IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, December 2025
Impact Factor: 7.67

AI-Driven Cyber Crimes and The Limitation of the IT Act, 2000

Adv. C S Suraj
LL.M. Student at School of Law,
Ramaiah University of Applied Science, Bangalore
Specializing in AI, Cyber Crime & Law

Abstract: *Artificial Intelligence has become an essential part of modern digital systems and services. It is widely used in areas such as communication, banking, governance, and education. While AI has improved efficiency and innovation, it has also introduced new forms of cybercrime. Cybercriminals now use AI technologies to commit offences. These AI-driven cybercrimes are more advanced, scalable, and difficult to detect than traditional cyber offences, posing serious risks to individuals, businesses, and national security. In India, cyber offences are primarily governed by the Information Technology Act, 2000. This law was enacted at a time when artificial intelligence and related technologies were not developed or widely used. As a result, the IT Act mainly addresses basic cybercrimes, and does not specifically recognize or regulate AI-based cyber offences. The absence of clear definitions and provisions related to AI-generated crimes, deepfakes, and autonomous cyber systems creates significant legal gaps in the current framework. This article examines the growing threat of AI-driven cybercrimes and critically analyses the limitations of the IT Act, 2000 in addressing these challenges. It highlights the need for legal reforms, clearer AI-specific provisions, improved enforcement mechanisms, and stronger cybersecurity awareness. The study concludes that updating India's cyber laws is essential to effectively combat AI-enabled cybercrime and to ensure digital safety in an increasingly technology-driven society.*

Keywords: Artificial Intelligence (AI), AI-Driven Cybercrime, Cyber Law, Information Technology Act, 2000, Deepfake Technology, Digital Fraud, Cyber Security, Automated Cyber Attacks, Data Protection, Legal Challenges in Cybercrime

I. INTRODUCTION

The rapid growth of digital technology has completely changed the way people live, work, and communicate. The internet, smartphones, and digital platforms have made information easily accessible and services faster than ever before. In recent years, Artificial Intelligence (AI) has become one of the most powerful technologies shaping the digital world. AI is now used in banking, healthcare, education, governance, surveillance, social media, and e-commerce. While these developments have brought great convenience and efficiency, they have also created new risks and challenges, especially in the area of cybercrime.

One of the most serious concerns with AI-based cybercrime is that it closely imitates human behaviour. AI systems can learn from data, predict responses, and adapt their methods to avoid detection. For example, AI-generated phishing emails look almost identical to genuine messages, making it difficult for ordinary users to recognize fraud. Deepfake technology can produce fake videos or audio recordings that appear real, leading to identity theft, blackmail, reputational damage, and financial loss. Such crimes can affect individuals, businesses, and even democratic institutions, thereby posing a threat to national security.

In India, the primary legislation dealing with cybercrime and electronic transactions is the Information Technology Act, 2000. This Act was enacted to provide legal recognition to electronic records, digital signatures, and online transactions. It also introduced provisions to punish cyber offences such as hacking, data theft, and damage to computer systems. At the time of its enactment, the IT Act was a progressive step towards regulating cyberspace and promoting digital

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, December 2025
Impact Factor: 7.67

governance. However, the technological environment of the year 2000 was very different from today's AI-driven digital ecosystem.

When the IT Act, 2000 was drafted, artificial intelligence, machine learning, deepfakes, and automated cyber tools were either non-existent or at a very early stage of development. As a result, the Act was designed mainly to deal with traditional cyber offences committed directly by human actors. Although the Act has been amended over time, it still does not contain clear and specific provisions to address crimes committed using advanced AI technologies. This creates a significant gap between modern cyber threats and the legal framework meant to control them.

In this context, it becomes essential to examine whether the existing legal framework is capable of addressing the realities of modern cybercrime. This article aims to study the nature and growth of AI-driven cybercrimes and critically analyse the limitations of the Information Technology Act, 2000 in responding to these emerging threats. It seeks to highlight the legal gaps, enforcement challenges, and the urgent need for reform in India's cyber law regime. By doing so, the article emphasizes the importance of updating laws to ensure digital safety, protect individual rights, and maintain trust in the digital ecosystem.

