ARE INDIAN CYBER LAWS ENOUGH TO TACKLE CYBERCRIME

By Yash Singh  
From Chanakya National Law University

INTRODUCTION

India, the second country after China, to have the most active users of the Internet numbering around 624 Million with an Internet penetration of 45%,¹ has reached its zenith on Internet usage, and thanks to the Covid-19 Pandemic, the tendency of Digital usage has increased to a great extent and has become an imperative factor for the Indians to have Internet and the related gadgets as a daily source of life but along with the Digital Revolution, crimes under the Cyberworld has exponentially increased which deprives the people of the basic usage of the Internet and their private space and this amounts to establishment and proliferation of the term “Cybercrime”.

Cybercrime, as the name suggests, is the extension of criminal activities through the usage of computers and other different networking entities which facilitate crimes related to the virtual aspect of the world like Cyberterrorism, Cyberextortion, Cybersex Trafficking, and many more. The offenses are committed under the purview of the virtual world which can be particularly committed against an individual or a group of individuals and the actions are backed by the criminal intention/motive to commit harm either inflicting a mental injury or physical injury when the act is very severe.

TYPES OF CYBERCRIMES

Since the inception of the Internet, cybercrimes have been committed through different modus operandi, and thus, a plethora of cybercrimes in different forms have been evolved and are inflicted upon the systems of different individuals through different levels of severity. Some of the types of Cybercrimes are:

- **WEB ATTACKS**— “These are the malicious sources that are employed on the Internet and can be downloaded by any user thereby causing irrevocable damages to the user’s system.”
- **SQL INJECTIONS**— “In this type of cybercrime, malicious codes are employed on the user’s system which in turn, attacks the backend databases and manipulates various types of sensitive information.”
- **CROSS SITE SCRIPTING**— “In this type of cybercrime the attacker himself sends the malicious scripts to the user unlike in SQL Injection where it is employed by the attacker on the Internet. The user unknowingly tends to open that script and thus the user’s system gets corrupted by that script.”
- **DDOS ATTACKS**— “This type of cybercrime is inflicted upon high-profile entities like Government, Big Business Firms, etc. In this, the network source of the intended user is polluted by malicious objects since the network is trafficked by a huge complex of malicious network entities, and the effective speed of the Internet gets hampered, thus lowering

down the efficiency of the Internet-specific activities.”

- **PASSWORD ATTACKS**- “These attacks are committed by sniffing the passwords of different users and are accessed with a criminal intention.”

- **EAVESDROPPING ATTACKS**- “This type of cybercrime is committed to access critical information of the user by intercepting the network traffic. This type of attack is called Sniffing or Snooping.”

- **DICTIONARY NETWORK ATTACKS**- “This type of attack is committed by using different possible passwords to access the user’s profile or information.”

- **INSIDER THREATS**- “This type of attack can also be committed by an individual who has authorized access to a user’s information or the data intruder is an insider.”

- **MAN-IN-THE-MIDDLE ATTACKS**- “It occurs when the attacker eavesdrops on the communication between two entities. The attacker can hamper both the communicating parties as it can manipulate any of the intercepted information.”

- **PHISHING ATTACKS**- “It is a type of Social Engineering Attack in which, the attackers camouflage to be bonafide service providers on different Internet sources and trick victims into opening malicious links.”

- **MALWARE**- “It is an umbrella term which consists of intrusive software which imprints different types of illicit objects in the networking program of a user and damages the system severely.”

- **RANSOMWARE**- “It blocks the data’s address of a network user and the user even with authorized permission cannot access his own data/credentials unless some ransoms are not fulfilled.”

- **TROJAN HORSE**- “It is a malicious software program which attempts to disguise itself and pretends to be a safe credential on the Internet services but inflicts various viral threats on the user and thus the system gets damaged.”

- **TEARDROP ATTACK**- “Teardrop attack is a form of attack that causes fragmentation in the general sequence of Internet Protocol (IP) packets and sends these fragmented packets to the victim’s machine that is attacked.”

Thus, such types of methodologies can be and are used to commit crimes in the virtual world, i.e. cybercrimes and many more other types of attacks can be committed to damage the server, data, information, or in toto, the system of a user.

