Library Progress International
Vol.44 No. 3, Jul-Dec 2024: P.9190-9210

Print version ISSN 0970 1052
Online version ISSN 2320 317X

Original Article

Available online at www.bpasjournals.com

Bridging the Cybersecurity Gap in India: Legal, Technical, and Public Awareness Issues

[1]Bhagesh Gupta,[2]Sarthak Bhatnagar

[1]University Manipal University Jaipur
bhageshgupta114@gmail.com
[2]University Manipal University Jaipur

How to cite this article: Bhagesh Gupta, Sarthak Bhatnagar (2024) Bridging the Cybersecurity Gap in India: Legal, Technical, and Public Awareness Issues. *Library Progress International,* 44(3), 9211-9225.

ABSTRACT
The Internet is often described as a unique tool, unique platform, unique experience – but what is the Internet for? One might get caught in an increasing population of criminals who master the social web brilliantly. Cyberspace or the Web is an environment that is ethereal and dynamic. Assuming that the claim of this paper is true, cybercrime or e-crime is characterized as a new form of criminality perpetrated by technologically sophisticated criminals.
This paper aims at describing cybercrimes by analyzing the actors involved in the commission of these acts and the reasons prompting such actions. That is why it also encompasses different categories of cybercriminal activities and outlines their peculiarities, which may concern the prevention, identification, and investigation of the respective crimes. Furthermore, the paper outlines the key parts of the Indian IT Act, 2000 besides offering recommendations as to possible changes

Key Words: Cyber Security, Technology, Harassment, Fraud, Misrepresentation.

Introduction

The rise of cybercrime in India with statistical data and new types of cybercrime.

[1]Modern technology has brought numerous benefits to India but on the other hand has also brought an entrance to ultramodern cyber threats to India. With emerging trends, cybercriminals find new ways to misuse the technological revolution making the battle more crucial against cybercrime. Cybercrime refers to illegal activities that are being done through digital devices like computers, mobile phones using the internet, and other facilities to initiate the crime, with an increase in technological advancement such crimes have become more usual. [2]Cyber phishing is one of the most common types of cybercrime, which is committed in India where fake emails, messages, and even phone calls are being made to people for to reveal the private data information of the victims to commit the crime. If we look at the shocking statistical data of cybercrime more than 65,000 cases were reported in 2022 to the authorities giving an increase of more than 13,000 cases which were reported in 2021. According to a report published by Norton, the country has been a witness to approximately 30 million victims of cybercrime which has led to a loss of almost 3 billion dollars to the victims. When we talk about the most committed cybercrime, financial fraud does comply with almost 60% of the crimes comprising of online banking scams, credit card scams, UPI scams and other unauthorized digital transactions. Upon the reported crimes 22% of crimes are phishing where the victims are tricked by the criminals by taking their private and sensitive information. When we talk about the crime geographical areas Delhi is considered as the hotspot of these cybercrimes where 20% of the total crimes are reported but with the changing trend of the crimes, the new targets are identified from rural India because of lack of digital literacy and awareness among the rural people in India. The main targets are the

[1] June 7, 2012), http://book.itep.ru/depository/security/trends/Eight_trends_changing_network_security.pdf.

[2] (May 5, 2022), https://ijarsct.co.in/A3402.pdf.

individuals who can trust the opposite side easily and can share sensitive information with them without getting any clue these comprise almost 70% of reported cases are of individuals and the same case is with the newly small and mid-sized businesses of which some do report a cybercrime once in a year. There are so many new emerging trends in types of cyber crimes

[3] **Types of cyber crimes**

1. **Phishing** – obtaining sensitive information fraudulently like passwords, unique numbers, login credentials, etc. by pretending to be an official authority or a trustworthy entity through electronic or digital platforms with mostly an intention of illegal financial gains. If we look at CERT-in report of 2022, the cases of phishing have increased rapidly, and more than 13,000 cases of phishing were reported. Out of these reported cases, 50% of the targeted victims are from the financial sector because of the rise in the digital payment sector as they use their user credentials and other important data to steal access for fraudulent transactions. There are different kinds of phishing like email-based, SMS-based, and call-based phishing where they try to trick the victim into sharing their secured data pretending to be a trusted authorized person. There are some new types also emerged like UPI phishing where fake links are sent to steal information and social media phishing where scamsters pretend to be you are sent known contacts and trusted brands. A study by Statista reported that India stands in 2nd place when it comes to phishing crime which include attacks originating and attacked victims and a report by NASSCOM reported that in the year 2022 India faced $18.5 billion in phishing.

2. **Cyberbullying**- Under this crime, threatening and defamation are caused to the victim using the online platform to harass them or any other benefit out of compulsion of the victim. Cyberbullying consists of trolling, harassment, stalking, doxing, impersonation, etc. The NCRB report of 2021 showed that the cases of cyberbullying and online harassment have increased over the period where they stated a rise of 11% in 2021 as compared to the data of 2020. Maharashtra, Uttar Pradesh, and Karnataka have reported the highest number of cyberbullying cases in 2021. Almost 12,000 cases of cyber bullying including harassment were reported in 2021. In the cases of cyberbullying young girls are targeted aged between 14 years to 24 years having cases of stalking, slut shaming harassment. Such cases are more in number but stay unreported by the victims and their families because of the social stigma. Due to advancing technology and a lack of awareness among the victims such crimes happen more and more. Because of inadequate enforcement agencies and jurisdictional issues such cases happen to more complicated. The government has been working on such issues by opening crime reporting portals and dedicated cyber cells in police departments all over the country.

Example- spreading of private photos or information on social media without the permission of the person. Sending mean or hurtful texts or posting them with the other person's identity to take revenge or bully.

3. **Software piracy**- Using a cracked version of software through unauthorized means, downloading or copying of software without a legitimate purchase from the owner, and also a threat to the software as well the company. India is considered as one of the biggest markets for software piracy having an average more than global piracy rate. According to a 2018 report by BSA, India's piracy rate is 58% while the global average is 37%. Despite lawing laws and enforcement agencies the piracy figures remain the same and the companies incur losses. With the changing times and technology, a shift from physical coping of the software has been changed to online methods of software piracy made through illegal websites and applications which create difficulty for the authorities for investigation and other procedures. The issue with the continuous rise of software piracy is the unawareness of the people that using pirated software is illegal in India which may lead to legal risks and costs. Only the public cannot be blamed the high premium charges of the software companies like Adobe and Microsoft which also lead to piracy of the software.

[3] Cyber Crime and Security – A Study on Awareness among Young Netizens of Anand (Gujarat State, India), https://ijariie.com/FormDetails.aspx?MenuScriptId=2392&srsltid=AfmBOorg2f3uUpqB8oOz5XhA-rx_uAsHhsQawfG05_N71DdHhJkpN6XB.