Artificial Intelligence (AI)

Artificial Intelligence, commonly known as AI, refers to the ability of machines and computer systems to perform tasks that normally require human intelligence. These tasks include learning from experience, understanding language, recognizing images, solving problems, and making decisions. In simple terms, AI enables machines to think and act in a way that is similar to humans, but with much greater speed and accuracy. AI works by using data, algorithms, and computing power. An algorithm is a set of instructions that tells a computer how to process information. AI systems are trained using large amounts of data so that they can identify patterns and improve their performance over time. Unlike traditional computer programs, which follow fixed rules, AI systems can adapt and learn from new information. This learning ability makes AI more powerful and flexible. There are different types of AI. **Narrow AI** is designed to perform a specific task, such as voice assistants, facial recognition systems, or recommendation systems used by online platforms. **General AI**, which is still mostly theoretical, would have the ability to perform any intellectual task that a human can do. At present, most AI systems used in daily life fall under narrow AI. AI is widely used in many fields. In healthcare, AI helps in diagnosing diseases and analysing medical images. In banking, it is used to detect fraud and manage customer services. In education, AI supports online learning platforms and personalized learning. AI is also used in law enforcement, transportation, social media, and cybersecurity. These applications improve efficiency and reduce human effort. However, AI also raises concerns. Because AI systems depend on data, they can misuse personal information if not properly regulated. AI can also be used for harmful purposes, such as surveillance, manipulation, and cybercrime. When AI is used without ethical guidelines or legal control, it can threaten privacy, security, and trust in digital systems. In conclusion, Artificial Intelligence is a powerful technology that allows machines to perform intelligent tasks by learning from data. While AI offers many benefits, it must be used responsibly and governed by proper laws to ensure that it serves human welfare and does not cause harm.

Cybercrime

Cybercrime refers to any illegal activity that is carried out using computers, mobile phones, the internet, or other digital devices. In simple words, cybercrime is a crime where technology or the internet is used as a tool to commit unlawful acts. These crimes can be committed against individuals, organizations, or even governments. Cybercrime includes a wide range of activities. Common examples are hacking into computer systems without permission, stealing personal or financial information, online fraud, identity theft, spreading computer viruses, and sending fake emails or messages to cheat people. Cybercrimes can also involve cyberstalking, online harassment, and the misuse of social media platforms. With the increasing use of digital technology in daily life, the number and types of cybercrimes have also increased. One important feature of cybercrime is that it can be committed from anywhere in the world. A cybercriminal does not need to be physically present near the victim. Using the internet, a person can target victims across cities, countries, or continents. This makes cybercrime difficult to detect, investigate, and punish. The anonymity provided by digital platforms also allows criminals to hide their identity. Cybercrime causes serious harm to individuals and society. Victims

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, December 2025
Impact Factor: 7.67

may suffer financial loss, emotional stress, damage to reputation, and loss of privacy. Businesses may face data breaches, financial damage, and loss of customer trust. Governments may face threats to national security and public safety through cyber espionage and cyber terrorism. To deal with cybercrime, many countries have enacted special cyber laws. In India, the Information Technology Act, 2000 is the main law that addresses cyber offences. However, as technology continues to evolve, cybercriminals use more advanced tools, making it necessary to continuously update laws and security measures.

In conclusion, cybercrime is a growing problem in the digital age. As dependence on technology increases, protecting individuals and systems from cybercrime becomes essential. Strong laws, public awareness, and effective enforcement are necessary to control cybercrime and ensure digital safety.

AI-Driven Cybercrime

AI-driven cybercrime refers to cyber offences in which criminals use Artificial Intelligence (AI) tools or systems to carry out illegal activities in the digital space. In simple terms, it is a form of cybercrime where AI is used to plan, execute, or improve criminal actions using computers, the internet, or digital networks. These crimes are more advanced and dangerous than traditional cybercrimes because AI systems can work automatically, learn from data, and adapt to different situations. In AI-driven cybercrime, AI is used to imitate human behaviour and decision-making. For example, AI can generate realistic fake emails, messages, voices, or videos that appear genuine. This makes it easier for criminals to deceive victims and steal personal information, money, or sensitive data. AI tools can also analyse large amounts of data to identify weak points in computer systems and exploit them without direct human control. One key feature of AI-driven cybercrime is **automation**. Once an AI system is set up, it can attack thousands of targets at the same time with little effort from the criminal. Another important feature is **adaptability**. AI systems can learn from past attacks and change their methods to avoid detection by security software. This makes AI-based cybercrimes harder to identify and stop. Common examples of AI-driven cybercrime include AI-powered phishing attacks, deepfake videos and voice cloning used for fraud, automated hacking, intelligent malware, and large-scale financial scams. These crimes can cause serious harm such as financial loss, identity theft, damage to reputation, and violation of privacy. AI-driven cybercrime also creates legal and enforcement challenges. It is often difficult to identify who is responsible for the crime, whether it is the programmer, the user, or the organization controlling the AI system.

