INDIAN JOURNAL OF LAW, POLITY AND ADMINISTRATION

ISSN: 2582-7677

LEGAL ISSUES IN CYBER SECURITY IN INDIA

REENU RANA

PARUL SINGH

FACULTY OF LAW, MSU BARODA

ABSTRACT

With the advancement of internet and technology cybercrime is becoming a major threat these days. Information technology Act 2000, does not define the word cybercrime clearly. Any crime which is committed by using an electronic device or a computer is placed under the category of cybercrime. While committing a cybercrime, the computer or the data contained in it is either the object used in the offence or is the target thereof. When Internet came into existence, it would never be thought of that such would lead to criminal activities requiring proper legislation for its regulation. The world of internet is termed as cyberspace whereas the laws that cover cyberspace are known as cyber laws. Due to advancement in technology, a number of cyber-attacks have been noticed through which the culprits make illegal money without leaving their homes. These cybercrimes necessitates cyber laws and the concern of government authorities in order to combat such threats. There are number of ways from making fraudulent transactions online to hacking the computer through which a person can become a victim of cyber fraud. Cyber laws are really important for all the individuals so that they can undergo online transactions without any threat of being becoming the victim of cyber fraud. National Cyber Security Strategy is being looked into in order to provide safety and security to internet users.

Keywords: *Cyber Space, Cyber Crime, Data theft, Cyber Laws, Cyber fraud, Hacking, Cyber Security.*

INTRODUCTION

The network of networks that uses technologies in order to transmit data between different networked computers for talking with each other by using the internet protocol (IP) is termed as

ISSN: 2582-7677

Internet. Every computer can talk as a peer with other computer on the network. This feature makes the internet very exciting but on the other hand it makes all its users vulnerable to cybercrimes. It was barely thought on the day when Internet came into existence that it would encourage frauds and criminal activities. Technology has its own pros and cons. It helps a person in almost every sphere of life and in return there are many challenges to it which one needs to overcome otherwise this technology would turn fatal. The greatest threat of technology to mankind is by cybercrimes. Cyber criminals abuse technology for giving effect to cybercrimes such as thefts and frauds. It is very difficult to avoid the cyber-attacks as the technology is still developing and that too at a very gradual pace. Our country is being driven towards a digitized phase by the Digital India Initiative.

There is a legal aspect of every activity undertaken by an individual in cyberspace.

One cannot assume life in today's world without internet. We do a lot of amusing things on internet but have to undergo a lot of trouble at the same time. Cybercrime is the curse of advancement of technology across the country. Cybercrime is a global phenomenon. It poses major threat to the security of a person as a whole. In this compact world, the internet is now considered as a part of globalization process which creates new opportunities and challenges associated with it. Internet has proved to be one of the greatest invention of mankind. However a major threat is caused by it to the society in the form of cybercrimes. The main victim of this transgression are the women and the children. At the Tenth United Nations Congress on Prevention of Crime and Treatment of offenders, cybercrime is defined as:

(a) In narrow sense, cybercrime is defined as any illegal behavior by means of electronic operations that targets the security of computer systems and the data processed by them.[1]

(b) In a broader sense, any illegal behavior committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network.[2]

There may be acts which are illegal in one country but legal in other. There is absence of set of comprehensive law anywhere in the world which is the greatest lacunae in this field.[3]

[1] *Virendra k. Pamecha, "The Cyber Crimes & The Cyber Law Be Aware and Beware Of!" pg. 17*
[2] *ibid*
[3] *Virendra k. Pamecha, "The Cyber Crimes & The Cyber Law Be Aware and Beware Of!" pg. 18*

ISSN: 2582-7677

Types of Cyber Crime

There are different ways by which the computer can be compromised and privacy of an individual can be infringed. Cybercrimes can be against person, property and government. Cybercrimes against persons include publication and transmission of child pornography, cyber stalking, trafficking and dissemination of obscene content, cyber harassment any many more. Child pornography is one of the most serious crime which if not controlled will leave irreparable scars on young generation. Unauthorized computer trespassing by way of cyberspace including computer vandalism, transmitting harmful programs, possessing unauthorized computer information are covered under cybercrimes against property. Cyber terrorism is covered under cybercrimes against government. Individuals and different groups use cyber space for threatening the international governments. Cyber space is used to terrorise the citizens of a country. Cyber terrorism is a premeditated use of disruptive activities or threat thereof, in cyber space, with the intention to further social, ideological, religious, political or similar objectives, or to intimidate any person in furtherance of such objectives.[4] Privacy violations, data theft, demolition of e governance base and network damage are the forms of cyber terrorism.

