EMERGING CYBER THREATS IN INDIA: A WAKE-UP CALL FOR LEGAL REFORMS

Samyuktha V, B.Com LLB, Sastra University, Thanjavur

Devarajan B, BBA LLB, Sastra University, Thanjavur

ABSTRACT

Crime is a crime if it is done physically or technically. Thanks to the advancement of technology, digital crimes are growing faster. The criminal activities that are carried out using technical/digital devices and networks are called as Cybercrimes. They may be in any form of fraud viz. identity theft, data breaches, computer viruses, scams, hacking, phishing, ransomware, and malware attacks. In the modern world, with the rise in internet usage, the cyber criminals can approach their victims easily but need not be physically. Cybercrimes are different from any other crimes taking place in the world; the main reason is that no geographical boundary is required to initiate cybercrime and most of the time the criminals are unknown. Cybercrime affects all the stakeholders leaving no exceptions. Women are generally easy targets for cybercrime. The paper discusses cyber laws, their antiquated status, and their impact on the nation. It signifies how outdated laws are turned to be a loophole for cyber-criminals to get away with their crime. It highlights the steps taken by the administration to counter the cyber-attacks. Additionally, vulnerabilities that make it simple for fraudsters to circumvent criminal prohibitions are addressed. Educating people about cybercrimes and their commission with ease are the important aspects of this study. In India, the Indian Cybercrime Coordination Center (I4C) is a government initiative that helps law enforcement agencies to work together to prevent cybercrimes. The mission of 14C which aims to create a safer place for internet users is also discussed here.

INTRODUCTION

The virtual realm of the internet is referred to as cyberspace. The term was coined by William Gibson, a science fiction writer, in 1984. Over the period, the word 'cyberspace' has been used to describe the internet and other computer networks. Subsequently, the nomenclature of 'Cyberspace' was changed and named as "Cybercrime." It means that any crime carried out with the help of computer, network or any other digital devices will come under the purview of Cybercrime. The Cybercrime will not only affect the life of individual but also the survival of Commercial as well Government entities

In today's world, as technology advances everything is done on online, from scrolling through social media to conducting larger monetary transactions. More people rely on networks and digital devices for day-to-day operations which lead to upsurge of the cybercrimes resulting in lack of privacy in safeguarding our personal information.

Cybercrime encompasses a broad range of criminal activities that involves the usage of various digital platforms and technologies. Some common cybercrimes include phishing, email spoofing, forgery of e-documents, the spread of defamatory statements online, publishing of obscene information, unauthorized access to protected systems, pornography, morphing, and breach of confidentiality and integrity. Nowadays, every internet user is prone to cybercrimes.

Modern-day crime has more to do with computers than guns. People's material possessions were stolen in the past, but today everything is stolen, including their privacy. The development of computers, software, and electronic devices may be taken as a boon and at the same time bane to the society.

Technology is the primary tool in cybercrime. The evolution of technology is not inherently bad, but some computer specialists have encountered its negative aspects, using them for their selfish motives and harming many lives. This has created a vicious cycle in society

Main cyber players in internet are cyber criminals. They hack banks and financial institutions for commercial gains. Cyber terrorists are people who attack the data servers of national infrastructure which are of high-level national security. Cyber hacktivists are groups of anonymous figures whose agenda is to hack into the sites and servers to communicate certain messages concerning their specific campaigns.

Classification of Cybercrimes

Cybercrimes are usually classified under

- Cybercrime against individuals,
- Cybercrime against property,
- Cybercrime against organizations,
- Cybercrime against society,
- Crimes emanating from Usenet newsgroup

Cyber Crimes Against Women in India

The rise of digital platforms and easy access to personal information has contributed to the increasing prevalence of cybercrime. The feminine gender becomes the main victim of cybercrimes nowadays. Usually, the womankind is very reluctant to address their grievances publicly. This attitude makes the culprits to play cyberattacks on women with the tool of modern technology. Hence the rate of cybercrime against women is increasing day by day. The ramifications are more that the cyberattacks will not only affect the physical and mental strength of the womenfolk but also their financial security.

The diverse categories of cybercrime against women are: online harassment, sextortion, morphing, cyberstalking, revenge porn and financial fraud.

