CYBER SECURITY AND AI: FRAUD AND CRIMES IN SOCIETY

Mridu Joydeb Mukherjee & Mr. Jainendra Kr. Sharma, LL.M., IILM University, Gurugram

ABSTRACT:

When the cyber network came into picture as a source or medium, over the period it also evolved with the new way and techniques to commit crimes. With the slow advancements, it was observed that there is need to introduce laws that will keep a check and balance in the emerging cyber world. The AI i.e. the artificial intelligence is a major part of this cyber world and network which exists both as a boon and bane for the society. As they have expanded, it has also been misused as a platform to perform and initiate new forms and patterns of crimes like forgery, fraud, hacking, etc. Even though we have cyber security laws to safeguard the interest of people but the question arises that is it efficient enough to deal with the evolving cyber-crimes against people or the society? This has also created the threat to people's privacy and 'right to life' which is a basic human right all around the world.

The cyber world and AI have made the life easier but also has led to vulnerabilities and threat without being present in a physical form. It is going to be a challenge as there is a need of more efficient stringent laws and technology to deal with the growing AI and cybercrimes.

CHAPTER-1: INTRODUCTION

This research paper is basic, descriptive, exploratory, and correlational based work in ILI style on Cyber Security and AI: Fraud and Crimes in Society.

The introduction of computer and networks paved a way to world of technology. The term '*Cyber*' means the virtual world that includes the involvement of computer, network, and the internet connection that is used to establish any kind of communication without the need of actual physical presence of any person.

The loop or the imaginative space of this world that connects people through computer system is known as '*cyber space*.' The illicit or illegal activities carried through this virtual space by using the computer, internet and digital devices is known as '*cyber-crime*.'

'*Cyber-security*' is the procedures and technologies intended to shield computers, networks, and data from vulnerabilities, illegal access, and cybercriminal's online attacks.

It seeks to lessen the possibility of cyberattacks and guard against unlawful use of networks, technologies, and systems.

The creation of computer systems that can carry out operations and reaching conclusions that normally call for human intelligence is known as *artificial intelligence, or AI*. It entails developing models and algorithms that let computers determine patterns in data, learn from them, and adjust to new knowledge or circumstances[1].

The question that arises to write on this subject-matter is to understand:

i. **Whether the cyber laws present are efficient and sufficient for remedial?**

ii. **Whether the jurisdiction a challenge in achieving the cyber security?**

iii. **Whether cyber & AI are boon or bane?**

[1]https://www.malwarebytes.com/cybersecurity/basics/risks-of-ai-in-cyber-security

In present, the growing role of cyber and AI in the cybersecurity and for committing crimes is contributing to social engineering in both positive and negative manner.

LITERATURE REVIEW:

1. **TITLE:** A Study on Artificial Intelligence and Cyber Crime in Indian Context

   AUTHOR: Dr. Rashmi Tapan Dubey, Dr. Ujwala Bendale

   MONTH AND YEAR OF PUBLICATION: June 2024

   NAME OF THE JOURNAL: Rabindra Bharati University: Journal of Economics

   ABOUT[2]:

With an emphasis on the Indian legal and societal environment, the paper examines how artificial intelligence (AI) can be both a tool and a threat in the realm of cybercrime. It draws attention to how AI can both improve cybersecurity and be abused for complex cybercrimes. With the proliferation of digital platforms, cybercrime in India is increasing quickly. Phishing, data breaches, identity theft, and AI-generated deepfakes are examples of common crimes. India is currently upgrading its legal system.

According to the paper's conclusion, artificial intelligence (AI) has enormous potential to improve cybersecurity, but when used improperly, it can result in previously unheard-of levels of cybercrime. To effectively address rising cyber dangers, India requires international cooperation in addition to current, strong, and AI-inclusive regulatory frameworks.