Most common types of cybercrimes as under:

1. **Hacking:** When an intruder access one's computer without taking permission is said to have committed the offence of hacking. The people who commit hacking are the hackers. Hackers are computer programmers having an expert understanding of computers and they misuse this knowledge for deceitful and illegal purposes. Hacking is basically computer trespass. Hackers can be divided into two groups on the basis of intention. (a) Hackers without any intention to do criminal activity. (b) Hackers with an intention to do criminal activity. There can be many reasons for such hacking. Some people do it for showing their expertise while others may do out of greed. Voyeurism may also be the reason behind hacking. Hackers intrude the system in order to extract personal information of the owner of the computer. Hackers who show destructive attributes are known as 'Crackers' or 'Black Hat Hackers'. On the other hand some companies hire computer experts who can find flaws in their security system and fix it off accordingly. Such computer enthusiasts are known as 'White Hat Hackers'. Some of the well-known computer geniuses like Ken Thompson, Dennis Ritchie, and Mark Zuckerberg were once hackers. In order to prevent hackers from accessing your system, it is necessary to know how hacking is done.

[4] *Virendra k. Pamecha, "The Cyber Crimes & The Cyber Law Be Aware and Beware Of!" pg. 20*

ISSN: 2582-7677

2. **Cyber stalking:** It is that form of cybercrime where a person is followed online. The victim is not followed physically by the cyber stalker rather the cyber stalker follows the online activities of the victim virtually in order to collect information about victim with the criminal motive to harass the victim. It is a kind of invasion on the online privacy of the individual. Mostly the victims of cyber stalking are women and children. A cyber stalker can be a stranger or someone who is known to the victim. Nowadays it is very easy to locate someone's presence by doing a Google search. The stalker by taking advantage of technology can easily extract information about the victim. The first conviction took place in Maharashtra in July 2015 in the case of Yogesh Prabhu v State of Maharashtra in Cyber stalking.[5]

   Cyber stalking is done in two primary ways:

- **Internet Stalking:** In Internet Stalking, stalking is done through internet. Sending obscene content and viruses by the stalker through email amounts to internet stalking. But this alone does not amount to cyber stalking. If the recipient is intimidated by sending email repeatedly or any other cybercrime by which the victim is harassed or threatened amounts to cyber stalking.
- **Computer Stalking:** Through Computer Stalking, the stalker gain unauthorized control over the victim's computer and this is done by controlling the working of the internet and the Windows operating system. Usually an expert stalker does such type of stalking but instructions regarding this can easily be taken from the internet.

  In today's world where social media platform like Facebook, Twitter, Instagram, YouTube, WhatsApp are so active, enough information is available about the victim without the victim being aware of it. Apps like 'check-ins' access the personal information, location and put it for information for all. People share almost every detail about their life on social networking sites and thereby giving way to cybercrimes.

3. **Cyber Pornography:** Making use of cyberspace for publishing, distributing or designing pornography is termed as cyber pornography. People can view thousands of porn on their laptops and mobiles due to easy availability of it on internet. Even pornographic content can be uploaded on internet. Once you share such content over a network, you enter into the dark world of cybercrime. Obscenity and pornography are widely used as synonyms for each other but in

[5] *Prasanto K Roy, 'Why online harassment goes unpunished in India'. 17 July 2015 (13 May, 2017, 4:30 PM), http//www.bbc.com/news/world-asia-india-33532706*

ISSN: 2582-7677

reality obscenity is a wider concept and pornography is a part of it. Obscenity includes immoral acts against the sentiments of people whereas causing sexual excitement through the medium of pictures, books or films is pornography. A lot of pornographic content is available on Dark web. Cyber pornography is banned in many countries. Production and distribution of cyber pornography is prohibited under IT Act but the viewing and downloading of cyber pornography is not prohibited unless it is not child pornography.