During the pre-Covid times, bullying irrespective of caste, sex, religion, etc used to take place in every corner of the world and the same could be witnessed in the virtual world but after the onset of the Covid-19 Pandemic, the advent of Digital inclusion and usage has rampantly increased which has exploited various members of the society and the specific term used for it is “Cyberbullying”.

Cyberbullying, as the name suggests, is the bullying of an individual in virtual platforms like Whatsapp, Facebook, other Internet sources, etc. It can be done

---

through texts, online messaging, accessing illicit internet sources, etc. Under the purview of Cyberbullying, one or the other individual gets vulnerable to the atrocities of the harasser which in turn, could lead to serious implications like imputation of harm on the reputation of the victim by way of societal exclusion, mental and psychological stress, development of lackadaisical attitude because of the lack of motivation behind performing any activity and many more. Due to restrictions during the advent of Covid-19, children and students had to acclimatize themselves to digital education due to which, the chances of vulnerability increased owing to extensive internet penetration.

GOVERNING INSTITUTIONS ON CYBERCRIME

To curb the menace of cybercrimes, the Indian Government time and again has come up with some of the governmental entities or institutions to govern the cause of cybercrimes and the allied activities, committed with a criminal intention to attack the victim. The first and the foremost of all the institutions is the Indian Cyber Crime Coordination Centre, better known as I4C, which is a scheme propounded by the Ministry of Home Affairs in 2018. It is a “nodal agency to curb cybercrime and the allied activities like cyberterrorism, cyber trafficking, and others, to amend some cyber laws to make them in consonance with the contemporary scenario, to organize Research and Development activities and to foster cooperation with the international laws. It comprises different components for smoother administrative purposes like Research Centres, Forensic Centres, Analytics and Investigation Team, Management Unit, and Grievances Reporting Portal.”

Under the purview of this scheme, the “National Cyber Crime Reporting Portal” has also been institutionalized to facilitate the reporting of cases about cybercrime and also provide services for addressing the grievances of an individual.

Article 15(3) of the Indian Constitution mandates the State to make special provisions or laws for women and children and considering this view, the Ministry of Home Affairs (MHA) came up with “Cybercrime Prevention Against Women and Children (CCPWC) Scheme to safeguard the digital privacy of women and children by performing various aspects like Reporting of Complaints, organizing Awareness Campaigns, facilitation of Research and Development Activities, etc.”

A wing of the Ministry of Home Affairs about Cybersecurity apart from the above-mentioned initiatives is the “National Cyber

---

4 ibid
6 Constitution of India, art 15(3)
Coordination Centre (NCCC), which is an e-governance agency in India, and is intended to screen communication and coordinate intelligence-gathering activities of other agencies.”

An agency supervised to go through intelligence gathering activities is the “National Technical Research Organization (NTRO) under the National Security Advisor (NSA) in the Prime Minister’s Office (PMO). It works on multiple disciplines including remote sensing, data gathering and processing, cyber security, geospatial information gathering, cryptology, strategic hardware and software development, and strategic monitoring.” Under the same entity, an organization has been commissioned by the Government of India under Section 70A of the Information Technology Act, 2000, that is the “National Critical Information Infrastructure Protection Centre (NCIIPC) whose mission is to take all necessary measures to facilitate the protection of Critical Information Infrastructure, from unauthorized access, modification, use, disclosure, disruption, incapacitation or distraction through coherent coordination, synergy and raising information security awareness among all stakeholders.”

One of the most promising and holistic governmental organizations established to curb the scourge of cybercrime is the “Cyber Emergency Response Team (Cert-in) under the Ministry of Information and Technology (MEITY) which performs inter-disciplinary works like collection, localization, and dissemination of user data and the cybercrime incidents, organizing awareness campaigns, preparing reports ad publishing whitepapers, issuing guidelines regarding protection and prevention of cyber-related crimes, forecasting of cybercrime-related accidents and many more. It is one of the most active bodies in India regarding cyber security which holds a plethora of working officials as well as the data for various activities.”