In conclusion, AI-driven cybercrime is a serious and growing threat in the digital age. While AI offers many benefits, its misuse for criminal purposes highlights the need for stronger laws, better cybersecurity measures, and greater public awareness to protect individuals and society.

AI-Driven Cybercrimes:

Nature and Types

The rapid development of Artificial Intelligence has changed the nature of cybercrime in a significant way. Traditional cybercrimes were mostly manual and required direct human involvement. In contrast, AI-driven cybercrimes rely on intelligent systems that can learn, adapt, and operate automatically. These crimes are more sophisticated, faster, and capable of causing large-scale damage. Understanding the nature and different types of AI-driven cybercrimes is essential to address the legal and security challenges they create.

Nature of AI-Driven Cybercrimes

AI-driven cybercrimes have certain distinct characteristics that differentiate them from traditional cyber offences. First, these crimes are **highly automated**. AI systems can carry out attacks without constant human control. Once programmed, they can run continuously, targeting thousands of victims at the same time. This makes AI-based crimes more efficient and difficult to stop. Second, AI-driven cybercrimes are **adaptive in nature**. AI systems can analyse responses from victims or security systems and change their methods accordingly. For example, AI-powered malware can modify its behaviour to avoid detection by antivirus software. Third, these crimes involve **high levels of impersonation and deception**. AI can imitate human voices, faces, writing styles, and online behaviour. This makes frauds and scams appear genuine, reducing the chances of detection by users. Fourth, AI-based cybercrimes are often **cross-border and**

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, December 2025
Impact Factor: 7.67

anonymous. AI tools can operate through servers located in multiple countries, making it difficult to identify the real location of the criminal. This creates jurisdictional and enforcement problems for law enforcement agencies. Finally, AI-driven cybercrimes pose a **serious threat to privacy, trust, and security**. The misuse of AI technologies can lead to mass surveillance, misuse of personal data, financial losses, and damage to individual reputation.

Types of AI-Driven Cybercrimes

AI-driven cybercrimes take many forms. Some of the most common and dangerous types are;

1. AI-Powered Phishing and Social Engineering Attacks

AI has greatly improved phishing attacks. Traditional phishing involved sending the same fraudulent message to many people. AI-powered phishing systems analyse user data from social media, emails, and online behaviour to create personalized messages. These messages appear genuine and are tailored to each victim, making them difficult to identify as scams. AI chatbots are also used to communicate with victims in real time and manipulate them into sharing sensitive information.

2. Deepfake and Identity Impersonation Crimes

Deepfake technology uses AI to create realistic fake videos, images, or audio recordings. Criminals use deepfakes to impersonate public figures, company executives, or private individuals. Such crimes can result in financial fraud, blackmail, reputational harm, and political manipulation. Voice cloning is commonly used to trick employees into transferring money or sharing confidential information.

3. AI-Based Malware and Ransomware

AI-enabled malware can learn how security systems work and modify itself to avoid detection. Unlike traditional malware, AI-based malware can identify weak points in a system and attack them intelligently. AI-powered ransomware can also decide which data is most valuable and demand higher ransom amounts. This makes cyberattacks more damaging and difficult to control.

4. Automated Hacking and Password Attacks

AI tools are used to automate hacking activities such as password cracking and system intrusion. AI systems can test millions of password combinations in a short time and analyse user behaviour to predict passwords. This increases the success rate of cyberattacks on personal accounts, banking systems, and corporate networks.

5. AI-Driven Financial Fraud

AI is widely used in financial cybercrime. Criminals use AI to analyse transaction patterns and bypass fraud detection systems. AI-generated fake documents, emails, and identities are used to commit online banking fraud, credit card fraud, and cryptocurrency scams. These crimes cause heavy financial losses to individuals and institutions.