4. **Morphing**: In morphing, the original picture of a person is downloaded through the social media sites and then transformed into another image by using morphing tools that are readily available on internet. Such morphed pictures are then uploaded on other websites or porn sites so as to malign the character of the victim. The victims of morphing are mostly females and morphing is done with the intent to tarnish the image of the victim. Such type of cybercrimes are rising in India at a very high rate.[6]
5. **Malicious software:** Commonly used word for malicious software is 'Malware". Virus or worm, Spyware and Trojan horse are the types of Malware.

(a) The computer program or piece of code that circulates to other computers on the network that spreads from file to file and program to program is a virus. It runs against our knowledge and wishes. It damages the data, disrupts the computer operation, crash computers and corrupts the files of operating system. It can transmit across networks and bypass the security systems. Worms are very similar to virus. It is a program which has the ability to self-replicate till all the available memory is eaten up. For reproduction, they do not infect other files so they are not strictly viruses. They reproduce until the system collapses. They can be eliminated through antiviruses. Worms are carried through e-mails, chat and networks.

(b) Trojan horses are another breed of malicious code that neither self-reproduce like worms nor reproduce by infecting other files. They enter a computer through any channel and seems to be a harmless program. They are unknowingly installed while playing online games, visiting a website or internet driven applications. They can delete files and can destroy information on hard drives. They hamper the functioning of the computer like other viruses.

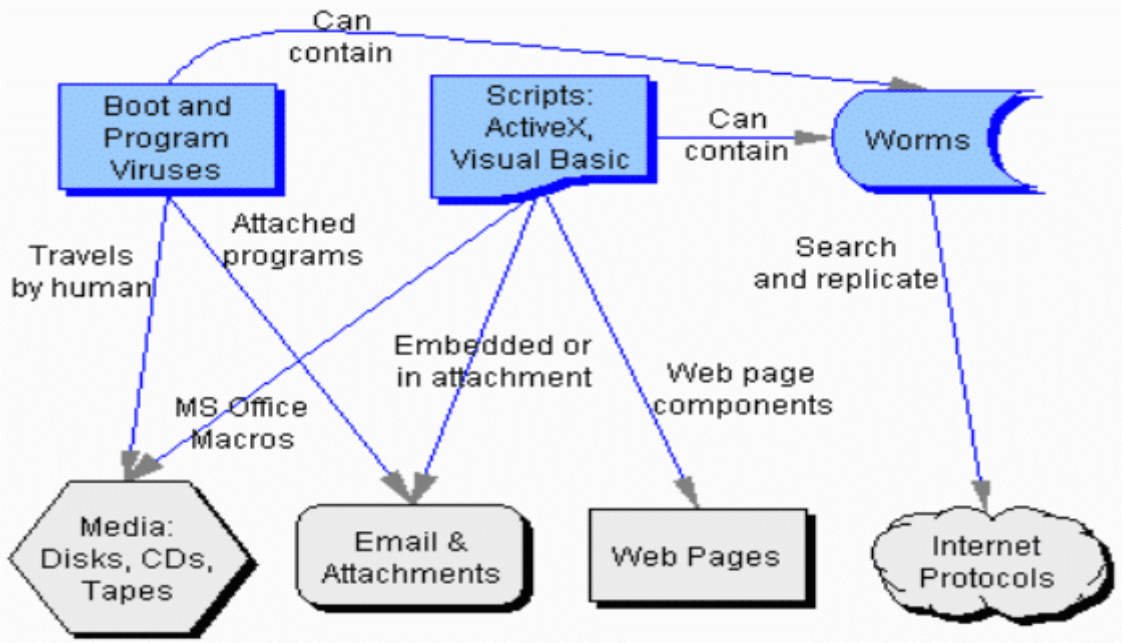
Spyware is an unwanted malicious software which we get by simply clicking OK to download program or it is installed along with downloading a free software. We should always have the knowledge of what we are downloading. The most common sign of spyware is pop-up

[6] *Cyber Crimes involving Morphed photos Rising, THE TIMES OF INDIA June 29, 2015*

ISSN: 2582-7677

advertising even when internet explorer is not open. Slow speed of operating system, changes in favourite list, modem always on run, change of settings which cannot be changed back, additional toolbars on the browser are all signs of spyware. Removable media or the internet are the spreaders of computer viruses. CD-ROM, flash disks, storage devices used in infected computers can infect all other computer where these are used.