4. [4]**Hacking**- Taking access to a computer system in an unauthorized way or illegally to obtain, alter or destroy any kind of data or information to conduct any crimes. Statistical data of 2024 reported that more than 2800 cyberattacks are reported by Indian organisations which is almost 33% more in comparison to 2023. According to a 2023 report by CERT more than 1.25 lakh were reported in the first half of 2023. When we talk about hacking, one of the biggest examples is Indian telecom data breach, in January 2024 affecting a large population's data breach from India's biggest telecom providers which was later available for sale on the dark web. Another example is the boat data breach of April 2024 where data of almost 70 lakh people were hacked including phone numbers, emails etc. In January 2024, Hyundai Motors also experienced a data breach from their own repair system where data of many customers was available online.

5. **Ransomware**- Under this cybercrime, malware attacks the computer system which encrypts or blocks the user data and asks for payment of ransom to unlock the data or software like before. For example, a user having important data blocked by a malware demanding payment through cryptocurrency otherwise it will remain locked. Ransomware usually enters the computerized system through malware mails, links or other ways. Once such ransomware finds its way to the computer system then it encrypts the system and locks it in the other users and owner asking for a decryption key to unlock the computer system. But for having the decryption key a message is displayed on the screen asking for a ransom amount which is usually asked in cryptocurrency in exchange for the decryption key. If the victim pays the ransom, then there are chances that the victim might get the key or might not, it depends upon the person to provide the decryption key or not. Here, the payment of ransom does not guarantee the key and restoration of the encrypted data. If we look to the statistical data, a report of 2022 by SOPHOS a cybersecurity firm reported that almost 78% of the Indian organizations faced ransomware attacks during the previous years which is higher than the global average of 66%. It is estimated that the average cost of ransomware for big organizations is $4.5 million in the year 2022 containing the payment cost, recovery cost, and losses to the organization. More than half of the victims of ransomware do pay the ransom but the data shows that about 10% of the victims only get the decryption key for the restoration of data. In most cases, it is seen that after the payment of ransom, most of the victims are still not able to recover their data resulting in huge losses to the organisations. The most targeted institutions are healthcare, energy, manufacturing, telecom, financial services sectors etc.

6. [5]**Cyber terrorism**- When the internet and digital technology are used by groups or other associations who are involved in terrorist activities, causing harm and fear to the victims they want to target. Such cyber-attacks usually target big institutions of a nation like government infrastructure and their systems, big corporations, and financial institutions. Such targeted institutions play an important role in the economy of a nation like the power grid system of a country, healthcare or transportation network etc which provide services daily to the nation's population. For such terrorist groups to create panic or immediate pressure on the government or society is by attacking their air traffic control, chemical industries, or even the nuclear power plants which create an instant situation of emergency in the country. These cyber-attacks happen because of many purposes but the main reason is to steal the data of the targeted country that may be from their government database or maybe from their military database which can be used by the terrorist for political or military purposes. To have funding, such terrorist organizations do ransomware attacks on institutions to have enough amount of funding with them to use in their terrorist attacks. There are different types of cyber terrorism where overwhelming or shutting down the important government digital infrastructure results in denial of service (DOS) attacks. Stealing critical data from government databases, military, health care etc for making a threat to the national security of the country or creating economic instability, this kind of attack is known as cyber espionage. These group uses the internet and social media to spread radicalization and inhuman propaganda and even use such platforms for recruitment of persons to join them in these terrorist acts. Cyber extortion or ransomware is also used by the groups to have funding to them which means doing cybercrime to do even more cybercrime. In the year 2020, Indian power grid systems were attacked

[4] Research Journal of Humanities and Social Sciences, (Sept. 27, 2024), https://rjhssonline.com/HTMLPaper.aspx?Journal=Research%20Journal%20of%20Humanities%20and%20Social%20Sciences;PID=2017-8-4-12.

[5] (Jan. 7, 2020), https://journals.indexcopernicus.com/api/file/viewByFileId/783266.pdf.

by some pre-planned hackers causing to system to stop resulting in blackouts in some parts of the country. At that time this attack was considered as an alarming sign for national security. India comes in the list of top ten nations which are targeted by these types of cybercrime. According to the CERT-in report of 2022, India received more than 13 lakh cases of cybercrime which include attacks on the crucial digital infrastructure of the country.

7. **Social engineering**- Social engineering is a kind of cybercrime where a criminal manipulates the individuals to reveal or tell their private or sensitive information. In social engineering the attackers use human psychology to get sensitive data like IDs, passwords, banking details, and user personal data rather than attacking the digital computer system directly. In India social engineering is used to commit various cybercrimes like phishing, data theft, and financial fraud. Sending fake emails or SMS pretending to be a trusted authority, for example, there have been cases reported that emails and SMS have been received by individuals from the Income tax department to give their personal credentials. The next level of social engineering is making a phone call pretending to be a trusted authority from banks and asking for sensitive information like OTP (one-time passwords), card pins, etc. Another way is by giving bait to the victim like a link for free download of a software or application or free subscription, where the victims get tricked and install malware into their systems. Another is impersonation on social media where the criminals create a fake profile of a person which the victims know like a friend or relative and ask for confidential information or financial assistance and gets tricked. According to the NCRB data of 2022, India reported over 50,000 such cases involving of social engineering where the psychology of a person is attacked rather than attacking their computer system. A report by RBI in 2021 revealed that almost 400 crores were lost by the banks in these kinds of frauds. A joint study by DSCI in 2022 reported that over all the reported cybercrimes in India, social engineering comprises of around more than 25% of the total crimes.

8. [6]**Banking fraud**- Banking fraud is a cybercrime that involves targeting of banking sector usually through online digital mediums to steal the personal information of the user like banking logins, pins, or card details. banking frauds in India are rising day by day because of a sudden increase is seen in the usage of digital and online banking services like e-banking, mobile banking, online banking, NEFT, digital payment methods like UPI, etc. The fraudsters send emails, SMS or even phone calls pretending to be from a legitimate bank. They ask for banking credentials like pins, OTP (one-time password), or card numbers which are later used to steal the money from the victim's bank account. According to RBI's annual report of 2021, banks have lost around 60,000 crore rupees due to frauds including both cyber and non-cyber frauds making a larger proportion of cyber frauds involved. Installation of skimming devices on ATM cards and other cards during the digital transaction to steal the card's information. Another method is SIM swapping where a duplicate SIM of the victim is taken by the fraudster to access the victim's bank account services to commit financial fraud. Here, the fraudster issues fake documents of the victims to the telecom company and gets issued a duplicate SIM to obtain the OTP to access the victim's bank account. These frauds have taken a new way where unauthorized digital payments from the stolen banking credentials of the victim by using the UPI method. According to a report of 2021 by RBI, there were more than 7500 cases of banking fraud where the amount exceeds the value of Rs 1 lakh. UPI has been a very easy method of online payment for the Indian currently but due to heavy usage and lack of cyber awareness most of the banking frauds are related to UPI methods. A report by the National Payment Corporation of India (NPCI) of 2021 reported that around 82% of the banking frauds are related to UPI payments.