Online harassment

It is a predominant cybercrime against women in India, with 66% of women reporting such experiences, according to the National Commission for Women. It may include abusive, threatening, or offensive messages on digital platforms. This online harassment can often cause mental distress, anxiety, and fear. For many women, this harassment led to a sense of vulnerability and insecurity in online spaces, resulting them to withdraw from digital platforms or restrict their online interactions to avoid further abuse.

Sextortion

It is an extreme offense against women with the use of artificial intelligence (AI) by threatening to release explicit images or videos to blackmail or coerce. AI sextortion is a deepfake algorithm, used to make counterfeit clear videos or images of women to threaten, blackmail, and harass. According to the National Crime Records Bureau (NCRB) Report for 2022, cybercrimes related to sexual exploitation was 5.2% and a total of 65,893 cases reported during that year, whereas statistically, it may increase further years.[1]

Morphing

It is altering images of women to create objectionable or pornographic content. India has alone recorded 37% of cases related to harassment of women due to morphed images.

Cyberstalking

Harassing or threatening through social media by tracking computer and internet uses of women, is a serious and growing form of cybercrime that women in India increasingly face in the digital age. The consequences of cyberstalking are severe the victims may experience anxiety, depression, and a constant sense of vulnerability. India has laws to address this crime, including provisions under the IT Act 2000 and section 354D of the IPC[2]. However, enforcement remains challenging due to a lack of awareness, insufficient training for law enforcement, and the rapid evolution of digital platforms.

Revenge porn

Revenge pornography is one of the dangerous cybercrimes against women. In India, its percentage of occurrence is increasing at rapid speed. It is particularly exploiting their privacy and dignity. This type of cybercrime involves the non-consensual distribution of sexually explicit images or videos which may lead to severe mental and emotional trauma, depression, anxiety, and feelings of shame. A report by the Cyber Peace Foundation highlights the alarming reality – a 150% increase in revenge porn cases in India in the past few years.

[1] Report on sextortion is available at https://www.drishtiias.com/daily-updates/daily-news-analysis/ncrbs-crime-in-india-2022-report

[2] S.354D of the IPC is available at https://www.indiacode.nic.in/repealedfileopen?rfilename=A1860-45.pdf

In conclusion, addressing these crimes requires collective action from the government, law enforcement, tech companies, and society at large. By fostering a culture of respect and accountability in online space, India can take significant strides toward ensuring the safety and digital of women in the digital realm.

Cybercrime Laws in India

According to the World Cybercrime Index, India is in 10th place and specializes in internet scams. The laws that are enacted to govern Cybercrimes are called Cyber Laws. All the netizens of this space come under the ambit of these laws as they carry a kind of universal jurisdiction. Cyber law can also be described as that branch of law that deals with the legal issues related to the usage of information technology. The laws are meant for limitations in the usage of for Digital devices/ internet.

The Indian government has enacted various technology-related legislation to resolve the violations in the digital space. Among them, the legislature primarily enacted the Information Technology Act to administer the application of technology in India. The Information Technology Act (IT Act), 2000 came into effect on October 17, 2000. At the international level, a resolution was passed by the United Nations on 30th January 1997 to introduce the Information Technology Act which subsequently became a part of the modern law on international trade law on electronic commerce.

The pace at which cybercrime laws are being enforced is increasing every day. From protecting its critical infrastructure to supporting research and development, India is fast stepping up its defenses against cyber threats. However, we cannot deny the fact, that there are lacunas in the enforcement and protection of citizens from cybercrimes.

Loopholes in cybercrime laws

Laws are not exhaustive and outdated: The law has not been updated to address past cybercrimes, despite the increasing number of cybercrimes happening worldwide. New types of cybercrimes are emerging daily, but there are no legal provisions to penalize them due to the lack of updated legislation. The Act has not been amended for the last 20 years, barring once in 2008. The IT Act 2000 addresses only some parts of cybercrimes as the IT Act 2000 are not a cyber-security law. Other cyber offenses like phishing, spamming, fintech issues like

internet banking fraud, identity theft, some offenses against women like cyberbullying, and defamations on electronic form are not stipulated in the Act. It does not provide any provision to penalize online trademark violations (relating to domain names) which are also known as cybersquatting and does not resolve Intellectual property-related issues like protection of copyright and patents. It is not an exhaustive Act. It does not have a foresight of evolving cyber offenses.