2. **TITLE:** Artificial intelligence and criminal liability in India: exploring legal implications and challenges

   MONTH AND YEAR OF PUBLICATION: 11 April 2024

[2]file:///C:/Users/MRIDU%20J.%20MUKHERJEE/Downloads/RashmiDubeyOthers-RBJE_PDF%20(1).pdf (https://www.researchgate.net/)

NAME OF THE PUBLISHER: Cogent social sciences 2024, Vol. 10, no. 1, 2343195

ABOUT[3]:

Artificial Intelligence (AI) has revolutionized industries such as healthcare, banking, and law in India, but it has also brought forth complicated issues in the areas of criminal liability and cybercrime. AI is being used more and more to commit complex crimes, such as financial fraud, data theft, and deepfake production, frequently escaping detection by conventional means. Current Indian laws, such as the Indian Penal Code and the Information Technology Act of 2000, are inadequate to deal with violations specific to artificial intelligence. Because AI systems lack legal personhood and are independent, it is difficult to attribute mens rea (guilty mentality), making the idea of criminal culpability for AI unclear.

3. **TITLE:** Cyber Crime and Criminal Law in the Era of Artificial Intelligence

AUTHOR: Murshal Senjaya (October 2024)

NAME OF THE JOURNAL: International Journal of Law and Society Vol. 1, No. 4

ABOUT[4]:

Artificial Intelligence (AI), which improves the effectiveness of identifying, inquiring into, and prosecuting more skilled cybercriminals, offers the legal system a great deal of promise in combating cybercrime. Although this technology is capable of massive data analysis, pattern recognition, and suspicious behavior identification, the legal system needs to be upgraded to include new offences like automated cyberattacks and AI-based fraud. Law enforcement faces many difficulties in dealing with AI abuse, particularly since there are no laws governing its application to cybercrime.

The efficacy of law enforcement suffers because existing regulations frequently do not address new situations. To overcome these obstacles, lawmakers must revise laws and create moral

[3]https://www.tandfonline.com/doi/epdf/10.1080/23311886.2024.2343195?needAccess=true(Artificial intelligence and criminal liability in India: exploring legal implications and challenges)
[4]https://international.appihi.or.id/index.php/IJLS(e-ISSN : 3046-9562, p-ISSN : 3046-9619, Page 268-276)

standards. International cooperation and the development of law enforcement's capabilities through training and education are also crucial for improving the efficiency of combating cybercrime.

4. **TITLE:** Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions

   AUTHOR: Thomas C King, Nikita Aggarwal, Mariarosaria Taddeo, Luciano Floridi.

   MONTH AND YEAR OF PUBLICATION: 2020

   NAME OF THE PUBLISHER: Springer

   ABOUT[5]:

The goal of artificial intelligence (AI) research and regulation is to strike a balance between the advantages of innovation and any possible risks or disruptions. However, the possible reorientation of AI technology to facilitate criminal acts—referred to in this article as AI-Crime (AIC)—is an unexpected consequence of the recent rise in AI research. Published attempts in automating fraud directed at social media users and evidence of AI-driven manipulation of virtual marketplaces have made AIC potentially possible. The future of AIC is uncertain, nevertheless, as it is still a relatively new field that is by its very nature interdisciplinary, ranging from formal science to socio-legal studies.

This paper presents the first comprehensive, multidisciplinary review of the literature on the predictable risks of AIC, giving ethicists, decision-makers, and law enforcement agencies a summary of the issues at hand as well as a potential area for resolution.

5. **TITLE:** Cybercrime And International Law: Jurisdictional Challenges and Enforcement Mechanisms

[5]https://pmc.ncbi.nlm.nih.gov/articles/PMC6978427/ - Bib1 (Artificial Intelligence Crime: An Interdisciplinary Analysis of Foreseeable Threats and Solutions)

AUTHOR: Tripti Singh (Shree ramswaroop memorial University, Lucknow)

MONTH AND YEAR OF PUBLICATION: September 2024

NAME OF THE JOURNAL: African Journal of Biomedical Research

ABOUT[6]:

Ransomware, cyberterrorism, identity theft, and hacking are all examples of cybercrime. It poses a grave risk to both domestic and global security and influences the economy because of monetary losses, harm to one's reputation, and national security risks. It examines the difficulties in identifying and prosecuting cybercrime in various jurisdictions, draws attention to inconsistencies in legal frameworks, and assesses the efficacy of international agreements and enforcement systems.

CHAPTER-2: BACKGROUND OF CYBER CRIME

Since the introduction and evolvement of the computer and internet, it has paved its way to commit crimes in a new form. This is what we call cyber-crime. There's no such specific time but some events mark cyber-crime events[7]:

- '1962: Allen Scherr's cyberattack against the MIT computer networks, which involved punch card password theft from their database, marked the beginning of the modern era of cybercrime.