9. **Defamation and online slander**- As cyber technology has advanced over the period, the social media reach of the public has also seen saw rise as a part of their daily routine and it also become a platform for online slander. Online slander refers to defamatory statements made on online or digital platforms like social media, vlogs, blogs, and websites. As the digital social platform has a very high reach such defamatory statements spread rapidly and can cause significant damage to the victim's reputations. Generally, public figures, celebrities, and politicians are the most targeted persons when it comes to online slander, they have a large fan base and good social media reach on such platforms. Here are some examples of online slander on different social media platforms where, Bollywood celebrity, Priyanka Chopra faced defamation on social media when rumours about her personal life

[6] Dr Eneji Sam, (May 7, 2019), https://ijisrt.com/wp-content/uploads/2019/05/IJISRT19MA504.pdf.

and relationships spread on social media. Even corporations have been victims of online slander where the rival companies spread such news or rumours on social media to defame them. For example, Tata Sons filed a defamation case against Green Peace Corporation for publishing fake news and rumours on their website. The creation of someone else profile and impersonation of the other person, posting defamatory content damaging the victims' identity. Another form of online slander can be sending defamatory messages in social media platform groups like WhatsApp and Telegram, accusing the victim without any evidential proof. A content creator on YouTube makes a video falsely accusing the victim without proper proof. Posting of vlogs or blogs on websites or social media applications claiming their immoral acts or illegal acts. Altering someone's image and creating of meme to defame their identity. A bunch of tweets continuously spread false rumours about the victim. In India, the defamation laws protect the victim's rights of individual reputation and balance the freedom of speech and defamation. However, due to technological advancement, our authorities do find it complex to combat such cases as social media has a very vast and fast reach.

10. **Spamming**- Spamming is a type of cybercrime where bulk texts or messages are sent to the victim, for advertisement purposes or for fraudulent means. There are many ways from which spamming can be initiated like spamming through emails, spamming through SMS, spamming through WhatsApp, and social media spamming. Spamming has been considered as the basis for committing serious cybercrimes like phishing, vishing, financial fraud or banking fraud, and identity theft of the user. Here are some examples of spamming; Email spam where bulk mails are sent containing advertisements or malicious links for the commitment of cybercrime. SMS spams, where bulk SMS are sent to the user containing ads or malicious links. Social media spam, where bulk messages are sent on social media platforms like Instagram and face book. Comment spamming where the bulk of messages and links are posted in the comment section of the posts of the user. Nowadays, lottery spam and job offer spam are also on the rise trying to track the user's sensitive data for commitment of financial fraud. Financial spams like cheaper loans and higher return investment plans are also on the rise for commitment to financial fraud. If we look at the statistical data by Kaspersky, India is ranked in the top 5 global countries when it comes to spamming consisting of 4% of total global spam volume. A study by True caller revealed that India is in the top nations where an average Indian receives more than 20 spam monthly. In the year 2022 WhatsApp detected and blocked nearly 5 billion spam messages. Facebook in the year 2022 reported that it removed more than 1 billion spam accounts from its application where most accounts were originating from India. According to CERT-in, the Indians in the past years due to trapping in spam Emails and SMS lost millions of Rupees. Spamming is an easy route to block the victim's digital online communication but is also considered as a significant danger to the user's privacy. The Indian government to combat and counter spamming actively participates with updated and modern regulations and public awareness campaigns and drives, but the changing nature of cybercrime is still a challenging issue for law enforcement agencies.

[7]Cyber Laws in India

In May 2000, both chambers of the Indian parliament approved the Information Technology Bill. The President signed it into law in August 2000. These laws are now referred to as the Information Technology Act, 2000 (IT Act), and they serve as the foundation for cyber laws in India. The primary objective of the IT Act is to establish a legal framework necessary for the advancement of e-commerce and other electronic transactions in India. Businesses need to have a detailed understanding of the IT Act and its provisions.

The IT Act, 2000 also defines electronic records and electronic transactions and allow agreements made through the transactions through electronic communication. This body of law helps to encourage growth of the digital economy by defining the necessary legal environment that facilitates the online business. Most importantly, where parties have conducted the formation and acceptance of contracts through electronic media, the latter is legally enforceable unless otherwise agreed.

Key provisions of the IT Act include: -

(a) **Chapter II:** This section indicates that an electronic record can be authenticated by attaching a digital signature. It also enables the verification of electronic records through the public key linked to the digital signature.

(b) **Chapter III:** concentrates on electronic governance, specifying that any legal obligation for information to be in writing or printed form is fulfilled if the information is accessible electronically and can be referenced in the

[7] (June 19, 2017), https://www.southcalcuttalawcollege.ac.in/Notice/50446IRJET-V4I6303.pdf.