The case of Tata Sons Ltd v. Manus Kosuri and Ors is about the domain contended which is an English and Tamil website of the brand "Taatas – The Premium Quality Food Brand" under which "Taatas (Pvt.) Ltd." seeks to provide all such agricultural produces like organic food, ghee, etc. to its consumers in Sri Lanka. The infringing website is owned and controlled by a native of Sri Lanka, Mr. Thobiyas Segaram Bernard Vasanthkumaar; "the Respondent" personal incorporation. The Complainant asserts in the current dispute that the disputed domain name "taatas.com" is identical to the Complainant's well-known "TATA" trademark and service marks in its site "tata.com". The Complainant alleges that the Respondent uses the disputed domain in bad faith to perpetrate crime which is a classic case of either domain name squatting. [3]

Lack of privacy protection: The Indian IT Act is not a cybersecurity law and therefore does not deal with the nuances of cybersecurity, explains Dr Pavan Duggal, Advocate, Supreme Court of India and founder of Pavan Duggal Associates. "The IT Act also doesn't address privacy issues – privacy is now a fundamental right and the law needs to specifically address privacy concerns, but that's not the case," he points out. Privacy is a fundamental right when it comes to technology. The IT Act 2000 lacks in providing privacy to internet users. It does not provide content to regulate data protection and privacy issues. When an individual invades the privacy, he gets penalized immediately but till now there is no provision to make the government accountable when they invade the privacy of the citizens. They take shelter under sovereign acts of the government. But whenever the information is taken it is not mentioned as public emergency. This can be portrayed as government's quirks.

According to Section 69(3)4 of the IT Act[4], all subscribers and intermediaries must decrypt information for government agencies upon request. Failure to do so could result in

[3] *Tata Sons* v. *Manus Kosuri*, No.159 of 1999

[4] S. 69(3)4 of the IT Act, 2000 is available at https://www.indiacode.nic.in/bitstream/123456789/1999/1/A2000-21%20%281%29.pdf

imprisonment for up to seven years and heavy fines. This raises concerns about potential privacy breaches by the government against individuals. The worded provisions must be framed to remove any ambiguity in the text and have foresight into the future advancement of technology because a possibility has arisen where an individual's privacy can be arbitrarily violated through cyberspace, which paves the way for many heinous offenses related to that.

Lesser punishment: If the punishment is severe, the commission of crime will be less. If the punishment is less severe it will not make a big impact and it will not stop the criminals from committing the crime. To reduce the crime rate and to inflict fear in the mind of the criminals, the punishment must be severe. The IT Act 2000 imposes penalties up to 5 crores under section 43A of the act[5]. Still, until 2019-23 no penalty has been beyond 12-13 lakhs to the intermediaries, who receive billions for the cybercrimes they commit. As a result, they will not mind committing the offense and even becoming repeat offenders as they can pay the penalties. Due to the lesser severity of punishment, we can find many offenders who have no regrets and are turned into habitual offenders.

For example, Section 67 A of IT Act 2000[6] pertains to the Punishment for publishing or transmitting material containing a sexually explicit act, in electronic form. The punishment is imprisonment for 3 years or a penalty upto 10 lakhs or both. Due to the severity and alarming nature of the crime, the punishment should be more than 3 years and the penalty should exceed 10 lakhs. Considering the crime concerns the safety and privacy of a woman, the punishment for such crimes should be severe.

Section 74 of the IT Act[7] is about the Publication of digital signatures for fraudulent purposes. The punishment is Imprisonment for a term of 2 years or fine for 1 lakh rupees or both. Currently, for most of the offenses, the imprisonment duration is up to 3 years and penalties range between lakhs. The 2008 amendment in the IT Act 2000 reduces the quantum of punishment and it is made as a bailable offense, also raising the fine which replicates a toothless tiger against the perpetrator. This paved the way for most of the offenders to pay the penalties and escape imprisonment only to start committing crimes again. To prevent the crime, the

[5] Supra note 3, s.43A.
[6] Supra note 3, s.67A.
[7] Supra note 3, s.54.

punishment should be rigorous to instill fright in the individual's mind and deter them from committing the crime.[8]