**INDIAN LAWS ON CYBERCRIME**

The Indian Parliament keeping in view the illicit activities committed under the ambit of Cybercrime came up with a holistic law called the “Information Technology Act, 2000” which dealt with the contemporary cyber-related issues and some other aspects related to the cyber world. Some of the provisions of this Act that dealt with Cybercrime are-

- **SECTION 65 (TAMPERING WITH COMPUTER SOURCE DOCUMENTS)**- “Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.”

---

8 Information Technology Act 2000, s 70A
11 Information Technology Act 2000
12 ibid s 65
Certain amendments were done in the IT Act 2000 to deal with the changing scenario of the Digital World and its provisions related to Cybercrime are-

- **SECTION 66D (PUNISHMENT FOR CHEATING BY PERSONATION BY USING COMPUTER SOURCE)**-
  “Whoever using any communication device or computer resource cheats by personation, shall be punished for imprisonment for a term which may extend to 3 years and shall also be liable to fine which may extend to one lakh rupees.”

- **SECTION 66E (PUNISHMENT FOR VIOLATION OF PRIVACY)**-
  “Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both.”

- **SECTION 66F (ACTS OF CYBERTERRORISM)**-
  “(1) Whoever— with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by—
  - denying or cause the denial of access to any person authorized to access computer resources; or
  - attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or
  - introducing or causing to introduce any computer contaminant, and using such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under Section 70; or
  - knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and using such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or about contempt of court, defamation or incitement to an offense, or the advantage of any foreign nation, group of individuals or otherwise, commits the offense of cyber terrorism.”

- **SECTION 67 (PUBLISHING OF INFORMATION WHICH IS OBSCENE IN ELECTRONIC**
FORM)- “Whoever publishes or transmits or causes to be published in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to two lakh rupees.”

- **SECTION 67B (PUBLISHING CHILD PORN OR PREDATING ONLINE)**- “Whoever publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in a sexually explicit act or conduct; or creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges, or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or cultivates, entices, or induces children to online relationships with one or more children for and on a sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or facilitates abusing children online, or records in any electronic form own abuse or that of others pertaining to sexually explicit act with children shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.”

- **SECTION 69A (POWER TO ISSUE DIRECTIONS FOR BLOCKING FOR PUBLIC ACCESS OF ANY INFORMATION THROUGH ANY COMPUTER RESOURCE)**- “Where the Central Government or any of its officer specially authorized by it in this behalf is satisfied that it is necessary or expedient so to do, in the interest of sovereignty and integrity of India, defense of India, security of the State, friendly relations with foreign states or public order or for preventing incitement to the commission of any cognizable offense relating to above, it may subject to the provisions of sub-section (2) for reasons to be recorded in writing, by order, direct any agency of the Government or intermediary to block for access by the public or cause to be blocked for access by the public any information generated, transmitted, received, stored or hosted in any computer resource.”

- **SECTION 43A (COMPENSATION FOR FAILURE TO PROTECT DATA)**- “Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns,
controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.”

Apart from the IT Act, 2000 and its Amendment, POCSO Act, 2012 (Act for the protection of children from Sexual offenses) also specifically entails a provision for the protection of children from their malicious usage by the perpetrator for pornographic purposes in the Digital Environment, that is Section 13 of the Act which mentions “Whoever, uses a child in any form of media (including program or advertisement telecast by television channels or internet or any other electronic form or printed form, whether or not such program or advertisement is intended for personal use or distribution), for sexual gratification, which includes-(a) representation of the sexual organs of a child; (b) usage of a child engaged in real or simulated sexual acts (with or without penetration); (c) the indecent or obscene representation of a child shall be guilty of the offense of using a child for pornographic purposes.”

Leaving aside the statutory laws about Cybercrimes, even the incumbent government has time and again brought before the citizenry, certain rules and regulations, notifications to create a sense of awareness and disciplinary approach around different aspects of the field concerned. The government came up with the “National Cyber Security Policy, 2013 to cope up with some of the ramifications of the cyber world while taking into consideration the contemporary scenario. It consists of the Vision, the Objectives, and the Mission behind the upliftment of Cyber Security and it also comprises holistic and comprehensive strategies for upholding the cause of Cyber Security like- a) Creating a secure cyber ecosystem, b) Encouraging open standards, c) Strengthening the regulatory framework, d) Securing e-governance services, e) Protection and Resilience of Critical Information Infrastructure, f) Promotion of Research and Development in cyber security and many more.”