- 1971: Bob Thomas at BBN Technologies generated the first computer virus for research reasons. The self-replicating software, known as the Creeper Virus, was discovered on the ARPANET in 1971 and predicted that future viruses would seriously harm computer

[6]https://africanjournalofbiomedicalresearch.com/index.php/AJBR (Afr. J. Biomed. Res. Vol. 27(3s) (September2024); 697-708 Research Article)

[7]https://www.bluevoyant.com/knowledge-center/cybercrime-history-global-impact-protective-measures-2022 (cybercrime-history-global-impact-protective-measures)

systems[8].'

- 1980s–1990s: the development of the internet brought with it the first cybercrimes, such as viruses, hacking, and illegal access. The Morris Worm (1988), one of the first well-known cybercrimes, seriously disrupted the internet.

  'United States v. Morris (1991): A computer software known as a "worm" was released onto the national computer network known as the Internet by a Cornell University graduate student. Due to the worm's quick propagation, numerous computers at military installations and educational institutions crashed or stopped working.

  The Act did not need proof of intent to do harm by impeding allowed usage, according to the U.S. Court of Appeals for the Second Circuit, and Morris's actions were considered "access without authorization"[9].'

  'As the internet and digital technologies grew in popularity in the early 1990s, cybercrime began to appear in India. The Information Technology Act of 2000, the first law to combat cybercrime, was passed in that year[10].'

  When the internet was first launched in India in 1995, there were no laws specifically addressing cyberspace. Traditional laws, such as the Indian Penal Code (IPC), which lacked digital provisions, were used to combat cybercrime.

  The incidents were infrequent and restricted to simple hacking or email spoofing.

- 2000s: Financial fraud, identity theft, and phishing scams increased in tandem with the growth of e-commerce and online banking. Groups involved in organized crime began to

[8]https://arcticwolf.com/resources/blog/decade-of-cybercrime/ (A Brief History of Cybercrime; April 19, 2024; by Arctic Wolf; Cyber Attacks and Breaches)
[9]https://studicata.com/case-briefs/case/u-s-v-morris/#:~:text=In%20U.S.%20v.,to%20crash%20or%20become%20inoperative.(U.S. v. Morris 928 F.2d 504 (2d Cir. 1991))
[10]https://www.nextias.com/blog/cybercrime-in-india/#:~:text=online%20crime%20rates.-,When%20did%20Cybercrime%20start%20in%20India?,evolved%20and%20became%20more%20sophisticated (Cybercrime in India: Types, India's Vulnerability & Solutions; October 22nd, 2024)

shift their activities online.

'Bazee.com Case – *Avnish Bajaj v. State* (2005): Due to an obscene movie that was posted for sale on Bazee.com, the CEO of an e-commerce portal was arrested and later released on bail under Section 67 of the IT Act. Although he shown due diligence, the Information Technology Act of 2005 contained no provisions pertaining to "intermediaries"[11].

- 2010s–Today: Ransomware, nation-state cyberattacks, data breaches, and deepfake-based scams were all made possible by sophisticated tools and international connectivity. Illicit cyber tools and services were sold on the dark web.

'United States v. Vladimir Drinkman (2015): One of the biggest data breaches in history was caused by a Russian hacker who took over 160 million credit card numbers. This instance illustrated how global financial systems could be the target of organized cybercrime.

Drinkman, a Russian national, can now be extradited to the US to face charges after a Dutch court decided in favor of the U.S. Drinkman was charged with playing a major role in a multinational credit card hacking network that obtained personal data from JetBlue and Nasdaq. The court chose to permit Drinkman's extradition to the US to face the accusations, even though he had preferred to be sent to Russia, where his family lived[12].

'Pune Citibank Call Center Fraud (2004, conviction in 2015): One significant incident that took place in 2004 was the Pune Citibank call center fraud case, which concerned an alleged fraud committed from a call center run by Mphasis. Although several people were detained and put on trial, it took a long time for the case to result in convictions; some convictions were finally finalized in 2015. Allegations of fraud and unlawful exploitation of Citibank customers' data were at the center of the lawsuit; charged with criminal

[11]https://www.itlaw.in/avnish-bajaj-vs-state/(Avnish Bajaj vs State (Bazee.com case))

[12]https://www.theguardian.com/world/2015/jan/27/russian-megahacker-vladimir-drinkman-credit-cards-extradition (Court rules accused Russian credit card 'megahacker' can be extradited to the US)

conspiracy under Sections 420 and 120B of the IPC and the IT Act[13].'