6. Data Theft and Privacy Violations

AI tools are used to collect, analyse, and misuse large amounts of personal data. Criminals exploit AI to scrape data from online platforms and use it for identity theft, profiling, and targeted scams. Such activities seriously threaten individual privacy and data security.

II. IT ACT, 2000: AN OVERVIEW

The **Information Technology Act, 2000 (IT Act)** is India's main law that governs the use of computers, the internet, and digital communication. It was enacted to give legal recognition to electronic records and electronic transactions and to deal with offences committed in cyberspace. Before the IT Act came into force, Indian laws were mainly designed for paper-based records and traditional forms of communication. As digital technology began to grow rapidly, there was a need for a separate legal framework to regulate electronic activities and prevent misuse of technology. The IT Act came into effect on **17 October 2000** and marked a major step towards the development of cyber law in India. It provided legal

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, December 2025
Impact Factor: 7.67

support for electronic commerce, online governance, and digital communication. At the same time, it introduced provisions to control cybercrime and protect computer systems from unauthorized access and misuse.

Need for the IT Act, 2000

The increasing use of computers and the internet created new types of crimes that could not be effectively addressed under traditional laws such as the Indian Penal Code. Crimes like hacking, online fraud, data theft, identity misuse, and spreading malicious software required specific legal attention. The IT Act was introduced to fill this gap and to ensure that activities in cyberspace were properly regulated.

Another important reason for introducing the IT Act was to promote **e-commerce and e-governance**. Digital transactions needed legal recognition so that electronic contracts and records could be treated as valid in law. The Act was also influenced by international standards, especially the **UNCITRAL Model Law on Electronic Commerce**, to ensure global compatibility.

Objectives of the IT Act

The Information Technology Act, 2000 was enacted with the following objectives:

- To provide **legal recognition** to electronic records and digital signatures
- To promote **online transactions and electronic commerce**
- To support **electronic governance** and digital service delivery
- To prevent and punish **cybercrimes**
- To ensure **security of computer systems and digital data**
- To establish legal mechanisms for **investigation and dispute resolution**

These objectives show that the IT Act aims not only to control cybercrime but also to encourage the growth of digital technology in a safe and secure manner.

Scope and Applicability of the Act

The IT Act applies to the whole of India and also has **extraterritorial application**. This means that offences committed outside India can still be punished under the Act if the computer system or network involved is located in India. This provision is important because cybercrimes often involve multiple countries.

The Act applies to individuals, companies, government departments, and intermediaries such as internet service providers and digital platforms. However, certain documents such as wills, power of attorney, trust deeds, and negotiable instruments (except cheques) are excluded from its scope.

Key Features of the IT Act

One of the most important features of the IT Act is that it gives **legal validity** to electronic records and digital signatures. This allows electronic documents to be accepted as evidence in courts and enables secure online transactions. The Act also defines various **cyber offences** and prescribes penalties for them. These offences include unauthorized access to computer systems, data theft, identity theft, online cheating, violation of privacy, and publication of obscene content. The Act empowers law enforcement agencies to investigate cyber offences and take necessary action. The **Information Technology (Amendment) Act, 2008** strengthened the Act by introducing new offences such as identity theft and cyber terrorism and by expanding the scope of existing provisions.

Important Sections of the IT Act, 2000 Related to Cybercrimes

The Information Technology Act, 2000 contains several provisions that specifically deal with cyber offences. These sections define different types of cybercrimes and prescribe punishments to prevent misuse of computer systems and digital platforms. Some of the most important sections related to cybercrime are explained below.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, December 2025
Impact Factor: 7.67

Section 43 – Unauthorized Access and Damage (Civil Liability)
Section 43 deals with unauthorized access to computer systems and networks. It applies when a person accesses a computer without permission, copies or downloads data, introduces viruses, disrupts services, or damages computer systems. This section mainly provides civil liability, meaning the offender may be required to pay compensation to the affected person.

Section 66 – Computer-Related Offences (Criminal Liability)
Section 66 applies when acts listed under Section 43 are done dishonestly or fraudulently. It converts civil wrongs into criminal offences. This section covers hacking, data theft, and damage to computer systems. Punishment may include imprisonment or fine, or both.