The Ministry of Electronics and Information Technology (MEITY) in collaboration with the Ministry of Information and Broadcasting (MIB) has notified the “IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 which mandates the social media intermediary as well as the significant social media intermediary to inform the user of its computer resource not to host, display, upload, modify, publish, transmit, store, update or share any information that contains a software virus or any other computer code, file or program designed to interrupt, destroy or limit the functionality of any computer resource in the form of rules and regulations, privacy policy or user agreement.”

19 ibid s 43A
20 Prevention of Children from Sexual Offences Act 2012, s 13
One of the most promising laws that are coming to be laid on the table of the Parliament after constant scrutiny by the Parliamentary Standing Committee is the “Personal Data Protection Bill, 2019 envisaged and drafted after the recommendations of B.N. Srikrishna Committee. It broadly deals with the data localization of the citizenry and certain statutory rules to be followed by the data controller about the data of the citizenry, be it ordinary, personal or critical and it also deals with a contemporary yet elusive term in the Indian subcontinent, that is ‘Right to be Forgotten’, and this law can prove to be very effective in dealing with cybercrimes as the data procured by different service providers can have some regulations to be abided by them and to punish the culpable to set a precedent for the future committers of cyber-related crimes, even though the same act is facing constant criticisms for some of its provisions like the exculpation of government agencies when found to be guilty of safeguarding the integrity and sovereignty of India, and regarding the excusal of the word ‘Personal’ from the Act.”

INTERNATIONAL CONVENTION ON CYBERCRIME

On the global level, many countries came up with a common convention to safeguard the country from the causes and might of cybercrime and to prevent the repercussions developed by it. The famous and the only convention on the global forefront is the “BUDAPEST CONVENTION which coordinates cybercrime investigations between nation-states and criminalizes certain cybercrime conduct and serves as a guideline for any country developing comprehensive national legislation against Cybercrime and as a framework for international cooperation between state parties to this treaty.” It came into existence in 2001 and was enforced in 2000 by the common acceptance of many subcontinents but, India did not become a part of this common group and in turn, has never been a signatory of this convention owing to the reason that “the data procurement by the foreign agencies under this convention can trample the national sovereignty and security of India.”

INDIAN JUDGMENTS ON CYBERCRIME

It was during the phase of 90s in the 20th century when India witnessed the advent of Internet services provided by different service providers but many people became the subject of this fast-transforming environment and inclined towards committing crimes. The first case that was filed on the issue of cybercrime was the “Akash Arora case which, the defendant, had started his Internet service provider, YahooIndia.com unlawfully which was in all probability, similar to the valid and the famous ‘Yahoo Inc’. The giant company filed a suit against the defendant on the fact that he was unlawfully used the company’s

0Ethics%20Code%20Rules%2020201%20English.pdf> accessed 19 Dec 2021
name and deceptively was providing the service and so was violating the trademark laws. The court held the defendant liable and imposed a permanent injunction on the deceptive domain.”

Subsequently, a case about IT Act, 2000 came up in 1999 that is the Madhvika Joshi case. In this case, “the plaintiff, Neeraj Kaushik was the husband of the defendant, Madhvika Joshi and both of them were witnessing a troubling matrimonial relationship. To bring substantial evidence under Section 498A of IPC, the defendant has approved unauthorized access to the plaintiff’s email id just to gather solid evidence but the plaintiff filed a suit against her under Section 43 of IT Act, 2000. The court held in favor of the defendant as there was no criminal intention behind committing this act and hence, no liability arises.”

This case unveils the fact that a malafide intention should be formed to be held liable under the provisions of the IT Act as unauthorized access of the data is concerned.

The most landmark case that revolves around the IT Act and the Freedom of Speech and Expression under Article 19(1)(a) of the Indian Constitution is the Shreya Singhal case. In this case, the constitutionality of Section 66A of the IT Act was put into question which said “Any person who sends, by means of a computer resource or a communication device (a) any information that is grossly offensive or has menacing character; or (b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; (c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.”