CHAPTER-3: INTERNATIONAL CONVENTIONS

'Geographical borders have become less distinct because of the digital revolution, making cross-border cyber activity possible. However, the global problem of cybercrime has also resulted from this unparalleled connectedness, calling for international cooperation[14].'

Key International Cybercrime Treaties[15]:

1. **The Budapest Convention (2001):**

'The first and most extensive international agreement addressing cybercrime is the Budapest Convention, officially known as the Convention on Cybercrime. It was created by the Council of Europe and offers a structure for:

- harmonizing national cybercrime legislation.
- improving methods of investigation.
- enhancing global collaboration.

The treaty, which has more than 60 signatories, including non-European countries like the US, Japan, and Australia, covers crimes like online fraud, data breaches, and illegal access.

Challenges:

- Major powers like China and India have not participated.

[13]https://www.citibank.com/tts/solutions/commercial-cards/fraud-protection/#:~:text=Through%20monitoring%20of%20our%20customers,you%20have%20authorized%20that%20purchase.(Protect Yourself Against Fraud)
[14]https://www.cyberlawconsulting.com/global_cybersecurity_sco_framework.php#:~:text=The%20Budapest%20Convention%2C%20formally%20known,Enhancing%20investigative%20techniques.
[15]https://www.cyberlawconsulting.com/global_cybersecurity_sco_framework.php#:~:text=The%20Budapest%20Convention%2C%20formally%20known,Enhancing%20investigative%20techniques.

- criticized for addressing changing cyberthreats in an antiquated and Eurocentric manner[16].'

***Yahoo! v. LICRA (France, 2000)*:**

'The US is pursuing this action in response to a French court's 2000 ruling that Yahoo, a US search engine and portal, must limit access to Nazi memorabilia auctions and information.

This brought attention to the difference in international cyber laws, which were subsequently resolved by agreements such as the Budapest Convention[17].'

Russia-led Convention[18]:

'Russia recently presented a second agreement called "Countering the use of information and communications technologies for criminal purposes" to the UNGA, or United Nations General Assembly, in contradiction to the Budapest agreement.

China and Russia challenged the Budapest Convention on the grounds of national sovereignty, leading to the creation of the Russia-led Convention.

In terms of cross-border data access, this convention provides more than the Budapest Convention does[19].'

2. The Malabo Convention (2014):

'On June 27, 2014, in Malabo, Equatorial Guinea, the African Union (AU) adopted the Convention on Cyber Security and Personal Data Protection, also referred to as the Malabo Convention. The goal of this historic agreement is to provide a thorough legal framework for electronic transactions, cybersecurity, and the protection of personal data throughout the African continent.

[16]https://www.cyberlawconsulting.com/global_cybersecurity_sco_framework.php#:~:text=The%20Budapest%20Convention%2C%20formally%20known,Enhancing%20investigative%20techniques.
[17]https://wilmap.stanford.edu/entries/yahoo-inc-v-licra (Court Decision United States; Yahoo Inc. v. LICRA)
[18]https://www.cyberlawconsulting.com/global_cybersecurity_sco_framework.php#:~:text=The%20Budapest%20Convention%2C%20formally%20known,Enhancing%20investigative%20techniques.
[19]https://www.cyberlawconsulting.com/global_cybersecurity_sco_framework.php#:~:text=The%20Budapest%20Convention%2C%20formally%20known,Enhancing%20investigative%20techniques.

The Malabo Convention is now in force ten years after it was adopted. According to Article 36 of the Malabo Convention, the pact would take force if 15 ratifications were obtained. After Mauritania ratified the convention in May 2023, it became operative on June 8, 2023, 30 days later[20].'

3. The UN Cybercrime Treaty (Adopted November 2023):

'An important turning point in international attempts to combat cybercrime is the UN Cybercrime Treaty. This treaty, which was approved by the UN General Assembly in November 2023, attempts to create a thorough framework to prevent the use of ICT (information and communication technologies) for illegal activities.

It is anticipated that the treaty will improve international cooperation, particularly for those nations that have not ratified the Budapest Convention.