Section 66B – Receiving Stolen Computer Resources
This section punishes any person who dishonestly receives stolen computer resources or communication devices, knowing that they are stolen. It is applicable in cases involving stolen data, computers, or digital devices.

Section 66C – Identity Theft
Section 66C deals with identity theft. It includes fraudulent use of another person's password, digital signature, biometric information, or unique identification features. This section is important in cases of online impersonation and fraud.

Section 66D – Cheating by Personation Using Computer Resources
This section addresses online cheating by impersonation. It includes offences such as phishing, fake emails, online scams, and frauds where a person pretends to be someone else using digital means.

Section 66E – Violation of Privacy
Section 66E protects an individual's privacy. It punishes unauthorized capturing, publishing, or transmitting of private images of a person without consent. This section is relevant in cases of online harassment and misuse of personal images.

Section 66F – Cyber Terrorism
Section 66F deals with cyber terrorism. It covers acts that threaten the sovereignty, integrity, security, or public order of India through digital means. Punishment under this section is severe, including life imprisonment.

Section 67 – Publishing Obscene Content
Section 67 punishes the publishing or transmitting of obscene material in electronic form. It aims to control misuse of digital platforms for spreading harmful content.

Section 67A – Publishing Sexually Explicit Content
This section deals with publishing or transmitting sexually explicit material in electronic form. It prescribes stricter punishment than Section 67.

Section 67B – Child Pornography
Section 67B specifically deals with publishing, browsing, or transmitting material involving children in sexual acts. It aims to protect children from online sexual exploitation.

Section 69 – Government Powers to Intercept Information
Section 69 authorizes the government to intercept, monitor, or decrypt digital information for reasons related to national security, public order, or prevention of crime. Failure to assist authorities may result in punishment.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, December 2025
Impact Factor: 7.67

Section 72 – Breach of Confidentiality and Privacy

This section punishes unauthorized disclosure of personal information by any person who has access to such information under lawful authority. It protects confidentiality and privacy.

Section 75 – Extraterritorial Application

Section 75 extends the application of the IT Act to offences committed outside India if the computer system or network involved is located in India. This is important for cross-border cybercrimes.

Importance of the IT Act in the Digital Age

The IT Act has played a crucial role in India's digital development. It has enabled online banking, digital payments, e-commerce, and e-governance by creating trust in electronic systems. Without this law, the growth of the digital economy would not have been possible. However, with rapid advancements in technology such as artificial intelligence and automated cyber tools, the Act now appears limited in addressing modern cyber threats. This highlights the need for updating cyber laws to meet present-day challenges.

III. LIMITATIONS OF THE IT ACT, 2000

The Information Technology Act, 2000 was enacted to regulate electronic communication, promote digital governance, and control cybercrime in India. At the time of its enactment, the Act was progressive and addressed the emerging challenges of the digital age. However, technology has advanced rapidly over the last two decades, especially with the rise of artificial intelligence (AI), automated systems, and data-driven technologies. As a result, several gaps and weaknesses have emerged in the IT Act, making it less effective in dealing with modern cyber threats. The major limitations of the Act are discussed below.

1. Outdated Legal Framework

One of the most significant limitations of the IT Act is that it is based on the technological realities of the early 2000s. When the Act was drafted, technologies such as artificial intelligence, machine learning, deepfakes, automated hacking tools, and algorithm-based decision-making systems were either non-existent or not widely used. As a result, the Act mainly addresses traditional cyber offences like hacking, data theft, and unauthorized access, and does not reflect the complexity of modern cybercrimes.

2. Lack of AI-Specific Provisions

The IT Act does not contain any specific provisions dealing with AI-driven cybercrimes. Crimes such as deepfake fraud, AI-generated impersonation, automated phishing attacks, and self-learning malware are not clearly defined under the Act. These offences are often forced to fit into existing sections, which leads to legal uncertainty and weak prosecution. The absence of clear definitions and regulations for AI systems makes it difficult to regulate the misuse of AI technologies. There are no provisions dealing with algorithmic accountability, ethical use of AI, or transparency in automated decision-making, which are crucial in the modern digital environment.

