looking to the quantum of digital presence of a common man of the country on the several social media platforms and professional portals, however with the same pace there is a noted increment and concerns rising over the cyber crimes and cyber frauds in India.

That in a country like India, where even after seven decades of independence a reasonable literacy rate can't be achieved, amid such a position it is extremely accessible and approachable for the cyber fraudsters or scammers to execute their malicious motives through using internet and online mediums and committing the crimes via cyber means, which may be a phishing mail, digital arrest, crypto fraud, e-commerce fraud, parcel

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue V May 2025

fraud, etc. Therefore for combating the cyber-crimes and to eradicate the perpetrators of cyber-crime from the country, it is essential to create public awareness and strengthen the base of the investigating agencies to firstly prevent the cyber-crime and secondly to curb or catch the cyber-crime at it's originating stage, so that the criminals can be punished for their crimes, the losses of the victims can be recovered and further the potential or prospective criminals can be demoralized from committing further crimes, with not only establishing the rule of law but also acting in furtherance of justice.

That it is a worrying trend to observe that in the first nine months of year 2024, according the data compilation of Indian Cyber Crime Coordination Center (I4C), which is division under Ministry of Home Affairs (MHA), the peoples of India lost around Rs.11,333 Crores (Eleven Thousand and Three Hundred and Thirty Three Crores) in which around 12 Lakh Complaints have been lodged against perpetrators who were mainly from the Southeast Asian Countries like Myanmar, Loas, Cambodia, etc.[1] That is it pertinent to mention here that amid the overall complaints the highest 2,28,094 complaints were against the Stock Trading Scams with losses of Rs.4,636 Crores, the next biggest scam is of Investment based Frauds with around 1,00,360 complaints and losses of around Rs.3,216 Crores, and then the next scam was of "Digital Arrest" with 63,481 complaints and losses of Rs.1,616 Crores.

That the Ministry of Home Affairs (MHA) has already established a National Cyber Helpline in order to provide hassle free lodging and tracking of complaints against the cyber-crimes in India, along-with designating a separate wing under it to look after especially for the cases of Crime Against Women (CaW), which has proved very beneficial in reporting and detecting the cyber-crimes in the country, along-with establishing a centralized database and communication mechanism among the State Cyber Cells and District Cyber Cells across the country.

That looking to the present need and infrastructure to combat with the cyber fraudsters in India the current system is not at par and sufficient to handle the complexities of cyber-crimes with ultimately compromising with the safety and security of a common man.

Legislations Governing Artificial Intelligence and Cyber Crimes in India

That it is worthwhile to mention that, with the drastic usage of Artificial Intelligence in India and around the globe, there is an acute need to regulate and administer it through some parliamentary mandate, in order to ensure appropriate usage of AI and curb the mis-use and unauthorized usage of AI Driven tools with ultimately hampering the overall interests of the society and leading to miscarriage of justice.

That there is no specific or particular statute or piece of legislation governing solely the complexities of Artificial Intelligence, however after the judicial pronouncement of K.S. Puttaswamy vs. Union of India, 2018 by Hon'ble Supreme Court of India, it has majorly contributed to secure the personal data and impose certain set of responsibilities on the service provider in order to avoid unwarranted hardships and intrusion into the privacy of any individual without consent, for which the Indian Parliament enacted The Digital Personal Data Protection Act, 2023 with an ulterior objective to protect the personal data of an individual and regulate the processing of such personal data obtained by the data fiduciary from the data principal to the consented extent and lawful purposes thereon.

However, the main provisions indirectly regulating the Artificial Intelligence and dealing with Cyber Crimes in India are:

The Digital Personal Data Protection Act, 2023 (DPDPA)-It aims primarily to regulate and safeguard from the misuse of personal data of an individual and imposes duty on the data fiduciary to use the data collected from individual, post his consent, only for the lawfully permissible purposes.

[1]THE INDIAN EXPRESS, https://indianexpress.com/article/india/cyber-scams-india-pm-modi-9692771/ (last visited on Jan. 3, 2025).

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue V May 2025

1.1 Section 06 (Consent)- That according to this section of the Act, the individual whose data is collected (Data Principal) has to provide his unequivocal, informed, unambiguous, free, specific and unconditional consent with a clear affirmative action, for which the intermediary who is collecting the information (Data Fiduciary) has to clearly inform that what information is collected from the Data Principal and for what purposes the information is collected, the most charming feature of the Act, is that the consent provided by the Data Principal is not absolute and can be revoked at any time.

1.2 Section 08 (Obligation of Data Fiduciary)- That according to this section, the data fiduciary posses some basic obligations for the data obtained by him from the data principal, like to use the data only for the purpose for which the data principal has originally consented for, to ensure implementation of appropriate measure for data protection, to make efforts to ensure the accuracy of data, etc. the non-compliance of the data will be dealt according to Section 33 of the Act.