It encourages more legal uniformity, which lessens jurisdictional disputes in cybercrime investigations.

Challenges:

During discussions, there were disagreements over the pact. Western countries supported the Budapest Convention, while China, Russia, and other poor countries supported the UN-led agreement.

Significant conformity between domestic laws and treaty provisions will be necessary for implementation[21].'

4. Russia-China Bilateral Agreement on Cybersecurity (2015):

'China and Russia inked a bilateral agreement in 2015 to work together to ensure global

[20]https://www.diplomacy.edu/blog/what-is-the-malabo-convention/(What is the Malabo convention? By Diplo alumni Andrew Gakiria and Tevin Mwenda Gitonga)

[21]https://www.cyberlawconsulting.com/global_cybersecurity_sco_framework.php#:~:text=The%20Budapest%20Convention%2C%20formally%20known,Enhancing%20investigative%20techniques.

information security. The following are the main points of this agreement:

- ❖ Fighting Cybercrime
- ❖ Cyberspace Sovereignty of States
- ❖ Cooperation in Information Control[22]'

5. The Russia-China Proposal at the UN:

'The plan is in line with China's and Russia's domestic internet regulations, which support strict censorship and restriction.

Western governments and democratic states argue that the idea might justify internet censorship under the pretext of "cybersecurity," weakening internet freedom and free expression[23].'

6. Russia-China Alignment on the UN Cybercrime Treaty:

'China and Russia were key players in influencing the UN Cybercrime Treaty negotiations, which were adopted in 2023. They promoted:

- "A treaty focused on sovereign control over domestic cyberspace.
- A less intrusive role for international bodies in domestic cyber policies.
- Provisions to counter the use of ICT for "subversive purposes," which critics argue could justify state censorship."

Many other nations, especially in the Global South, who are also concerned about Western

[22]https://www.cyberlawconsulting.com/global_cybersecurity_sco_framework.php#:~:text=The%20Budapest%20Convention%2C%20formally%20known,Enhancing%20investigative%20techniques.
[23]https://www.cyberlawconsulting.com/global_cybersecurity_sco_framework.php#:~:text=The%20Budapest%20Convention%2C%20formally%20known,Enhancing%20investigative%20techniques.

domination in global internet governance, backed their efforts[24].'

7. ASEAN Cybersecurity Cooperation Agreement:

'To improve cooperation among member governments, the Association of Southeast Asian Nations (ASEAN) is pursuing a cybersecurity pact for the whole region. This agreement is anticipated to:

- Encourage the exchange of information.
- Increase smaller countries' cybersecurity capabilities.
- Deal with local cyberthreats such as phishing scams and ransomware attacks.[25]'

8. India's Push for a BRICS Cyber Treaty:

'To combat cyberthreats within the group, India is pushing for a cybercrime framework adapted to the BRICS. This project consists of:

- establishing common rules and regulations.
- promoting cooperation in the development of capabilities.
- tackling international concerns such as data sharing and digital forensics[26].'

CHAPTER-4: INDIAN LEGAL PERSPECTIVE

'The Indian Penal Code, the Companies Act of 2013, the National Cyber Security Policy of 2013, and the Information Technology Act of 2000 of India (IT Act) serve as the main pieces of

[24]https://www.cyberlawconsulting.com/global_cybersecurity_sco_framework.php#:~:text=The%20Budapest%20Convention%2C%20formally%20known,Enhancing%20investigative%20techniques.
[25]https://www.cyberlawconsulting.com/global_cybersecurity_sco_framework.php#:~:text=The%20Budapest%20Convention%2C%20formally%20known,Enhancing%20investigative%20techniques.
[26]https://www.cyberlawconsulting.com/global_cybersecurity_sco_framework.php#:~:text=The%20Budapest%20Convention%2C%20formally%20known,Enhancing%20investigative%20techniques.

legislation to combat these crimes. To regulate and punish cyber-related incidents, Section 66 addresses hacking, Section 67 addresses obscenity, Section 69 addresses computer data interception, and Section 43A addresses data privacy. The dynamic nature of cyber threats, jurisdictional issues, a lack of technical staff in law enforcement organizations, and legal understanding are some of the barriers that prevent efficient cybersecurity enforcement within the legal framework[27].'

According to Section 43 of Chapter IX of the Act, anyone who accesses, downloads, installs a computer virus, or prevents access without the owner of the computer system's consent faces a fine of up to Rs 1 crore.