3. Unclear Liability and Accountability

Another major weakness of the IT Act is the lack of clarity regarding liability in AI-based crimes. Traditional criminal law assumes that offences are committed by human beings with clear intent. However, in AI-driven cybercrimes, it becomes difficult to determine who should be held responsible—the developer of the AI system, the user who deployed it, the organization controlling it, or the platform hosting it. The IT Act does not provide guidelines on assigning responsibility in cases involving autonomous or semi-autonomous AI systems. This creates confusion for law enforcement agencies and courts while deciding criminal intent and liability.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, December 2025
Impact Factor: 7.67

4. Enforcement Challenges

Effective enforcement of the IT Act remains a serious challenge. Investigating modern cybercrimes requires advanced technical knowledge, digital forensic tools, and trained personnel. However, many law enforcement agencies in India lack adequate infrastructure and expertise to deal with sophisticated cyber offences, especially those involving AI and automation. The slow pace of investigation and prosecution further weakens the deterrent effect of the Act. Cybercrime cases often take years to resolve, reducing public trust in the legal system.

5. Jurisdictional and Cross-Border Issues

Cybercrimes are often committed across national borders, involving servers, platforms, and perpetrators located in different countries. Although Section 75 of the IT Act provides for extraterritorial jurisdiction, enforcing this provision in practice is difficult. International cooperation in cybercrime investigation is slow and complex, and differences in legal standards across countries further complicate matters. The IT Act does not provide clear mechanisms for effective cross-border coordination, making it challenging to investigate and prosecute international cyber offences.

6. Inadequate Data Protection and Privacy Safeguards

The IT Act does not provide a comprehensive data protection framework. Although some provisions address privacy and confidentiality, they are limited in scope. With the rise of AI technologies that rely heavily on personal data, stronger data protection laws are essential. The lack of clear safeguards increases the risk of data misuse, surveillance, and privacy violations.

7. Weak Regulation of Intermediaries

While the IT Act includes provisions for intermediary liability, the responsibilities of online platforms in controlling AI-generated harmful content are not clearly defined. This leads to inconsistent enforcement and confusion regarding the role of intermediaries in preventing cybercrime.

In conclusion the Information Technology Act, 2000 laid the foundation for cyber law in India, but it is no longer fully equipped to address the challenges of modern, AI-driven cybercrimes. The lack of AI-specific provisions, unclear liability rules, enforcement difficulties, jurisdictional limitations, and weak data protection measures reduce its effectiveness. To ensure digital safety and legal certainty, there is an urgent need to update the IT Act or introduce a new comprehensive legal framework that addresses artificial intelligence, emerging technologies, and advanced cyber threats.

IV. COMPARATIVE LEGAL APPROACHES: INTERNATIONAL PERSPECTIVE ON AI-DRIVEN CYBERCRIMES

Cybercrime is a global problem that does not respect national borders. With the increasing use of artificial intelligence in cyber offences, many countries have begun to update their legal frameworks to address new technological risks. A comparative study of international laws and best practices helps in understanding how different jurisdictions deal with AI-driven cybercrimes and highlights areas where India's Information Technology Act, 2000 can be improved. The legal approaches of the **European Union (EU)** and the **United States (USA)** are particularly important due to their advanced digital economies and evolving cyber laws.

European Union (EU)

The European Union follows a rights-based and preventive approach towards digital regulation and cybercrime. Rather than relying on a single cyber law, the EU has adopted multiple regulations and directives that together create a strong legal framework for dealing with cyber threats, including AI-driven crimes. One of the most significant EU laws is the **General Data Protection Regulation (GDPR)**. GDPR provides strong protection for personal data and places strict obligations on organizations that collect or process data. Since AI systems heavily depend on large amounts of data, GDPR indirectly regulates AI misuse by ensuring transparency, consent, and accountability. Heavy penalties under GDPR act as a strong deterrent against data misuse and privacy violations. Another important legal instrument is the **EU Cybersecurity Act**, which strengthens the role of the European Union Agency for Cybersecurity (ENISA). It promotes

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, December 2025
Impact Factor: 7.67

coordinated responses to cyber threats across member states and encourages the development of cybersecurity standards. This helps in addressing large-scale and cross-border cyber-attacks. The EU has also taken a pioneering step by introducing the **Artificial Intelligence Act (AI Act)**. This proposed legislation classifies AI systems based on risk levels and imposes stricter obligations on high-risk AI applications. The AI Act focuses on transparency, human oversight, and accountability, making it highly relevant for preventing AI-driven cybercrimes such as deepfake manipulation and automated fraud.