A simple diagram to show how malware can propagate



6. **Cyber bullying**: It is harm done by done by sending messages of threatening or intimidating nature wilfully and repeatedly by using computers, cell phones or any other electronic devices. It is done when the superior strength or dominant position transmits intimidation or aggressive behaviour through electronic medium. India ranks third after China and Singapore in cyber bullying.[7] In India though the magnitude of cyber bullying of women is not known but it is frequently reported.
7. **Online Frauds**: Many times we receive e-mails promising to pay huge sums of money by way of rewards and lotteries. Such are the online frauds where the sender tries to trap the recipient into a fraudulent transaction. At times such e-mails carry attachments prompting the recipient to

[7] *T.E. Raja Simhan, India Ranks Third in Cyber Bullying, BUSINESS LINE, March 12, 2018*

ISSN: 2582-7677

click on it. These attachments can be a form of malware and in case the working of the computer.

Some common methods used in online fraud are as under:

(a) Fraudulent e-mail: Such e-mails tries to extract sensitive personal and financial information from the recipient. These appear to be as if sent by a legitimate bank.

(b) Pharming: In order to defraud the internet surfers, fraudulent websites are created which look identical to the websites of trusted companies or legitimate banks. These websites are also known as 'spoofed websites'. The motive behind such websites is to steal sensitive information. These websites do not begin with 'https' in the URL bar.

(c) Phishing: It is a type of online fraud where the recipient of the e-mail is lured to disclose personal information about himself/ herself. In order to protect yourself never respond to any e-mail requesting personal information.

(d) Vishing: It is a combination of voice and phishing. In phishing e-mail is sent for extracting personal information whereas in vishing phone calls or voice messages are sent representing themselves to be from reputed companies for getting personal information like credit card details and bank details.

ISSN: 2582-7677

(e) Smishing: It is a kind of phishing which involves text message in SMS or phone number. A number of people are aware of risks involved in clicking on links provided in e-mails. Such is not true when we talk about text messages. By sending such messages smishers try to get personal information from the receiver of text message. Such messages are sent from a number that does not look like a normal number.

(f) Lotteries: Fake lottery scams also try to get the personal information revealed when you try to collect your winning amount. In fake lottery scams you are persuaded that you have won a big amount of money in an online draw in lottery that you have never entered.

8. **Card related frauds**: In card related frauds, card of a person is used by another person for personal reasons without the knowledge of the owner of the card. Credit card fraud is an inclusive term for fraud committed using a payment card such as a credit card or a debit card.[8] Now-a-days internet has become a New World Market due to the expansion of trans-border or global socio-economic and political spaces capturing consumers from the countries around the world. So the level from which the fraudsters operate has become transnational. The techniques used for such type of frauds are as under:

(a) Site cloning: The entire site or the pages from which orders are placed are cloned by the fraudsters in this technique making the customers genuinely believing in that they are dealing with the real company with which they want to purchase their goods and services. The cloned site share the e-mail containing the receipt to the customer in the same manner as real companies do.

(b) False merchant sites: These sites offers extremely cheap services to the customer. These sites take customer's credit card details. These sites are generally linked to larger criminal network base which collects the personal information of the customers for committing fraud.

(c) Credit card generators: The computer programs through which valid credit card numbers and their expiry dates are generated are the credit card generators. Through credit card generators, a number of credit cards as the user desires may be illegally generated whether it be Visa card or Master card.

Need for Cyber Law in India

Cyber Law includes all legal and regulatory aspects related to Internet and World Wide Web. Cyber law applies to all the legal issues related to the use of technology in cyber space. Cyber

[8] *"Credit Card Fraud - Consumer Action" (PDF). Consumer Action. Retrieved 28 November 2017.*

ISSN: 2582-7677

laws are applicable to all the human activities in relation to internet. Violation of cyber laws would lead to action by the government in the form of imprisonment or fine or an order to pay compensation. Cyber law applies to all cybercrimes, intellectual property, data protection and privacy and electronic and digital signatures. Initially internet was developed as a research and information sharing tool. Later on it became applicable to a number of activities such as e-business, e-commerce, e-procurement and many more. Cyber law deals with all issues related to internet crime. With the spurt in e-commerce and online share trading, the incidents of cybercrime are on a rise.