Theft is defined as the dishonest removal of movable property from another person's possession without that person's consent in Section 378 of the Indian Penal Code (IPC), 1860. With only slight language changes to bring the legislation up to date, this concept has been preserved in Section 303 of the Bharatiya Nyaya Sanhita (BNS), 2023. The fundamental components—movable property, lack of consent, dishonest intent, and property movement—remain unaltered. With the same penalty, Section 304 of the BNS now covers the equivalent punishment under Section 379 of the IPC, which was up to three years in prison, a fine, or both.

India's first data privacy law, the Digital Personal Data Protection Act, 2023, outlines the rights of data principals, associated penalties, and fiduciary duties[28].

In the areas of AI and cybercrime, India's legal system is still developing. The absence of AI-specific legislation leaves significant gaps in handling contemporary digital risks, even if the IT Act establishes a fundamental framework for cyber offenses. Comprehensive AI legislation is desperately needed, supported by strong data security, moral principles, and the development of judicial competence.

[27]https://recordoflaw.in/legal-perspectives-on-cybercrime-in-india/

[28]https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india#:~:text=Possession%20or%20use%20of%20cybercrime,Similarly%2C%20in%20State%20v.

Shreya Singhal v. Union of India, 2015:

'A historic ruling by the Indian Supreme Court that had a big impact on the nation's digital content control and online free speech.

The Supreme Court ruled on March 24, 2015, that Section 66A was unconstitutional in its entirety. The Court determined that the clause had a chilling impact on free speech because it was ambiguous and overbroad. The reasonable limitations allowed by Article 19(2) of the Constitution did not apply to it. The Court stressed that a significant quantity of protected and innocent expression could be restricted because of the law's unclear definition of its restrictions[29].'

Kalandi Charan Lenka v. State of Odisha (2017):

'The victim, a teenager, went to court because she had been the target of derogatory remarks at school that damaged her reputation. Her father's character was also impacted by abusive messages he received from an unidentified mobile number. When he found out, the father told the victim what had happened and apologized. Despite this, the accused was found guilty of sexual harassment prima facie by the High Court, which denied bail[30].'

CHAPTER-5: ANALYSIS

'There's a need to a comprehensive approach to deal with these issues. First and foremost, lawmakers need to revise and create necessary, unambiguous legislation that address emerging crimes brought about by technology advancements. Additionally, creating moral standards for the application of AI in maintaining public confidence in the judicial system and defending human rights depend on law enforcement. Through international agreements controlling legal processes and information sharing, international cooperation is also essential in combating transnational cybercrime[31].'

[29]https://www.dhyeyalaw.in/shreya-singhal-v-union-of-india#:~:text=Summary%20of%20Recent%20judgment&text=The%20case%20of%20Shreya%20Singhal,to%20life%20and%20personal%20liberty).&text=1.,Article%2021%20of%20the%20Constitution.

[30]https://www.drishtijudiciary.com/current-affairs/stalking

[31]Cyber Crime and Criminal Law in The Era of Artificial Intelligence Murshal Senjaya

The Indian Laws are only **partially efficient** and **not fully sufficient** for modern cyber threats.

'In a denial-of-service (DoS) attack, the attacker purposefully overloads a server or network with requests, knowing that this will probably interfere with services and result in loss[32].'

'According to the National Cybercrime Reporting Portal (NCRP), victims of online financial frauds were tricked into losing more than 103.19 billion rupees in 2023. Additionally, the Administrative Standing Commission on Finance discovered significant domestic embezzlement in FY '23 alone, with an estimated total of ₹2,537.35 crores. Similarly, a stunning6. The severity and scope of cybercrimes in India were illustrated by the 94 lakh complaints that were filed in 2023[33].'

The Information Technology Act, 2000 and the more recent Digital Personal Data Protection (DPDP) Act of 2023 are two examples of cyber laws in India. The IT Act addresses common cybercrimes including online fraud, phishing, and hacking, while the DPDP Act establishes much-needed standards for protecting personal data.

However, the legal structure is reactive rather than proactive against emerging technologies; there are no explicit provisions for AI-driven crimes such as deepfakes, voice cloning, or algorithmic manipulation; there are also few remedies for cross-border cybercrimes and jurisdictional barriers.