Emerging sophistication in cybercrimes and criminals: Cyber Criminals are tech-savvy. With their criminal mind, they engulf themselves in modern technologies and come out with new advanced methods like proxy servers, VPNs(Virtual Private Networks), encryption etc. to keep their identities in dark. As the Law Enforcement Agencies are yet to be full-fledged with the modern technologies, they find it very difficult in tracking the crime doers down. Private networks such as VPNs are easily available to the internet user, allowing them to hide their IP address and their location which makes it difficult to track them in time. India has experienced a significant increase in cyberattacks over the recent years. The Home Ministry's National Cyber Crime Reporting Portal has been receiving around 7,000 complaints daily between January and May 2024. 85 percent of these complaints are related to online financial fraud. There is considerable increase in the number of complaints for the past few years. Up until May 2024, the portal received 7.4 lakh complaints related to cybercrimes. This figure was over 26000 in 2019, 2.5 lakhs in 2020, 4.5 lakh in 2021, 9.5 lakhs in 2022, and 15.5 lakhs in 2023. The cost of cyberattacks is significant. It is reported by the Indian Cybercrime Coordination Centre (14C), the Central Government's Nodal Agency that a total of 4599 cybercrime complaints i.e. digital frauds amounting to Rs.1203.06 crores were registered during the period from January to April of the year 2024, as per ANI report.[9]

INITIATIVES TAKEN BY GOVERNEMENT OF INDIA

Indian Cyber Crime Coordination Centre

In October 2018, the Ministry of Home Affairs of India launched the Indian Cyber Crime Coordination Centre as an initiative to collaborate between law enforcement agencies of various countries to fight cybercrime. The center aims to combat cybercrime, focusing on cyber terrorism, child exploitation, financial fraud, and others.

The main objective of I4C is to create a platform for law enforcement agencies to collaborate and coordinate among themselves to provide information on cybercrimes happening in their

[8]https://eprocure.gov.in/cppp/rulesandprocs/kbadqkdlcswfjdelrquehwuxcfmijmuixngudufgbuubgubfugbububjxcgfvsbdihbgfGhdfgFHytyhRtMjk4NzY=

[9] https://www.indiatoday.in/business/budget/story/budget-2024-cybersecurity-artificial-intelligence-projects-allocation-jump-2571272-2024-07-24

jurisdiction, cyber threat investigations, and the best method to prevent cybercrime and for investigations.

It aims to create a reliable communication channel for sharing information among different agencies of different countries to enable effective coordination and response to cybercrimes.

The 14C brings together agencies such as the Central Bureau of Investigation, the National Investigation Agency, the Indian Computer Emergency Response Team, etc., and it becomes a platform for apprising each other in connection with the salvation of cybercrime frauds. They can exchange their views and sharing their knowledge in tackling the online frauds.

Objectives of I4C

(i) To act as a nodal point to curb Cybercrime in the country:

As an intervening point to mitigate Cybercrime in the country, the I4C coordinates the efforts of police and other actors, including those between law enforcement agencies. It coordinates activities with other countries through Mutual Legal Assistance Treaties (MLAT).

(ii) To protect from cyber threats against women and children:

The government evolved a scheme for Cyber Crime Prevention against Women and Children. The Ministry of Home Affairs has formulated the Scheme for Cyber Crime Prevention against Women and Children (CCWC) to establish an effective system for processing cybercrimes targeted against women and children. The Indian Cyber Crime Coordination Centre (14C) was established by the Government of India to build up a coordination among the Law Enforcement Agencies (LEAs) in tackling cybercrimes at large.

(iii) Paving the way for easy filing of complaints related to cybercrime and identifying Cybercrime trends and patterns:

The I4C and the National Cyber Crime Reporting Portal facilitate reporting of cybercrime and trend analysis. Users of the NCRP can file online complaints with the concerned states or union territories. Complaints are automatically re-directed to the responsible state or union territory law enforcing agencies for expeditious redressal. The NCRP covers a plethora of cybercrimes, such as hacking, identity theft, online fraud, and cyberbullying. Once the complaint has been

filed and submitted, an acknowledgment is sent to the registered mobile number of the complainant. The complainant can track his/her complaint/status with the help of the registered number received on their mobile.

(iv) Creating awareness among the public about preventing Cybercrime:

I4C is initiating a public awareness campaign. Cybercrime cannot be prevented unless the victim knows how to avoid cybercrime. The main objective of the campaign is to create awareness among the public about the seriousness of cybercrime and the basic things they can do to protect themselves from cybercrime. The campaign is spreading awareness through 72 TV channels, 190 Radio FM channels, theatres, bus stands, railway stations, telecommunications, and many more platforms. Also creating awareness regarding the cybercrime helpline 1930 and other platforms of I4C will increase its utility and help prevent cybercrimes.