Cyber law includes:

(a) Information Technology Law for regulating transactions related to the use of computer

(b) Communications Law for regulating telecommunications and broadcasting

Cyber laws are necessitated due to the growth of internet for various purposes that led to numerous legal issues. In the light of emerging cyber space, the existing laws of India could not be interpreted to include all aspects of cyber space. So need for cyber laws become inevitable. Cyber laws induces the people to do online transaction without any fear of misuse. As of now, there is absolutely no comprehensive law on Cybercrime anywhere in the world and for this reason the investigating agencies like FBI are finding the Cyberspace to be an extremely difficult terrain.[9]

A framework is provided by the Information and Technology Act, 2000 for the security of electronic governance through identification to electronic records and digital signatures. It also provide penalties for cybercriminals. A Cyber Appellate Tribunal is statutorily established to resolve the disputes related to Cyber Crimes and Online Frauds.

The Information Technology Act 2000 was implemented to keep legal jurisdiction over cybercrimes. The Act ensures that the information will not be denied on the ground that it is in form of digital records. Information Technology Act regulates the activities that violate the rights of an individual. Some of the sections of the IT Act 2000 as amended by IT Act 2008 that provide safeguard against cyber abuse are as under:

- Section 65 provides punishment for a person who intentionally conceals, destroys or alters any computer source code which is required to be maintained by law with an imprisonment of 3 or a fine of 2 Lakhs INR or both

[9] *https://infosecawareness.in/cyber-laws-of-india*

ISSN: 2582-7677

- Section 66 C makes identity theft a punishable offence. The offender shall be punishable with imprisonment of either description for a term which may extend to 3 years and fine which may extend upto Rs. 1 lakh.
- Section 66 D deals with cheating using computer source and punishes a person with imprisonment up to 3 years or/and fine up to 1 Lakh INR for cheating someone using a computer resource or a communication device.
- Section 66 E deals with violation of privacy of a person. The offender shall be punishable with imprisonment which may extend upto 3 years and/ or fine upto 2 lakh INR or both.
- Section 66 F deals with cyber terrorism. Acts covered under cyber terrorism are non bailable offences. A person can be punished with life imprisonment in case he/she denies the access to the computer resource or attempts to penetrate/access a computer resource without authorization to an authorized person, with an intention to threaten the unity, integrity, security or sovereignty of the nation.
- Sec 67 provides punishment for publishing child pornography or predating children online. A person can face imprisonment up to 7 years or fine up to 10 lakhs INR or both if he/she is found capturing, publishing or transmitting images of a child in a sexually explicit act or induces anyone under the age of 18 to involve into a sexual act. Section 67 penalises only transmission and publication of obscene material but the viewing, downloading, and possessing such content is not made punishable under this section unless the victims are children. While it is impossible to try each person in possession of the content, but rendering the ones who are complicit in the commission of the crime (though inactive) free from liability defeats the purpose of hindering the obscene content.[10]
- Sec 67 A makes the publication, transmission or causing of transmission of sexually explicit material punishable with imprisonment extending upto 5 years and fine upto ten lakh rupees for first conviction and upto 7 years and fine upto ten lakh rupees upon second conviction.
- Sec 67 B makes publication / transmission of sexually explicit content depicting children in electronic form punishable with imprisonment of either description for a term which may extend to five years and with a fine which may extend to ten lakh rupees in first conviction and

[10] *https://criminallawstudiesnluj.wordpress.com/2020/06/02/section-67-of-it-act-2000-scope-misuse-and-the-striking inadequacy/#:~:text=DEFINING%20SCOPE%20OF%20OBSCENITY,that%20is%20lascivious%20in%20nature.*

ISSN: 2582-7677

imprisonment of either description for a term which may extend to seven years and fine which may extend to ten lakh rupees in subsequent conviction.