future. This chapter emphasizes the legal recognition of digital signatures, granting them equivalent status to traditional handwritten signatures in digital transactions.
(c) **Chapter IV**; Describes the responsibilities of the certifying authorities' controller. This person monitors what certifying authorities do, establishes rules for them, and specifies how they should operate. It also details the types of digital signature certificates and allows foreign certifying authorities to be approved. It explains how licenses for digital signature certificates are granted.
(d) **Chapter V**: Describes what makes electronic records secure and what makes digital signatures secure.
(e) **Chapter VI**: provides information regarding the guidelines and procedures followed by certifying authorities concerning rules and regulations along with their functions.
[8](f) **Chapter VII**: briefly explains the framework that relates to digital signature certificates and the obligations of subscribers.
(g) **Chapter VIII**: It gives more details about the responsibilities of the customers as outlined in the law.
(h) **Chapter IX:** concerning sanctions and decisions that refer to different sorts of violations. It sets maximum compensation for loss to Computer or computer system at Rupees One Crore only. The law states that adjudicating officers must be appointed and they should be at the level of a director in the Indian government or a similar officer in the state. These officers have the power to judge violations under the law and have the authority of a civil court.
(I) **Chapter X**: The Cyber Regulations Appellate Tribunal is created to review decisions made by the adjudicating officers.
(j) **Chapter XI**: The document lists different crimes that are covered by the law, and these must be investigated by a police officer with the title of at least Deputy Superintendent of Police. Some of the offenses mentioned are altering computer files, posting indecent material online, and unauthorized access to computer systems.
(a) **Section 66**: The term "hacking" has been replaced with "data theft. " It clarifies that hacking is performed with the owner's consent, while cracking is deemed a criminal offense.
(b)**Section 66a:** this section pertains to sending offensive messages through electronic communication, including the act of sending deceptive emails to mislead the recipient regarding the message's origin, commonly known as email spoofing. Breaking these rules can lead to a punishment of either being jailed for a maximum of 3 years or paying a fee.
(c)**Section 66B:** Individuals who unlawfully obtain stolen computer resources or communication devices will be subject to an extreme of 3 years in prison, a fine of up to ₹1 lakh, or both.
(d) **Section 66C**: Committing identity theft by using another person's password or electronic signature can result in a maximum of 3 years in jail, a penalty of ₹1 lakh, or both.
(e) **Section 66D:** Using a computer or communication device to cheat by pretending to be someone else can result in being put in jail for a maximum of 3 years or being fined ₹1 lakh, or more.
(f) Section 66E: Breaking someone's privacy by sharing personal information or content without their permission can result in a jail sentence of up to three years, a fine of ₹2 lakhs, or both.
(g) Section 66F: Engaging in cyber terrorism, such as posing a threat to the unity, security, or sovereignty of the country, trying to access computer systems without permission, or infecting computers with harmful intent to endanger lives, can result in a sentence of life in prison.
(h) Section 67 of the IT Act covers the sharing or sending of inappropriate satisfied in digital arrangement, now including child exploitation within its range.

Under the Indian Penal Code (IPC), identity theft and cyber fraud are punishable offenses. Relevant sections include: -
(1) **section 464**: creating a false document or electronic record.
(2**) section 465**: penalties for forgery.
(3**) section 468**: forgery of an electronic record intended for deceit.
(4) **section 469**: forgery of an electronic record aimed at damaging reputation.
(5) **section 471**: utilizing a forged document or electronic record as if it were authentic.

[8] Cyber Laws, Ministry of Electronics and Information Technology (Dec. 8, 2023), https://www.meity.gov.in/content/cyber-laws.

[9]Changes in IT Act 2000

The following provisions should be considered:

a. Trap and Trace Orders:

The new IT Act would make it easier for cyber agents to get "trap and trace" orders. Trap and trace strategies capture incoming IP packets to find out where they come from. Since hackers can easily fake their true locations, the best way to follow the path of a virus, DoS attack, or hacking incident is by using trapping devices that record the original malicious packets as they go through each router or server. In the past, it was simple for investigators to get these orders when dealing with just one telephone company. But now, with modern communications involving many different companies, tracking becomes more complicated. If part of the route goes outside the jurisdiction of one court, investigators must ask the next jurisdiction for a new trap and trace order for that part. The proposed law should allow for one order to trace a whole online communication, no matter what jurisdictions are involved.

b. **Young Perpetrators in Serious Computer Crimes**:

The new legislation should propose that individuals aged fifteen and older be held accountable for serious computer crimes. This provision seeks to make sure that whenever a young offender is involved in the computer crimes mentioned above, he/she is adequately dealt with in the law.

c. **Regulation of Cyber Cafes and Computer Training Centres**:

Places such as internet cafes, computer schools, and any other location that uses computers for training should be controlled by creating new laws. This will make sure they are properly monitored and enhance the safety measures in these places.

Advantages of Cyber Laws

The IT Act is a legislation intended to modernise archaic structures of legal systems and combat crimes with technological influence. This is very useful when it comes to the protection of people's financial information especially while undertaking online transactions such as use of credit cards. It affords legal recognition to an electronic record, meaning that it cannot be refused legal acceptability, efficacy or enforceability, all because that record is in electronic form. Taking into consideration the fact that a significant volume of transactions and communications occurs in electronic environments, the act grants the government departments the authority to accept, create and retain official documents in electronic media format. Additionally, it also gives official approval to digital records and their authenticity by using electronic signatures for confirmation and validation.

From the viewpoint of e-commerce in India, the IT Act 2000 offers several key advantages: -

(a) The courts now accept emails as lawful, acceptable legal communication that can be used in court as evidence.
(b) Commercial ventures can affect electronic transactions according to the legal provisions espoused by the Act.
(c) Digital signatures have been given the recognition and the validity of the law.
(d) The Act thus allows corporate entities to become certifying authorities for engaging in the said business of issuing digital signatures certificates.
(e) This also benefits the public as words can now be forwarded by the Government departments through the web thus fostering e-governance.
(f) Companies are permitted to deliver forms, applications, or any other documents to the governmental bodies in the electronic format in compliance with the set requirements.

The Act also deals with other important security issues which are crucial in the effective implementation of e-transactions. Although, it legally prescribes what is a secure digital signature, which must adhere to security standards laid down by the government. Also, with the enactment of the provisions of IT Act, corporations have legal recourses wherein they can approach the court for monetary compensation for loss or theft of data and or loss due to computer misuse and hacking.

India has made notable strides in enacting technology-related laws, yet there is still considerable work required to ensure these laws evolve in tandem with technological advancements. As technology use expands, the demand for comprehensive regulatory frameworks intensifies. While India has made considerable progress in this area, existing laws still contain gaps that need addressing. The following outlines the major shortcomings in the technology-related laws:

[9] https://www.hindustantimes.com/india-news/amendments-to-it-act-decriminalise-offences-increase-penalties-101701517892813.html.

[10]Legalization of Technology and Data Protection laws in India Some of the ambiguities in Technology and Data protection laws.

Loopholes of cyber law

[11]Loophole 1: Ambiguities in Data Protection Regulations: Regarding the Indian laws about data protection there is certain rules known as the Information Technology Rules which were framed in the year 2011 with some modifications introduced in the year 2018. Still, these rules pay a certain attention to the question of how to protect personal data, but they do not explain what kind of information would be considered as 'sensitive personal data'. This makes it difficult for businesses to follow the set rules and makes the consumers to be worried whether their personal data is safe or not.

Loophole 2: Outdated Cybercrime Legislation The legislation of the Information Technology Act 2000 defines cybercrime in India but has not adapted itself with the advancement in technology. Despite being amended in 2008, it does not cover areas of interest that have evolved with time such as 'revenge porn,' which is the sharing of obscene materials without consent. The most significant issue arising from this is the failure to have well-defined laws for these acts leaving the general prosecution and protection of people involved in jeopardy.