1.3 Section 27 (Powers and Functions of Board)- That under this provision, the Central Data Protection Board Established U/s.18, shall have power to inquire into complaints under data breach and direct any remedial measures to the data principal, alongwith imposing penalty of the Data Fiduciary asper rules.

1.4 Section 33 (Penalties) R/w Schedule I- That according to this provision if upon the receipt of the complaint filed by Data Principal alleging breach of data or compromise with his privacy and the Data Protection Board of India draws the conclusion post adjudicating the facts that the Data Fiduciary has failed to protect the personal data of the data principal, then it may order to impose penalty on the erring Data Fiduciary, which in case of Breach in taking reasonable security safeguards to prevent data breach may extend upto Rs.250 Crores, in failure to giving notice of data breach to the data principal may extend upto Rs.200 Crores, and in case of breach in observance of additional obligations in relations of children U/s.9 may extend to Rs.200 Crores.

2 **Information and Technology Act, 2008-** It aims primarily to curb and discourage the perpetrators of cyber crime, along-with imposing hefty fines and rigorous imprisonments on the intruders in order to maintain the rule of law, the violators of privacy or perpetrators of security breach can be bought under the ambit of the act.

2.1 Section 66 (Hacking)- That under this section, unauthorizedly accessing any computer resource or data in absence of the consent of it's owner, shall be punishable with imprisonment upto three years or with fine upto rupees five lakhs or both.

2.2 Section 66-C (Fraudulently Using Password of Any Person)- That under this section, if any person with proper authorization obtains the password of any computer resource or device of any person without that person's consent, that for unwarranted intrusion to his privacy, the wrongdoer shall be punishable with imprisonment upto three years or with fine upto Rupees One Lack or both.

2.3 Section 66-E (Violation of Privacy)- That under this section, whosoever unknowingly without authorization captures the image of any person without that person's consent shall be liable for imprisonment which may extend upto three years or with fine upto Rupees Two Lacks or with both.

2.4 Section 67 (Publishing Obscene Material via any form)- That under this section, if any persons publishes any obscene material by objectifying any person without that person's consent, or compels any third person to commit the said crime or compels any person to omit to do a act which he is legally bound to do, shall be liable for imprisonment which may extend upto three for the first conviction and for five years in the second conviction, alongwith imposition of fine which may extend upto Rupees Ten Lacks only.

2.5 Section 67-A (Publishing or Transmitting Sexually Explicit Material via Electronic Form)- That under this provision, if any person circulates any sexually explicit material through any social media or otherwise with maligning the image and privacy of any person, shall be punished with imprisonment which may extend upto five years and fine which may extend upto Rupees Ten Lacks on the first in the first

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue V May 2025

conviction, and in subsequent conviction with imprisonment which may extend upto seven years and fine upto Rupees Ten Lacks.

3 **Bhartiya Nyaya Sanhita, 2023-** The Act primarily aims to punish the offenders of the crime and establish a rule of law in the society, being enacted as a part of criminal jurisprudence by repealing the old colonial Indian Penal Code, 1860, the Act introduced several changes and enhanced punishments for the crimes committed by the perpetrators.

3.1 Section 77 (Voyeurism)- That under this section, if any person through deploying any spyware mechanism or installation any hidden camera or AI Tool in any room or lavatory, captures the image of a women engaging in private act, shall be punished with imprisonment which shall not be less than one year but may extend to three years for the first conviction, however in the second conviction the perpetrator of the crime will be punishment with imprisonment of either description of three years which may extend upto seven years, and shall also be liable to fine.

3.2 Section 78 (Stalking)- That under this provision any stalker or cyber stalker, who stalks a women on social media or attempts to contact such women despite of her clear indication of disinterest, shall be punished on first conviction with imprisonment of either description which may extend upto three years and shall also be liable to fine, and on second and subsequent conviction with imprisonment of either description which may extend upto five years and shall be liable to fine.

3.3 Section 308 (Extortion)- That under this provision whosoever puts any person in fear to cause injury any deliver any private data or report to the third party without the free consent of the individual shall be liable to punished with imprisonment of either description which may extend upto seven years or with fine or with both.

3.4 Section 340 (Using as Genuine the Forged Document or Electronic Record)- That under this provision any person who forges any document or creates any document for the purpose of causing injury to the image of any individual or to commit cheating shall be punished with imprisonment of either description of two years which may extend to seven years or with fine or both.