The 2018 Aadhaar Data Breach:

'In 2018, millions of people's personal information was exposed due to an Aadhaar data breach in India. The first significant weakness in the safeguarding of digital data was this breach, which also posed a potential risk to security and privacy. Based on the idea of data protection, the case took a legal turn and mandated the implementation of stricter data protection laws. In addition to the need to strengthen security measures, the past years saw the enactment of laws that tightly enforced data protection[34].'

[32]https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/india#:~:text=Possession%20or%20use%20of%20cybercrime,Similarly%2C%20in%20State%20v.
[33]https://recordoflaw.in/legal-perspectives-on-cybercrime-in-india/
[34]https://recordoflaw.in/legal-perspectives-on-cybercrime-in-india/

Deepfake of Bollywood Actress (2023, India): A well-known actress's deepfake video went viral. There were no explicit provisions against synthetic media in the Indian Cyber Laws (IT Act, 2000).

Calls for AI regulation under the planned Digital India Act were fueled by public outcry.

Now, this new trend of Ghibli art[35] Unapproved use of Studio Ghibli's characters or copyrighted style to produce phony goods, art prints, or NFTs. This turns into intellectual property infringement, a type of crime made possible by cyberspace.

Cybercriminals may create "Ghibli-style" art without authorization using AI techniques, then sell it. Fans and customers are confused by art scams in the deepfake style. Violates laws pertaining to consumer protection and copyright.

Voice Cloning Fraud Cases (2024, Bengaluru and Delhi): 'Cybercriminals tricked customers into wiring money immediately over UPI by using AI to mimic family members' voices[36].'

Election Deepfakes (2024 Lok Sabha Elections, India): **'**Fake films of political figures produced by AI were shared to sway public opinion. Raised important questions regarding digital ethics and deception[37].'

Because cybercrimes frequently cross-national borders, they are challenging to investigate and prosecute. International criminals take advantage of jurisdictional loopholes, and MLATs (Mutual Legal Assistance Treaties) are difficult and slow to negotiate.

Since cybercriminals can work from anywhere in the globe, it can be difficult to catch and prosecute them, particularly if they are based in a country with poor cybersecurity regulations.

Indeed, jurisdiction is a big obstacle.

[35]Refers to the stunning, unique animation style of Spirited Away, My Neighbor Totoro, and Howl's Moving Castle, all of which were produced by the renowned Japanese studio Studio Ghibli.

[36]https://the420.in/ai-enabled-voice-scams-a-growing-threat-in-india-and-beyond/(AI-Enabled Voice Scams: A Growing Threat in India and Beyond)

[37]https://www.resolver.com/blog/deepfakes-targets-lok-sabha-election-2024/ (Alarming wave of AI-generated content floods social media around Lok Sabha Election 2024)

'Due to their transnational nature, cybercrimes cross national boundaries, making it impossible and illegitimate to enforce domestic laws that are typically based on geographic or territorial jurisdiction. Cybercrimes are carried out through the interconnectedness of cyberspace networks, so they are not limited by geographic boundaries[38].'

The Chinese Loan App Scam (2020–2022): **'**demonstrated how, despite obvious local effects, servers situated outside of India obstructed law enforcement operations[39].'

Ransomware Attack on AIIMS Delhi (2022): 'Said to have requested from the All-India Institute of Medical Sciences over Rs 200 crore, or $24.5 million, in cryptocurrency. It should be mentioned that the attack caused the AIIMS server to be down for six consecutive days.

Hackers wanted cryptocurrency from the hacked AIIMS hospital servers. suspected to be run out of East Europe or Russia.

Jurisdictional loopholes made it difficult for Indian agencies to track the assailants[40].'

Dark Web Drug & Weapons Markets (2023): Through foreign dark web marketplaces, Indian buyers and merchants were discovered engaging in illicit activity. The need for coordination between Interpol and India's CBI demonstrates the lengthy delay of multi-jurisdictional investigations.

'Cybersecurity is one of the many industries that have seen significant change because of the recent advent of generative AI. GenAI is regarded as a revolutionary tool for enhancing cybersecurity and is well-known for its ability to generate content and forecast trends. However, its expansion also presents fresh difficulties and potential risks.