Loophole 3: Inadequate regulation of digital content This is especially the case given the fact that digital content such as movies, television shows and music is immensely popular in India but remains mostly uncontrolled. Whereas there are certain rules for movies and television programs, the content available on the web is not highly regulated. This gap allows for the sharing of restricted content such as pirated works and films and allows for such materials which incite hate speech which are not well regulated.

Loophole 4: Insufficient Social Media Regulation Although social media is an inseparable part of today's life, India lacks proper laws and regulation of social media. This way current guidelines are lacking, and many problematic phenomena appear misinformation, hate speech and cyberbullying. The above-mentioned legal loopholes encourage the use of social media to incite violence; an aspect that is till this date not well covered for by the existing laws.

Loophole 5: Gaps in E-commerce Regulation Gaps in the regulation of E-commerce. Although there are general measures that can be adopted by the e-commerce firms, there is no legal regulation of the same. This creates issues like a lack of scrutiny in fraudulent transactions and where consumers' rights are barely protected; this makes the buyers vulnerable to fraud and poor services.

Loophole 6: Limited Regulation of Fintech Sector Online payment gates and other services, electronic wallets, and P2P lending are considered as the modern and rapidly developing sectors in India. But this comes with shortcomings of regulations which are insufficient at times of fraud and data break-ins. There, however, is need for a more strengthened legal basis in an endeavour to deal with these problems.

Loophole 7: Weak enforcement of existing laws Technology laws of India face enforcement issues that arise due to shortage of equipment, inadequate infrastructure, and low consciousness of the legal authority. The extent of enforcement that currently exists is insufficient, thus allowing cybercriminals to somewhat act without much consequence since the likelihood of detection and subsequent prosecution is very low.

Loophole 8: Deficient International Cooperation Cybercrime always has a cross-border nature making it abnormally hard to combat. Lack of international cooperation weakens the ability of law enforcement agencies to arrest and prosecute offenders who operate in different jurisdictions. There is need for cooperation especially when having to deal with transnational technology-related crimes.

Social Impact of Cyber Crime

Crime, as one of the inherent problems in any society results in touching every segment of the society in as much as no state or social structure can claim to be free from the vice. Offenders act in not only the real environment but also more and more in cyberspace. Computer criminality has continued to rise and with this it has led to

[10] Technology Laws in India: Impact and Loopholes, https://www.legalserviceindia.com/legal/article-10604-technology-laws-in-india-impact-and-loopholes.html.

[11] Legal gaps and concerns abound as cybercrime rises unabated in India, (Jan. 1, 2024), https://ciso.economictimes.indiatimes.com/news/cybercrime-fraud/legal-gaps-and-concerns-abound-as-cybercrime-rises-unabated-in-india/106434980.

significant loss in all aspects of people's life as well as businesses.

Cybercrime has many and multifield effects. On this front, people suffer from identity theft and credit card fraud while businesses in entertainment and software lose their revenues to piracy among other vices. Piracy is rife and virtually everyone can download software programs and other creative work without necessarily paying for it. In addition to claiming measurable monetary losses, such cybercrimes as cyberbullying, defamation, pornography, and stalking causing damage to countless of victims. Privacy is largely an issue in the social media; persons' details or private images are likely to be posted to the social media without their consent with threats of increased violence, blackmails among other worse forms of vices. Women and teenagers are more vulnerable to these cybercrimes as they are most likely to be bullied, defamed or sexually exploited online. Cybercrimes eruptions cut across all society sister sect and thus the need for enhanced mechanism to protect society personalities from the wrath of cyber criminals in the digitized world.

[12]Cyber security challenges with the judiciary and other Indian authorities.

India has the largest population in the world about 1.5 billion do have almost internet users almost half of the population or we can say more than 800 million users of the internet. such easy approach to technology to such a huge population, the nation also faces a rapid increase in cybercrimes which range from data theft to attacks on digital infrastructure. To handle such large and complex cases requires strong legislation which does empower the law enforcement authorities and judicial authorities but when we look upon the current legislation and other enforcement laws India does lack the ability to resolve cybercrime and faces several challenges lack of technical expertise with the Indian authorities, inadequate and delay in legal proceedings, legislative loops, lack of cyberinfrastructure and most important lack of cyber awareness with the public which do motivates the criminals to do the crime again and again.

- An overview of the technical expertise of the Indian judiciary and Indian authorities.

Cybercrimes such as phishing, ransomware, cyberbullying, cyberstalking, data theft, identity theft, etc. such crimes do contain technical bars like encryption, blockchain systems, advanced hacking, digital forensics, technical mechanisms etc, this is the complex nature of the cybercrimes which do changes in some time and in India, the judicial authorities and the law enforcement officers do lack the knowledge of cyber security and working with such complexities. There can be many reasons for such incompetency with Indian authorities like the training of the authorities and officers which might be outdated an insufficient in considering the current scenario. A UNICEF 2019 report revealed that only 32% of the Indian authorities who are connected directly or indirectly received any form of training related to cyber security. Yet such a lack of expertise does result in digital misinterpretation of data evidence, reliance on external experts for the cases, and delayed proceedings.

For the authorities to investigate cybercrime cases they need digitally advanced equipment and digital forensic laboratories to solve complex digital loops and data information but in India, there are not sufficient digital labs across the nation they are distributed very unevenly across the nation and many states must rely upon the centre labs for the investigation and the reports. These types of expertise issues do cause delays in cyber cases as these limited labs are already over burden. In the year 2022 the CAG of India stated in a report that 75% of the cybercrime cases in the investigation procedure do have delays and backlogs due to a lack of technical expertise and digital labs are not enough and evenly distributed to carry over the burden of the huge number of cases. Even if the reports and technical analysis of the cases are done in the judicial proceedings the prosecutor, the judges and other officers do face struggle and complexity in the interpretation of law and other regulations. Such a lack of knowledge and other technical understanding do result in insufficient legal representation of the victims and sometimes misapplication of the laws also happens due to a lack of understanding of the technical part of the case. These problems arise due to a general lack of cyber security training and education in the judiciary and law enforcement agencies. Such incompetency does result in the authorities remaining unfamiliar with the changing technology like the tech jargon, nature of cyber-attacks, and how to deal with new types of cyber-attacks. A 2019 report by the Ministry of Home Affairs revealed that only 20% of the Indian police personnel received any training or education in cybercrime cases and the number is even lesser with investigation of digital forensics.

[12] vikaspedia Domains, http://vikaspedia.in/education/Digital%20Litercy/inf ormation-security/cyber-laws.