- Sec 69 provides power to government to block websites if it find it necessary in order to protect the sovereignty and integrity of India. Any information generated, transmitted, received or stored in any computer resource can be intercepted, monitored or decrypted by the government in the interest of sovereignty and integrity of India.
- Section 69 A empowers the central government to block public access to any information in order to protect sovereignty and integrity of India.
- Section 43A provides protection of data at corporate level. Any body corporate if negligent in implementing reasonable security practices thereby causing wrongful loss or gain to any person shall be liable to pay damages to the affected person.
- Under Section 72A of the (Indian) Information Technology Act, 2000, disclosure of information, knowingly and intentionally, without the consent of the person concerned and in breach of the lawful contract has been also made punishable with imprisonment for a term extending to three years and fine extending to INR 5,00,000.[11]
- Under Section 70B of the IT (Amendment) Act 2008, the government constituted CERT-In, which the website of the Ministry of Electronics and Information Technology refers to as the 'Indian Computer Emergency Response Team'.[12] CERT-In is a national nodal agency responding to computer security incidents as and when they occur.[13]
- The Ministry of Electronics and Information Technology established Cyber Regulations Appellate Tribunal in October 2006 under section 48(1) of the IT Act 2020. The Tribunal is renamed as Cyber Appellate Tribunal (CAT) by the IT Amendment Act 2008. Pursuant to the IT Act, any person aggrieved by an order made by the Controller of Certifying Authorities, or by an adjudicating officer under this Act, may prefer an appeal before the CAT which is headed by a chairperson who is appointed by the central government by notification, as provided under Section 49 of the IT Act 2000.[14]

Sec 66 A of the IT Act was struck down due to its rampant misuse. Sec 67 is being misused for filing cases of cyber defamation. There are instances where this section is misused to curb

[11] *https://www.mondaq.com/india/it-and-internet/133160/data-protection-laws-in-india*
[12] *https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/india*
[13] *ibid*
[14] *ibid*

ISSN: 2582-7677

political dissent. In one instance of Chhattisgarh, a journalist was arrested for posting comments against Samajik Ekta Manch through WhatsApp for circulating obscene matter and in another instance, for posting an objectionable matter against Yogi Adityanath, Chief Minister of Uttar Pradesh, a woman from Bangalore was booked.[15] This section is also misused where no actual harm is caused due to the asserted obscenity. In a recent case in Pune, section 67 of the IT Act was inflicted upon four boys along with relevant sections of IPC and POCSO for filming and sharing a video where they can be seen performing sexual acts on each other. A report 'Guavas and Genitals' which drew its matter from this case analyzed NCRB data and found that between 2015-17, 99 cases of obscenity were registered out of which only 28 involved non-consensual production.[16]

Information Technology Rules

The government in order to broaden the scope of IT Act routinely provides for sets of Information Technology Rules under various sections of the IT Act that focusses and regulates the specific areas of collection, processing and transfer of data. Most recent IT Rules are as under:

- The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, requiring entities holding users' sensitive personal information to maintain certain specified security standards.[17]
- The Information Technology (Intermediaries Guidelines) Rules, prohibiting content of a specific nature on the internet.[18]
- The Information Technology (Guidelines for Cyber Cafe) Rules, requiring cybercafés registration with a registration agency and requiring them to maintain a log of users' identities and their internet usage.[19]
- The Information Technology (Electronic Service Delivery) Rules, allowing the government to make specification that certain services, such as applications, certificates and licenses should be delivered electronically.[20]

[15] *https://criminallawstudiesnluj.wordpress.com/2020/06/02/section-67-of-it-act-2000-scope-misuse-and-the-striking-inadequacy/#:~:text=DEFINING%20SCOPE%20OF%20OBSCENITY,that%20is%20lascivious%20in%20nature.*
[16] *ibid*
[17] *meity.gov.in/sites/upload_files/dit/files/GSR313E_10511(1).pdf*
[18] *meity.gov.in/sites/upload_files/dit/files/GSR314E_10511(1).pdf*
[19] *meity.gov.in/sites/upload_files/dit/files/GSR315E_10511(1).pdf*

ISSN: 2582-7677

These rules are the statutory law specified under sec 43A of the IT Act on 11 April, 2011.