How Artificial Intelligence is assisting the Investigating Agencies in Detecting the Cyber Crimes in India

1. **Prediction based Policing-** That with the use of Artificial Intelligence the investigating agencies can many times analyze the place at which the crime is most likely to be committed, can study the common pattern and modus-operandi of the criminal and can take preventive measures to curb the crime before happening. For Example, in Pennsylvania, the Police Study Department had developed a software which is programmed to tell the place by synchronizing the history that where the crime of most likely to happen, which acted as a great assisting hand for the investigating agencies and police in India.

2. **Data Records and Face Recognition**[2]**-**That as widely seen in almost all cases that the Investigating Agencies and Police while investigating any case, collects the images of the perpetrators of crime from the various CCTV Cameras installed at public places, then through using the Face Recognition Technique the images are collected in the database and the criminal is recognized making it extremely easy for police personnel to trace and catch the criminal, this whole operation is not possible to be performed without the support of AI driven tools and software. That in the most recent times, the Delhi Police has widely used this technique to identify the criminals involved in protesting at Delhi Red Fort on 26 January 2021, which has greatly benefitted the police authorities to catch the criminal with great ease.

3. **Forensic Investigations-**That the Artificial Intelligence has greatly assisted the Investigating Agencies in collecting and validating the evidences through forensic department like fingerprint, ossification

[2]Amber Sinha, *The Landscape of Facial Recognition Technologies in India,*TechPolicy, (last visited on 07/01/2025 on 08:25 AM), (https://www.techpolicy.press/the-landscape-of-facial-recognition-technologies-in-india/)

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue V May 2025

tests, poison contaminants, etc. That through AI tools the forensic team is well equipped with technology to identify the evidences with great pace and easily trace the criminal.

4. **Release Decisions-** That the prisoners who are convicted and the under-trial prisoners who's fate is not decided yet by the courts, are to be released on bail or parole for which the Artificial Intelligence plays a major role, that many times the AI Tools identifies the percentage of risk which is involved in releasing a particular convict or prisoner on parole or bail as the case may be. In this inclination, the United States of America (USA) has employed a software named as Westcoin Data Collaborative (WDC) which conducts a bottom-line risk assessment for granting parole or bail to any person, with further analyzing the tenure for which the parole or bail is granted.

Ethical Considerations and Responsibilities in Using Artificial Intelligence in India

That is an acknowledged fact that the robust use of artificial intelligence by the investigating agencies and police authorities in India has widely contributed to the society, with not only making the investigation and meeting ends of justice more transparent but also quick, however with the growing use and sphere of AI based investigations and policing in India, there are some serious ethical considerations regarding it's use, which should be handled and dealt very meticulously in order to prevent it's misuse resulting into unwarranted hardships to the common man of the nation.

That the most common ethical factor involved in the use of AI based policing using Face Recognition Technology (FRT) is that, sometimes due to mismatch of algorithms and combinations, it draws a wrong conclusion or misidentifies the suspect, who is then harassed by the police personnel despite of not having any default on his part, the main issue is regarding the paucity of accountability of artificial intelligence or any person handling the use of the same, which completely defeats it's purpose in case a wrong culprit is identified or a case is registered against him on the basis of the wrong conclusion drawn by the AI based policing.

That in India where the issue of police atrocities is at it's top, and we can hear about the cases on daily basis where the police misuses it's power to harass and individual or physically injuring him in the police station with a motive of extortion by intimidating him for registration of false cases against him, under such circumstances depending solely upon the conclusion formed by the AI based mechanism may lead to unwarranted prosecution and malicious action by the police officials on the common and innocent citizen of the country.

That recently in the State of Uttar Pradesh 41 children were illegally detained and beaten up for protesting against the Citizen Amendment Act, who were identified through CCTV Cameras by using the FRT[3], apart from it recently in 2023 at Manipur Ethic Conflict[4] the police totally failed to maintain the law and order of the state and after the wide-spread circulation of the videos in which the uncontrolled mob crossed all it's limits which shock the conscience of the nation, police and CBI came into action and registered FIR's.

That amid such incidents, shaking confidence on the authenticity and genuineness of the conclusion reached through AI tools is quite obvious, for which some safety parameters have to be complied with by the investigating authorities which includes:

- Establishing an accountable mechanism for AI based policing and mechanism, and
- Genuine and reliable evidence must be tried to be collected, rather than solely depending on the conclusions and results of AI based tools, and
- Introducing and Incorporating software and algorithms to prevent wrongful or erring conclusions, and

[3]SCROLL, https://scroll.in/article/952964/up-police-detained-41-children-during-caa-protests-some-were-tortured-says-citizens-report (last visited on 07/01/2025)

[4]STUDYIQ, https://www.studyiq.com/articles/manipur-conflict/?utm_source=google&utm_medium=cpc&utm_campaign=20420166717&utm_term=_____c&utm_content=__&gad_source=1&gclid=CjwKCAiAm-67BhBlEiwAEVftNmaC5l3lQScI0ImFHMXw3j2nOTMRDmC513NPzJRg3ZOwkZ3x_JFggxoCiTcQAvD_BwE (last visited on 07/01/2025)

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue V May 2025

- Setting up a grievance redressal mechanism to deal with the complaints related to AI usage or victimization due to the improper results of AI, and
- Ensuring Compliance with safety standards and ethical standards of AI.