United States (USA)

The United States follows a more decentralized and sector-specific approach to cybercrime regulation. Instead of a single comprehensive cyber law, the USA relies on a combination of federal and state laws, along with regulatory guidelines and enforcement by agencies. The **Computer Fraud and Abuse Act (CFAA)** is the primary federal law dealing with cybercrime in the USA. It criminalizes unauthorized access to computer systems and data theft. Although CFAA does not specifically mention AI-driven cybercrime, it is flexible enough to cover many technology-based offences. The USA also focuses strongly on **cybersecurity standards and enforcement**. Agencies such as the Federal Trade Commission (FTC) play a key role in regulating unfair and deceptive digital practices, including misuse of AI technologies. The FTC has taken action against companies using AI systems in misleading or harmful ways. In recent years, the USA has introduced AI-specific guidelines and executive policies rather than strict legislation. These policies emphasize ethical AI development, transparency, and risk management. While this approach allows innovation to continue, it sometimes lacks the clarity and consistency of binding laws.

International Best Practices and Global Cooperation

Apart from the EU and USA, several international frameworks provide guidance on combating cybercrime. The **Budapest Convention on Cybercrime**, adopted by the Council of Europe, is the first international treaty aimed at addressing internet and computer-related crimes. It promotes international cooperation, harmonization of laws, and efficient investigation of cross-border cyber offences. Global organizations emphasize the importance of capacity building, information sharing, and cross-border cooperation to combat cybercrime effectively. These practices are essential in dealing with AI-driven cybercrimes that operate across multiple jurisdictions.

Comparison with India's IT Act, 2000

Compared to the EU and USA, India's IT Act, 2000 appears limited in scope. While the Act provides a basic framework for cybercrime, it lacks AI-specific provisions, strong data protection measures, and advanced enforcement mechanisms. Unlike the EU's preventive and rights-based approach, the IT Act largely focuses on punishment after offences occur. The absence of a dedicated AI regulatory framework in India contrasts sharply with the EU's AI Act and GDPR. Similarly, India lacks the flexible enforcement mechanisms seen in the USA, where regulatory agencies actively monitor and regulate digital practices.

V. SUGGESTIONS AND RECOMMENDATIONS

The rapid growth of artificial intelligence and digital technologies has significantly changed the nature of cybercrimes. While the Information Technology Act, 2000 laid the foundation for cyber law in India, it is no longer sufficient to deal with modern AI-driven cyber threats. To ensure effective prevention, regulation, and prosecution of such crimes, several legal and policy reforms are necessary. The following suggestions and recommendations aim to strengthen India's legal framework and improve cyber safety.

1. Updating the Information Technology Act, 2000

One of the most important recommendations is to update the Information Technology Act, 2000 to reflect current technological realities. The Act should be revised to include clear definitions of emerging technologies such as artificial intelligence, machine learning, automated systems, and deepfake technologies. Specific offences related to AI-driven cybercrimes should be expressly recognized under the law. The amended Act should clearly cover crimes such as AI-

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, December 2025
Impact Factor: 7.67

generated impersonation, automated phishing attacks, manipulation of digital content using deepfakes, and AI-based identity fraud. Clear legal provisions will help reduce ambiguity and ensure more effective enforcement.

2. Introduction of AI-Specific Legislation

In addition to updating the IT Act, India should consider enacting a **separate AI-specific law**. Such legislation can focus on regulating the development, deployment, and misuse of artificial intelligence systems. The law should define responsibilities and liabilities of AI developers, users, organizations, and intermediaries. An AI-specific law should include provisions on transparency, human oversight, accountability, and ethical use of AI. It should also establish standards for risk assessment and mandatory safeguards for high-risk AI applications. This approach would help prevent misuse of AI while encouraging innovation.

3. Clear Rules on Liability and Accountability

There is an urgent need to clearly define liability in cases involving AI-driven cybercrimes. The law should clarify who is responsible when an AI system is misused or causes harm. Liability may be shared among developers, operators, and platform providers depending on their level of control and negligence. Clear accountability rules will help courts and law enforcement agencies determine responsibility more effectively and ensure justice for victims of cybercrime.