Some of the provisions of Indian Penal Code 1860 can also be inflicted on the accused like abetment of suicide, fraud, criminal intimidation, cheating, breach of trust, defamation and many more considering the circumstances and discretionary power of the court but a person cannot be double jeopardized i.e. punished twice for the same offence as it violates the fundamental right of a person guaranteed under article 20(2) of the Indian Constitution.

Property rights can based on Copyright Act 1957 can also be enforced sometimes for data protection. Other legislations that are relevant in data protection are the Criminal Procedure Code 1973, the Competition Act 2002, the Indian Telegraph Act 1885, the Companies Act 1956, and the Consumer Protection Act 1986.

In order to protect information and monitor cyber-attacks, the National Cyber Security Policy 2013 was released by the Government of India in 2013 which aims to secure cyberspace for citizens, government and the business houses. The main objective of this policy is to strengthen the regulatory framework. Though this policy is treated as an important step for providing security to our cyber space but certain areas remain outside the ambit to it. The provisions to safeguard against the risks undertaken by the use of new technologies such as Cloud Computing are not considered. The risk factor involved due to use of social networking sites by criminals and anti-national elements is also not addressed. Need is also felt to incorporate cybercrime tracking, cyber forensic capacity building and creation of a platform for sharing and analysis of information between public and private sectors on continuous basis.[21]

There have been several cyber-attacks in India, especially during the COVID-19 lockdown and the cyber-attacks have soared to about 86% during March and April which led to the work on overhauling the 2013 cyber security policy.[22]

India does not have a dedicated Data Protection Law. In 2017, the Indian Supreme Court ruled that Indian citizens have a fundamental right to privacy, guaranteed primarily under Article 21 of

[20] *meity.gov.in/sites/upload_files/dit/files/GSR316E_10511(1).pdf*

[21] *https://idsa.in/idsacomments/NationalCyberSecurityPolicy2013_stomar_260813#:~:text=With%20an%20aim%20to%20monitor,by%20the%20Government%20of%20India.&text=The%20objective%20of%20this%20policy,and%20strengthen%20the%20regulatory%20framework.*

[22] *https://nickledanddimed.com/2020/10/06/cybersecurity-in-the-indian-legal-scenario/*

ISSN: 2582-7677

the Indian Constitution and the Court specified that this right includes, inter alia, the right to informational privacy.[23]

In the wake of this judgment, and in order to give it meaning in the form of comprehensive legislation, the government empanelled a 10-member committee under the chairmanship of Justice BN Srikrishna, a former Supreme Court Justice.[24] The committee published its report in 2018 which is accompanied by the draft Personal Data Protection Bill 2018. In December 2019, the Personal Data Protection Bill 2019 was tabled in parliament.[25] The report states that:

"to make [the right to privacy articulated by the Supreme Court] meaningful, it is the duty of the state to put in place a data protection framework which, while protecting citizens from dangers to informational privacy originating from state and non-state actors, serves the common good."[26]

Personal Data is not defined in the current legislation. The IT Rules define personal information as any information that relates to a natural person that, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, is capable of identifying such a person.[27] The Personal Data Protection Bill 2019 defines 'personal data' as 'data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling'.[28]

The Personal Data Protection Bill 2019 provides for the formation of data protection authority and its places great duty on data processors and controllers. In case it is enacted, it will apply to wide range of stakeholders and actors from different sectors.

The bill was placed under active consideration of a Joint Parliamentary Committee in the year 2020.[29]

During the pandemic, there is a steep rise in cases of cybercrimes. Financial transaction information of citizens have been attacked during the phase of pandemic. Lt. Gen. Rajesh Pant, India's National Cyber Security Coordinator (NCSC), told the Economic Times that

[23] *https://thelawreviews.co.uk/title/the-privacy-data-protection-and-cybersecurity-law-review/india*
[24] *ibid*
[25] *ibid*
[26] *ibid*
[27] *ibid*
[28] *ibid*
[29] *https://www.tribuneindia.com/news/punjab/india-needs-a-dedicated-cyber-security-law-216669*