The positive aspect is that it is a powerful tool for predictive threat identification because of its capacity to examine enormous volumes of data and spot trends. By identifying abnormalities and

[38]https://shodhganga.inflibnet.ac.in/bitstream/10603/189479/7/07_chapter-2.pdf(Cyber crime in India a critical study in modern perspective)
[39]https://www.news18.com/world/decoding-chinas-global-cyber-financial-warfare-loan-app-scams-data-theft-economic-sabotage-exclusive-9282535.html
[40]https://www.cm-alliance.com/cybersecurity-blog/aiims-ransomware-attack (AIIMS Ransomware Attack Date: 5 July 2023)

odd patterns in network traffic, it can predict cyberthreats and help enterprises take preventative action.

May greatly cut down on the amount of time needed to handle security breaches by automating incident response procedures. It can swiftly determine the type of danger and recommend the best defences by utilizing machine learning algorithms.

Organizations can improve their vulnerability management procedures with GenAI. Compared to conventional techniques, it can more effectively scan software and systems for vulnerabilities, producing thorough findings and suggestions for fixing flaws.

By examining behavioral biometrics like mouse movements and typing patterns, GenAI can strengthen user authentication systems. This increases security by making it harder for unauthorized people to get in[41].'

Delhi Police's Facial Recognition System (2023): 'Assisted in locating offenders and tracking down missing children. Investigative speed and accuracy were increased with the use of AI[42].'

Aadhaar-Based e-KYC and Digi-Locker Expansion (2024): AI-powered document verification increased the effectiveness of governance and banking.

'The Possible Risks and Restrictions: Advanced Cyberattacks: Although GenAI can enhance cybersecurity, it also gives hackers access to advanced tools that they can use to carry out increasingly complex attacks. For instance, phishing emails produced by AI might be very convincing and challenging to identify.

False Positives: Due to the complexity of GenAI systems, occasionally harmless activities may be mistakenly identified as threats. This may result in needless interruptions and lower security operations' effectiveness.

[41]https://www.compunnel.com/blogs/generative-ai-in-cybersecurity-boon-or-bane/#:~:text=About%2063%25%20of%20organizations%20focus,a%20threat%20to%20replacing%20humans.
[42]https://caravanmagazine.in/technology/dangers-of-facial-recognition-technology-in-indian-policing

Data Privacy Challenges: GenAI is frequently used in cybersecurity to process vast amounts of sensitive data. Because improper data processing can have serious legal and reputational consequences, maintaining data privacy and regulatory compliance becomes extremely difficult.

Over-reliance on GenAI may result in a fictitious sense of security. Because AI systems are not perfect and can be tricked or exploited by skilled adversaries, human oversight is still essential[43].'

Voice Cloning Fraud Cases (2024, Bengaluru and Delhi):

Cybercriminals tricked customers into wiring money immediately over UPI by using AI to mimic family members' voices.

Election Deepfakes (2024 Lok Sabha Elections, India):

Fake films of political figures produced by AI were shared to sway public opinion. Raised important questions regarding digital ethics and deception.

CHAPTER-6: CONCLUSION

Artificial intelligence (AI) and cyberspace's explosive growth have transformed politics, trade, and communication, but they have led to previously unheard-of types of criminal activity. In addition to empowering society, the combination of AI and cyber networks has also made it more vulnerable. This study demonstrates that although India and the global community have made great progress in enacting laws such as the Digital Personal Data Protection Act of 2023 and the Information Technology Act of 2000, legal frameworks are still primarily reactive and frequently inadequate to address the complex and constantly changing nature of cybercrimes and offences driven by artificial intelligence.

Prosecution and enforcement are extremely complex because to jurisdictional issues, cybercriminals' anonymity, and the global spread of digital networks. Furthermore, although AI

[43]https://www.compunnel.com/blogs/generative-ai-in-cybersecurity-boon-or-bane/#:~:text=About%2063%25%20of%20organizations%20focus,a%20threat%20to%20replacing%20humans.

has significant potential for enhancing cybersecurity, it also gives criminals new means of carrying out sophisticated assaults like ransomware, voice cloning, and deepfakes.

Even while India's legal system is changing, it must change faster with proactive laws tailored to AI, robust international collaboration, modernized investigative tools, and moral standards for using new technology. Both national security and individual liberties are still in grave danger in the absence of these steps. Therefore, protecting the future digital ecosystem requires finding a compromise between strong cyber governance and technical innovation.