- [13]**Inadequate technical infrastructure and technical reso**urces- for an adequate level of disposal of cases, courts do need enough vacancies in accordance with the burden of cases But as we look upon the data of 2023, more than 5000 of the judicial officer's posts are lying vacant in the lower courts and about 30% of the sanctioned judge post for the high courts of India are lying vacant, even the supreme court of India do have lot of burdens as it also struggles with the backlogs and delay of the cases. When we talk about the burden on courts as to final disposal of the cases, more than 3.5 crore cases are pending in the lower courts of India whereas more than 50 lakh cases are pending in the high courts of India and more than 70,000 cases are pending in the supreme court of India, comprising of more than 4 crore cases pending all over the nation the main issue with such a high pendency and delay in disposal is mainly due to the vacant posts and need for more vacancies to be filled for the judicial officers as to lower the burden and fasten the disposal of cases. The infrastructure of the Indian courts does lack basic amenities like seating arrangements, and drinking water is not available. When we talk about the digital infrastructure of the nation like e-courts which do have made progress like most of the courts do have VC facilities and digital evidence storages and other basic computerised mechanisms. But the problem arises when it comes to the digital training of the judicial officers, a study by the Vidhi centre for Legal Policy found that about 34 % of the judicial officers of the lower courts are comfortable and can use digital technology in courts which results in the underutilization of the current existing digital resources. The e-courts project had achieved success, but it also failed to cover the rural courts of India which do work on the same old manual pattern. Even if the rural courts do have the digital resources, they still have the internet issues and create difficulty to the working of rural courts in India. Such problems are faced due to a lack of funding for the development of the judicial infrastructure, only 0.1 % of the GDP is allocated to the judicial infrastructure which stops the new infrastructure to created and the current infrastructure to maintained. Inadequate infrastructure, lack of digital resources and overburdening of the cases do create an impact on the justice delivered.

- [14]**Lack of cyber awareness among the public**- India has witnessed a digital revolution over the last decade. India has the largest population in the world do has a significant number of internets who have increased over a period. The Telecom Regulatory Authority of India (TRAI) has issued a report where it stated that India has more than 800 million active internet users in the nation which makes it the 2nd largest internet consumer all over the globe. whereas, if we look at the cyber awareness of people is does not make a balance with rapid internet usage. The growth in cyber technology has also resulted in many cyber threats to the country. According to a report of 2022 by Norton Life Lock about 59% of internet users lack basic cyber knowledge like having strong passwords, how to secure private digital information, and recognition of phishing attempts. These data reveal that there is a huge gap between the usage of the internet by the people and the cyber awareness they have. When we about the reason for such lack of awareness it comes out the digital illiteracy among the people. Despite the initiatives by the government like “Digital India”, people living in the rural and semi-urban areas of the nation still lack awareness of safe internet practices. In a 2022 survey by the Data Security Council of India (DSCI), almost 70% of rural internet users do not understand the potential risk of cyber threats and later they are the victims of cybercrimes. The cyber awareness amongst the people not only includes the rapid usage of technology without having knowledge but also considers what steps a victim should take after committing such a crime. Cyber Peace Foundation in the year 2023 reported that more than 60% of the victims of cybercrime do not know how to report cybercrime and where to report the cybercrime, they do not have the basic knowledge of the same technology they use. Because of these gaps in awareness and usage, cybercrime increases day by day making it a challenging situation for the cyber security authorities to counter the crimes resulting in a lack of evidence and delays in procedures. The Indian government has launched several initiates to spread cyber awareness like Cyber Swacchta Kendra (Cyber Hygiene Centre) to spread the cyber awareness among people however the reach of such programs has been limited to a few people and most of the people are still not able to cope with the usage and awareness

[13] Untitled, (Mar. 14, 2012), http://www.unipune.ac.in/university_files/pdf/old_papers/oct2011/law/diploma_cyber_law_oct2011.pdf.

[14] Microsoft Word - ijtsrd48, (Apr. 13, 2017), https://core.ac.uk/download/pdf/266990702.pdf.

issue. There is an urgent need for awareness programs and education for people to combat cybercrimes and be able to use digital technology safely.

Due to the rise in cybercrimes, the judiciary, as an independent institution, plays a vital role in addressing these conflicts.

(1) In the case of Avnish Bajaj v. State (NCT of Delhi), 2004 Bazee. com case:

The CEO of Bazee. com was arrested after the sale of an obscene CD on one of the sites of this platform. This CD containing such vulgar material was also available in the markets across all the major localities of Delhi. In this case, Mumbai Police intervened along with Delhi Police wherein the accused was charged under Section 67 of the Information Technology Act, 2000 and Section 292 of the Indian Penal Code. But after that, he was let off on bail. These issues brought legal complexities into focus, especially in relation to the difference between an ISP and the content provider. The main area of concern was the ability of the accused because this was not a case of the creator of the contents but rather a service provider. Since then, this case has brought further talks as to what extent online platforms bear the responsibilities and the legal complexities involved in trying to differentiate between the 'distributors' of content and 'publishers' of content.

(2) Syed Asifuddin v. State of Andhra Pradesh

In this case, the individuals were accused of breaking the law under the Copyright Act and IT Act. The High Court of Andhra Pradesh clarified the requirement for service providers to assign a unique code to each device used to provide services, as stated in Section 2(1) of the IT Act. The court ruled that changing the electronic serial number (ESN) of a device falls under Section 65 of the IT Act, which classifies a mobile phone as a computer according to the law.

(3) Bank NSP Case: State by Cyber Crime Police v. Abubakar Siddique

This case involved a bank trainee who was getting ready for marriage. Both the trainee and his fiancée utilized the bank's computers. After their relationship concluded, the fiancée established a fraudulent email account under the name "Indian Bar Associations" and utilized the bank's computer to communicate with the bank's international clients via email. These emails inflicted considerable damage on the bank, resulting in the loss of multiple clients who later initiated lawsuits against the institution. The court determined that the bank was responsible for the actions, as the emails were generated from its system.

(4) My Space Inc. v. Super cassettes industries ltd

In this case, the court underscored the necessity for a coherent interpretation of sections 79 and 81 of the IT Act in conjunction with sections 51(a)(ii) of the Copyright Act. It was determined that although section 81 does not supersede the safe harbour protections granted to intermediaries under section 79, actual knowledge of infringement is required for liability, and general awareness is inadequate. Intermediaries are liable only when they possess specific knowledge of unlawful content.