Probably implementation of these measures will prevent or to a major extent will reduce the plausible misuse of AI in policing and investigations, which will result in establishment of a responsible Artificial Intelligence Mechanism in real sense.

Suggestions for Building a Responsible Artificial Intelligence in India

That establishing a responsible artificial intelligence in every facet and policing is need of the hour, as the policing is directly concerned with the law and order and imbibes paramount consideration with the fundamental rights (guaranteed under PART III of the Constitution of India) of a citizen, therefore some constructive suggestions based on the personal research of the author are as follows:

1) That enacting a statutory framework is acute and extremely important for not only eliminating the chances of perpetuating biases, but also for establishing a responsible, efficient and efficacious artificial intelligence-based system in India.
2) That considering the Right to Privacy while implementing AI based policing is also significantly important as because, after the judicial pronouncement in *K.S. Puttaswamy vs. Union of India, 2017* the Privacy Rights are regarded as Fundamental Rights of the individual under Article 21 of the Constitution, therefore over surveillance or intruding AI technologies should be avoided.
3) That liability should be fixed for the biasness or discriminatory conclusions of AI in policing and investigations, as because it directly affects the fundamental rights and curtails the freedom of a person, building software to mitigate the erroneous conclusion or imparting expert level training to the personnel handling the AI should be implemented to bring an acknowledgeable improvement for the problem.
4) That setting up a grievance redressal mechanism to report incidents of misuse of AI or victimization or wrongful conclusions or unnecessary perpetuating should be established so that the common person can report such events before the concerned supervisory authority and a check and balance on the use of AI can be ensured.
5) That making people aware through campaigns and social media regarding the use of AI and benefits of AI, along-with the complaint procedure should be done, so that the overall confidence of general public on the use of AI can be restored or enhanced to a remarkable level.

CONCLUSION

That from all the following research algorithms, one thing is aptly clear that the Artificial Intelligence is the pre-requisite of human conscience in today's era, as because in the absence of which the human development and providing ease to a common person of the society is impossible.

However as well said by L.R. Knost that "*Every Coin has Two Sides*", which means that every experiment or thing has two plausible outcomes, one is good and one is bad, similarly the widespread use of AI in India or across the globe has different experiences and issue which has be handled with utmost care and caution, in which the basic requisite essential in eliminating it's misuse is to enact a legislation covering AI within the boundaries of legal analogy and secondly to make people aware regarding uses and benefits of AI, in which line the NITI Aayog has introduced the National Program for Artificial Intelligence (NPAI) which widely elucidates the features and benefits of AI to the common public, ultimately raising awareness among with common citizens of the country, and strengthening the very foundation and roots of AI in India, which is an appreciable job.

That as explained in the paper, the AI has widely contributed the investigating agencies in dealing with the cyber-crimes and investigations in India, with the same pace it has connected families and has established an inter-departmental harmony among the various ministries and organizations of India, which is commendable

ISSN No. 2321-2705 | DOI: 10.51244/IJRSI |Volume XII Issue V May 2025

and priceless, however a more pragmatic, reasonable and meticulous use of the same is to ensured by human efforts, which is awaited.

Therefore, it can hopefully be said that, in the coming time the Government of India and State Governments will definitely take a call to bring the AI within a legal framework and will form policies and rulings restricting the use of AI for illegal purposes, with making the present structure of AI more compatible and suitable than today.

REFERENCES

1. Coursera, https://www.coursera.org/articles/what-is-artificial-intelligence (last visited on 08/01/2025)
2. Control Risks, https://www.controlrisks.com/our-thinking/insights/how-artificial-intelligence-is-lowering-the-barrier-to-cybercrime (last visited on 07/01/2025)
3. Innefu, https://www.innefu.com/blog/how-artificial-intelligence-in-policing-helps-crime-detection (last visited on 07/01/2025)
4. The Hindu, https://www.thehindu.com/business/openai-private-study-finds-ai-in-education-to-be-a-major-risk-in-india-but-experts-disagree/article69028993.ece (last visited on 07/01/2025)
5. NITI Aayog, https://www.niti.gov.in/sites/default/files/2023-03/National-Strategy-for-Artificial-Intelligence.pdf (last visited on 08/01/2025)