4. Strengthening Enforcement Mechanisms

Legal reforms alone are not sufficient unless enforcement mechanisms are strengthened. Law enforcement agencies must be provided with advanced technical tools, digital forensic infrastructure, and specialized training to investigate AI-based cybercrimes. Special cybercrime units with expertise in artificial intelligence and data analytics should be established at both central and state levels. Fast-track cybercrime courts may also be introduced to ensure speedy justice.

5. Improving Jurisdiction and International Cooperation

Since AI-driven cybercrimes often operate across national borders, India must strengthen international cooperation mechanisms. This includes entering into bilateral and multilateral agreements for information sharing, joint investigations, and extradition of cyber offenders. Adopting international best practices and aligning domestic laws with global cybercrime conventions will improve India's ability to tackle cross-border cyber threats.

6. Enhancing Data Protection and Privacy Laws

Strong data protection laws are essential in the age of artificial intelligence. India should ensure effective implementation of comprehensive data protection legislation to safeguard personal data used by AI systems. Clear consent mechanisms, data minimization, and accountability standards should be enforced to prevent misuse of personal information.

7. Awareness and Capacity Building

Public awareness plays a crucial role in preventing cybercrime. Regular awareness programs should be conducted to educate citizens about AI-driven cyber threats such as deepfake scams, online fraud, and identity theft. Digital literacy programs should be introduced at school and college levels. Capacity building is equally important for professionals, law enforcement officers, judges, and policymakers. Continuous training programs on emerging technologies and cyber laws will improve understanding and effective application of the law.

II. CONCLUSION

The rapid growth of artificial intelligence has transformed the digital world, bringing both benefits and serious challenges. While AI has improved efficiency, innovation, and connectivity, it has also been misused to commit sophisticated cybercrimes. AI-driven cybercrimes such as automated hacking, identity theft, deepfake manipulation, and online fraud are more complex, faster, and harder to detect than traditional cyber offences. These evolving threats have exposed significant limitations in existing cyber laws, particularly the Information Technology Act, 2000.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 3, December 2025
Impact Factor: 7.67

The IT Act, 2000 played a crucial role in establishing the legal foundation for cyber regulation in India. It provided legal recognition to electronic records, enabled digital transactions, and defined punishments for cyber offences. However, the Act was drafted in an era when artificial intelligence and advanced automated technologies were not widely used. As a result, it lacks specific provisions to address AI-based cybercrimes, clear rules on liability, and effective mechanisms to regulate emerging technologies.

Comparative analysis with international legal frameworks, especially those of the European Union and the United States, shows that modern cyber laws are moving towards preventive regulation, transparency, accountability, and strong data protection. India's cyber legal framework must evolve in a similar direction to remain effective in the digital age.

To address these challenges, there is an urgent need to update the IT Act or introduce AI-specific legislation that clearly defines AI-related offences and responsibilities. Strengthening enforcement mechanisms, improving international cooperation, and enhancing public awareness are equally important. Capacity building among law enforcement agencies, judiciary, and digital users will help ensure better implementation of cyber laws.

In conclusion, combating AI-driven cybercrimes requires a balanced and forward-looking legal approach. Law must evolve alongside technology to protect individuals, institutions, and national security while encouraging responsible innovation. Reforming India's cyber laws is not only necessary but essential to ensure digital safety and justice in the era of artificial intelligence.

REFERENCES

[1]. Information Technology Act, 2000
[2]. Information Technology (Amendment) Act, 2008
[3]. Indian Penal Code, 1860
[4]. UNCITRAL, Model Law on Electronic Commerce, United Nations Commission on International Trade Law, 1996
[5]. Convention on Cybercrime (Budapest Convention), 2001
[6]. General Data Protection Regulation (GDPR), 2018
[7]. European Commission, *Proposal for a Regulation Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*, 2021.
[8]. Computer Fraud and Abuse Act (CFAA), 1986
[9]. National Crime Records Bureau (NCRB), *Crime in India – Cyber Crime Reports*, Government of India
[10]. M P Jain, Indian Constitutional Law
[11]. Ministry of Electronics and Information Technology (MeitY), Government of India, *Cyber Security and Digital Governance Reports*