(5) State of Tamil Nadu vs. Suhas Kutti

The victim, who had gone through a divorce, was repeatedly bothered by annoying phone calls. These calls started because of a harmful and inappropriate message posted in a Yahoo group, as well as emails that were forwarded. The offensive message led others to mistakenly believe that the victim was asking for that kind of attention. The person responsible for posting the message was a family friend of the victim who wanted to marry her. The Additional Chief Metropolitan Magistrate found the accused guilty under certain sections of the Information Technology Act, 2000, and the Indian Penal Code. The court sentenced the accused to two years of tough imprisonment. This case shows that cybercrimes are becoming more common and are being handled by courts at all levels in India.

[15]Cybercrime in India requires a positive approach and steps involving legal and technological measures. Here are some steps by which India can strengthen its cyber security.

- **Creation and need for a dedicated cybercrime police force**- over a period India has witnessed a significant rise in cybercrime as a part of technological advancement. Cybercrimes such as phishing, data theft, ransomware, hacking, and cyberbullying have been done to target individuals and organizations. Such criminals even operate from outside India making a complex technological issue creating difficulty for the law enforcement authorities.

[15] Cyber crime affects society in different ways, https://thefinancialexpress.com.bd/views/reviews/cyber-crime-affects-society-in-different-ways.

The current existing police force in India lacks the specialized skills required to solve the complex technological investigation and gathering of evidence as a part of the procedure. Specialized. The rapid revolution in cyber threats has been an alarming call for the authorities and makes its essential to have a dedicated cybercrime task force that is well-equipped to handle such complex technological crimes. Such a dedicated police force must have officers who are well-trained in technological parts like cyber forensics, digital evidence handling, ethical hacking, and other technological advancements. The role and power must be to that level that they are able to connect with other national and state authorities and able to investigate without delays in the procedure. When it comes to the ground level there have been cyber cells working at district and state levels and some kind of facilities for the rural people to have ease in reporting the crime without delaying of time. The national crime reporting portal is good at first instance but there must be a ground existence of such cells for local level assistance and to curtail enough information regarding the crime. A dedicated cybercrime police force will play a crucial role in the enforcement of the new data protection laws. By providing training, having adequate infrastructure and digital facilities India can build a cybercrime task force that not only manages the current crimes but will also get ready to counter future attacks.

- **Public awareness and education in cyber security**- India has undergone a digital revolution during the last decade resulting in more than eight hundred million active internet users but this revolution happened so fast that it created a lack of awareness with the public about what things to consider when using these technologies. Public awareness programs can play a crucial role in empowering individuals and organizations to safeguard their digital identity. The people to have knowledge of a certain topic education also plays a critical role in enhancing cyber awareness and securing the future of the people and students. With the increased use of technology, students are generally the targets of cybercriminals. The government, the non-governmental organisation, and the private sector can come together to organize workshops seminars, and camps to spread knowledge and awareness regarding cybersecurity. and Having cyber security added to the curriculum of schools and universities, will help a whole generation to be digitally literate in understanding the cyber risks like the use of strong passwords and multilevel authentication, lessons on the legal use of technology, their restrictions, safer online interactions which will help the students to develop habits regarding good use of technology and how to avoid getting trapped into the cybercrimes. The most important benefit of cyber education will be that it creates a workforce that is skilled in cyber technology and can defend against complex cybercrimes.

- **[16]The need for enhancement of cybersecurity infrastructure in India-** with the rapid digital revolution and technological advancement in India, it has made a crucial need to have a digital infrastructure to safeguard the national security of the country, to protect the data and data privacy and to have the smooth economy in the nation. A digital shift has been seen in healthcare, banking, financial, corporate, and governmental sectors where dependency is seen, resulting in an increase in cyber threats. Hacking, phishing, ransomware, and data theft have increased over a period resulting in not only financial losses but also a threat to the national security of the nation. For the detection and prevention of such crimes can be done but with a change in the digital infrastructure of the nation. The Indian cyber infrastructure faces an immediate need to have a good digital infrastructure but today we see challenges like outdated infrastructure, lack of encryption, lack of security protocols, and faces significant shortage of cyber security professionals. The updated infrastructure may include regular updating of hardware and software, enforcing good security protocols for all sectors, and ensuring that all public and private sectors use the latest cybersecurity technology. If a nation has good infrastructure for its cybersecurity, then it can protect the most confidential information like defence, finance, energy, and telecommunications because attacks on these sectors will directly impact the economy and the national security of the country. A critical component of having good digital infrastructure is the establishment of specialized cyber cells across the nation and the establishment of digital labs. The cyber cells are the ground-level point for the cyber investigations. These cyber cells and offices must that up to date to handle all major cybercrimes. Further, the digital labs will help identification of accurate digital shreds of evidence by cooperating with law enforcement agencies. Alongside, the digital infrastructure development, there is a need for fast-tracking cyber procedures. If the infrastructure is competent enough then it will help in the procedure of law and also assist the enforcement agencies. Currently, the judicial and investigative

[16] (Sept. 27, 2024), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7927777/.

procedures are slow because of a lack of knowledge and infrastructural issues. The Digital Data Personal and Data Protection Act facilitates the procedure with grievance redressal by the Data Protection Board which will address the complaints regarding the data breach and violations. India with a strong digital infrastructure will help combat the rising cybercrime and will strengthen the nation and its safety.

- **Promotion of research and development in cybersecurity**- Due to the digital revolution and technological advancement in the cyber world. It had been a major need for a nation like India to have research and development (R&D) a top priority. India is expected to have a $1 trillion digital economy and technological advancement by the year 2025 which is an inviting call for cybercriminals. To counter these threats India is actively investing in R&D for the development of advanced cybersecurity solutions. If we look at the statistical data by NASSCOM, India is expected to grow its cybersecurity economy by $13.5 billion by the year 2025 with a CAGR of 21% annually. Over the period, the government has recognized the importance of a cybersecurity framework in India, where the government has launched the national cybersecurity policy and National Cyber Coordination Centre (NCCC) to improve its cyber defence capabilities. The government of India is also fostering collaboration between academic institutions and research organizations to promote innovation in cybersecurity. Institutions like CERT-in and DSCI are the recognized research organization for cybersecurity. The Ministry of Electronics and Information Technology has allocated a cybersecurity R&D fund to support the projects and research on AI threats, secured payments, and blockchain technology. One of the best advantages of having R&D on cyber technology is the development of indigenous cybersecurity solutions that are tailored to the unique cyber threats in India. Further, having good R&D will produce a skilled workforce in cybersecurity who will handle complex cyber threats and issues. Indian startups like Sequester and Wi Jungle have been able to provide advanced cybersecurity solutions globally, these initiatives have played a vital role in combating the cyber threats analysis and making the country to pre-empt the threats. A sustained investment in R&D and strong legislation will help the nation to build a strong cybersecurity ecosystem which it will help the nation to safeguard its digital assets in future too.