National Cybercrime Reporting Portal

The National Cybercrime Reporting Portal is an online platform for filing complaints against cybercrime such as hacking, online bullying, identity theft, and financial fraud in India. It was launched as a part of I4C by the Ministry of Home Affairs on 30.08.2019. The main purpose of NCRP is to take quick action against cyber criminals. Once the complaint is filed it is assigned to the subsequent state and union territories and law enforcement agencies to act against the cybercrime. Back then they take complaints such as rape/gang rape and sexually abusive content only. But now after the amendment, it takes all types of cybercrimes.

Digital Personal Data Protection Act (DPDP), 2023

The Digital Personal Data Protection Act (DPDP), 2023 was introduced to establish rules and regulations for data handling. It also mandates heavier and stricter penalties for breaches and encourages organizations to manage data effectively.

Cybercrime Cells

The cybercrime cells are established by the State government in their States. It investigates cybercrimes, performs digital forensics, and renders technical assistance to law enforcement agencies. States have set up cybercrime cells to tackle cyber-related offences.

Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Center)

Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Center) is a scheme launched by the Ministry of Electronics and Information Technology (MeitY). The main objective is to create awareness about malware and potential threats to electronic devices. They also provide free tools to remove the malware. They also distribute information kits to inform the users about the cybercrimes happening in the country.[10]

Budget allocation by the government for cybersecurity in the past years:

India's budget for cybersecurity projects was relatively small before 2022. In the 2022-2023 budget, the Ministry of Electronics, and Information Technology (MeitY) allocated only ₹30 crore, showing that strong cybersecurity practices were only beginning to be taken seriously. However, there was a remarkable increase in the 2023-2024 interim budget with the government assigning ₹400 crore for cyber security activities.

In February 2023, the Indian government allocated fund over six billion Indian rupees to MEITY for developing cybersecurity infrastructure. The budget allocated for cybersecurity projects drastically increased to 90 percent in the past financial year and reached Rs 759 crore in 2024. India's important agency for cybersecurity cases is the Indian Computer Emergency Response Team (CERT-In), which was given Rs 238 crore to improve its functioning.

They also allocated Rs 52.8 crore for schemes that are mainly focused on preventing cybercrimes against women and children, whereas the Data Protection Board of India – being set up under the Digital Personal Data Protection Act, 2023 was given Rs 2 crore for salaries and other expenses for its members, according to the budget documents.[11]

Capital invested by the government in MEITY is 581.01 for the year 2024-2025 in the interim budget for various cybersecurity programs, schemes, developments, introducing advanced AI technologies to combat cyber threats, and many.[12]

[10] https://www.csk.gov.in/
[11] https://indianexpress.com/article/business/budget/union-budget-2024-cybersecurity-budget-digital-economy-9462862/
[12] https://www.indiabudget.gov.in/doc/eb/sbe27.pdf

CONCLUSION

It is encouraging on the part of the Government of India to initiate various measures to tackle the cybercrimes by allocating a considerable budget for cyber security projects. However, it requires proactive measures and vigilance. The laws for cybercrimes are to be amended now and then to meet out the fast growing of the cybercrimes. Much importance should be given in prevention and awareness among public, data collection, research, and analysis on cybercrimes. The Cybercrime doers will usually aim and target the people who are using the digital devices with less authentication or weak passwords, ordinary privacy settings with no stronger value and lapsed security software. Public should be educated to update the systems with security patches and use reliable security software with multi-factor authentication. Training of law enforcement agencies, judiciary, and prosecutors to handle cybercrime cases is to be put in place. Possible creation of dedicated cybercrime investigation training centers such as the Central Detective Training Institutes will aid in the effective initiation of actions against cybercrimes. Tech companies should be a part and an indispensable ally with the Government to fight against cybercrime. The engagement of public-private sector will also help to clamp down the cybercrimes. The Cybercrime Detecting and Law Enforcement Agencies should be fully equipped in all fields i.e technically, physically and financially. Then only they can combat the cybercrimes. The hands of Law Enforcement Agency should always be in upper hand in order to bring the cybercriminals into their fold. Cybercriminals are not born; they are created by the advancement of technologies. With the use of the same modern technologies, we will give a strong knock out to the cybercrimes. So, it is in the hands of every citizen to put a full stop to the cybercrime.

Be vigilant and proactive to make the cybercrime into cypher (zero) crime.