ISSN: 2582-7677

cybercriminals had launched thousands of "fraud portals" related to the coronavirus.[30] The citizens were lured by these sites to make donations. The PM cares fund initiative by the office of the Prime Minister for fighting Coronavirus had multiple fraudulent websites. A study reveals that there have been several malware and phishing schemes operating under the pretext of COVID prevention efforts and the so-called "coronavirus malware" is aimed at stealing bank account details, password and other sensitive information from users.[31]

Prime Minister Narendra Modi, in his speech on Independence Day 2020, announced that the Government is cognizant of the cyber-attacks on India and its potential threats therefore, he announced that there needs to be an immediate implementation of new cyber security policy.[32]

There is a need for National Cyber Security Strategy 2020 for providing security to business data which if not secured would impact the security of the nation and would impact economy of the country. The National Cyber Security Strategy 2020 is necessitated as the existing structure requires to be revamped and revitalized. New challenges included in National Cyber Security Strategy 2020 will be data protection/privacy, law enforcement in evolving cyberspace, access to data stored overseas, misuse of social media platforms, international cooperation on cybercrime and cyber terrorism, and so on.[33]

CONCLUSION

Due to advancement in technology a large number of people have access to the cell phones and the internet thereby resulting in cybercrimes especially against women and children. So it would be ludicrous to think that the existing act would tackle each and every type of cybercrime. According to a data released by National Commission for Women around 28 complaints were received in March and 54 complaints were received in the month of April. 462 complaints were received in the months of March and April by Akancha Foundation.[34]

The conviction rate for cybercrimes in India has been less than 10 convictions in the last 12 years since the IT Act came into force and there have been zero convictions after IT (Amendment) Act, 2008 was implemented.[35] The current cybercrime legislation makes only cyber terrorism as

[30] *https://nickledanddimed.com/2020/10/06/cybersecurity-in-the-indian-legal-scenario/*
[31] *ibid*
[32] *ibid*
[33] *ibid*
[34] *Supra 15*
[35] *https://www.digit.in/technology-guides/fasttrack-to-cyber-crime/indian-cyber-crime-laws.html*

ISSN: 2582-7677

non bailable rest all cybercrimes are bailable providing a good opportunity to the offenders to destroy all electronic evidence after getting bail. This non serious approach towards cybercrimes has led people in losing hope in the legislations.

There is a remarkable increase in cybercrimes, where cyber criminals used cyber space for giving effect to crime during the nationwide Covid-19 lockdown. Even if this unique situation of Covid-19 is disregarded, then also such crimes are on a surge which requires serious considerations and amendments in the existing legislation for providing protection to people against this serious misuse of technology. These amendments are deemed necessary for keeping the data of people safe and secure on the online platforms. Proper mechanism is required for identifying the cyber criminals and taking legal action against them. As suggested by reports, women complaining about cyber harassment have to undergo 'secondary victimization' by media, police and judiciary. Keeping in mind the sensitivity attached to such matters need is felt for more specific and effective legislation. Protection Data Protection Bill 2019, if passed in Parliament would provide stringent obligations for each and every data handling entity. Information technology ecosystem of India will be strengthened and personal data will get more protection from cyber frauds after this bill gets implemented. The government should come up with new strategies for dealing with the protection of non-personal data as non-personal data is not within the ambit of Personal Data Protection Bill 2019.

The Information Technology laws are required to be updated frequently so as to deal with the ever growing cybercrimes. A hacker in US can hack into servers of Mumbai Stock Exchange. Which cyber laws are going to apply in such cases as different nations have different laws for cybercrimes and there is a possibility that an act may be considered as cybercrime in one country whereas it may not be an offence in the other country? The provisions of Information Technology Act 2000 would apply to an act committed outside India provided computer system or computer network located in India is involved in the crime.

The legislative bodies of the country should always keep in mind the pace with which cybercrimes are flourishing in the country so that appropriate laws can be made to combat them. As in today's world one cannot live without internet, the law making bodies and government should ensure that each and every aspect of cybercrime is included in the scope of cyber laws so as to protect the users against any probable misuse. International cooperation of countries of the world deems necessary as the nature of cybercrime is same everywhere.