International Framework

European Union and Indian approach to cybersecurity.

The European Union has a good framework for cybersecurity covering major areas like data protection and privacy concerns, their adopted legal framework, and their policies whereas in India, the development of cybersecurity is still an ongoing process.

The General Data Protection Regulation (GDPR) is the basis of the EU cybersecurity framework which provides a strict approach towards data protection and data privacy. This regulation focuses on individual rights over data protection and data privacy, data processing, and enforcement of strict penalties for non-compliance with the regulation. At the same time, India's primary legislation for cybersecurity is the IT Act, of two thousand. This act includes cybercrimes and e-commerce, it also includes provisions related to basic data protection, but it lacks the EU approach of cybersecurity and GDPR provisions like data processing and individual rights. However, a new data protection act has been introduced in India for a more organized approach in terms of data protection. The Digital Personal Data Protection Act, of 2023 provides a stricter approach to data processing which includes localization of data, consent requirements, and the individual rights of the user. The new legislation is revised a few times and is currently delayed by the government but still, it is not as comprehensive as the GDPR provisions. When it comes to the comprehensiveness of both the regulation of GDPR is likely to be more detailed where it covers all major aspects of data protection and data privacy but the Indian IT Act and DPDP Act, 2023 are less detailed not covering all major aspects of data protection and data privacy and still lacks in enforcement mechanisms. The EU approach to data privacy aims to have lawful, fair, and transparent requirements and stricter penalties for non-compliance. The IT Act, of two thousand is an outdated law covering only the basic provisions of data protection, and if we talk about the new legislation, it enhances data privacy, access, and rectification process. However, it is still a less strict approach than GDPR. India to a positive approach towards cybersecurity and standards and compatible enough with the GDPR, India needs to adopt a more detailed framework covering all major aspects of the cyber world, establish strong mechanisms and enforcement agencies, and align itself with international cooperation in cybersecurity.

[17]Right to privacy and data protection

The General Data Protection Regulation (GDPR) provides the rights of people over privacy and data protection and ensures people have pervasive control over their personal data like the right to access the personal data of people held by the organizations, the right to be ratified, right to be informed over the usage of personal data of people, right to data portability, it most important right is over the consent of the user, where the companies or the organizations must take the full consent of user before data processing. If we look at the non-compliance of these rights, then the penalty goes for 4% of the company's global turnover or 20 million euros whichever is greater. But when we talk about the Indian legal framework, the primary legislation, the Information Technology Act, of 2000 after the amendment of 2008 provides basic rights over data protection and privacy regarding cybercrimes. Currently, the new Digital Personal Data Protection Act, of 2023 aims at a wider aspect of cyber rights to its citizens like codification of data portability, data erasure, and the right to access which is like the rights provided under the GDPR provisions. The proposed legislation also aims to provide consent-based data processing, which is a very positive move, but it comes with an exception of access by a government authority or when the question is of national security. Enforcement of the Data Protection Authority (DPA) will regulate and oversee the DPDP Act, of 2023. When we look at the difference, or what India still lacks even after the enactment of new cyber laws, it provides power and access to personal data to the government for situations like national security or state governance. Whereas, if we talk about GDPR, focuses on individual rights of personal data and consent-based rights for its citizens.

The GDPR works on robust mechanisms of enforcement of the laws and imposes hefty fines and penalties for global organizations for example, Google was fined by the European Union of 50 million Euros for non-compliance with transparency provisions and consent-based issues. While we look at India, the new Data Protection Act puts heavy penalties on non-compliance with the provisions but is considered modest in comparison to the international standards. Imposing heavy costs will apply when India does not have a specialized authority and adequate digital infrastructure for cybersecurity. However, the new data protection law aims to provide in reduction of gaps in cybersecurity and cybercrime. The Indian legal framework allows the government to access personal data without consent which can make a situation of government surveillance. This kind of exception can lead to conflicts between individual privacy and governmental control over personal data. India at its place is making development in its cybersecurity by considering the GDPR provisions as significant for India but is still lagging behind the European Union. Currently, India is moving towards a balanced approach focusing on the protection of personal data rights and national security.

There are some steps by which India can improve its cybersecurity considering the GDPR provisions like the alignment of the Indian legal framework with GDPR and strengthening the centralized governance which can coordinate between various agencies regarding guidelines and protocols. Introducing a certification framework for digital and technological products ensures that cybersecurity is built into the design like the GDPR provisions. Improvement in the incident reporting sector like quicker response teams for most cases will help in a better and faster way. A key step for India would be enforcing the DPDP Act, 2023 which will enhance the public-private partnership focusing on smoother technological development and a public who is aware of cybersecurity. Learning from the EU and the GDPR, India can enhance its cybersecurity match the global standards and move towards a safe digital economy.

Conclusion

Crimes related to cyberspace occur virtually in every country of the world, and states are taking different actions to address it. The new generation of users, born and raised within a generation of digital technology, often with the support of parents and caregivers who have also became active users of technology since the beginning of COVID-19 virus in year 2020. This had forced the reliance on digital technology in an enormous extent, and as a result cases of cybercriminal ties have been on high this period. For example, routine criminal acts include cyber bullying, defamation, and cyber fraud and scams. Most of the time such crimes take place because people have easy access to devices or compound the mistake of their users. There is still a high level of ignorance about cybercrimes in India, and when people get hacked, they end up losing their property without knowing why it has happened. Hence, it is necessary to increase people's awareness about such crimes and their rights in the

[17] Right To Privacy And Data Protection Era, https://www.legalserviceindia.com/legal/article-10664-right-to-privacy-and-data-protection-era.html.

information space. The fight against cybercrime in India involves various governmental measures; however, this has remained more of a challenge even today. In this respect conscious efforts are being made to see that victims are compensated and get justice.

References

1. Etter,B. (2001), The forensic challenges of E-Crime, Current Commentary No. 3 Australasian Centre for Policing Research, Adelaide.
2. Etter B. (2002), The challenges of Policing Cyberspace, presented to the Netsafe: Society, Safety and the Internet Conference, Auckland, New Zealand.
3. Eric J. Sinrod and William P Reilly, Cyber Crimes (2000), A Practical Approach to the Application of Federal Computer Crime Laws, Santa Clara University, Vol 16, Number 2.
4. Gengler, B. (2001), Virus Cost hit $20bn, The Australian, 11 September p.36.
5. The IT Act 2000.
6. Cyber stalking India, www.indianchild.com.
7. Cyber crime a new challenge for CBI, www.rediff.com, March 12, 2003 12:27 IST
8. Richard Raysman & Peter Brown (1999), Viruses Worms, and other Destructive Forces N. Y. L.