The court held that “since the word “offensive” is vague in its ambit and is very subjective when it comes to its interpretation, Section 66A is void and is unconstitutional in its entirety. Though Reasonable Restrictions under Article 19(2) of the Indian Constitution have been bestowed up on the State to prevent the citizenry from committing acts that go against the ethos of the “Rule of Law”, the State itself cannot count this provision as one of the Reasonable Restrictions and the court upheld the Freedom of Speech and Expression of the petitioners.”

ARE INDIAN CYBER LAWS ENOUGH TO TACKLE CYBERCRIME?

Since the inception of the IT Act, 2000, the rate of cybercrime incidents have been increased as compared to the pre-IT Law era, which is quite obvious but what is
paradoxical and startling to our understanding is that even the IT Law was quite comprehensive and holistic during the time of its formulation but due to the Digital Revolution and the advent of new horizons like Artificial Intelligence, Internet of Things, etc, the people abscond from their malicious acts and various crimes are committed on the face of the absence of the laws regulating the cyber world. After the onset of Covid-19 Pandemic, the digital, rather internet penetration has rampantly increased and the first cyberattack during the rage of Covid-19 Pandemic is “China’s Red Echo’s prepared malware, ‘Shadow Pad’, which devastated some of the inter-connection of some of the ports of Mumbai and a mass-outage took place in Mumbai in October 2020 due to the power grid failure in Power Plants installed nearby the town. The USA claims the attack to be sponsored by China and was also reported by solid facts, depicting the lacuna in the security net of these entities.”

Subsequently, “the indigenous vaccine maker of India, Dr. Reddy’s Laboratories was also attacked by malicious software at a time when it got approval from DCGI to produce Sputnik V vaccine in India, though the implications of it were mitigated by the officials.” Further, in November 2020, one of the biggest data breaches and data leaks India had ever witnessed was the “Big Basket data breach in which, one of the groups ‘ShinyHunters’ which hosted the personal details of the 20 million users of the company on a dark web, thus making the same section of people vulnerable to the acts of the perpetrator.”

A similar incident happened with one of the Indian payments apps ‘Mobikwik’ in January 2021 where the database amounting to a size of 8.2TB was leaked on a dark web which consisted of critical information like KYC Details, Aadhaar Card Details, Phone Number, etc. Even the fleet carrier companies got exposed to be vulnerable to the data leaks that happened online and this incident happens to be caused to the national air carrier ‘Air India’. “The sensitive information of the aircraft giant got exposed perpetually for a period of 10 years, that is from February 2011 to February 2021, and around 4.5 million passengers got their information intruded by a malicious software fabricator.”

Not only India, the superpower of the world, “the USA in 2021 itself, was preyed on by the masterminds when its national fuel operator ‘Colonial Pipeline’ was exposed to the vulnerability of the attack of the hackers and

the fuel operator had to be shut down to suffer minimal damage and data breach does not occur. The repercussions of the shutting down of the entity led to the surge in global oil prices, stock prices of the operator trashed, and therefore, the ultimate sufferer was the common citizenry.”

Not only this, one of the biggest cyberattacks the mighty subcontinent had ever seen, was the infamous ‘Solarwind cyberattack’. “In this attack, a US-based IT company, Orion was attacked through a supply chain strategy by directly attacking its data localizer, Solarwind (a Texas-based company) due to which, the data of some of the high officials and outfits from public authorities like the Pentagon, Centers for Disease Control and Prevention, the State Department, the Justice Department, and others, was compromised leading to the indirect attack against the federal government of the USA.”

A very fresh ventilated incident occurred with the most top government official, that is the “Prime Minister of India, Narendra Modi where his Twitter account was hacked in the early hours of December 12, 2021. The tweet read- ‘India adopted bitcoin as legal tender and the government of India has bought 500 bitcoins to distribute among residents of the country’. The account was compromised for a short period and the account was later restored.”

So adhering to these facts and considering them, when the top official of the State is himself exposed to such vulnerabilities, how will the security of the common citizenry be ensured to the utmost priority? Apart from this, data breaches and the data leaks that take place globally is also not promising factor when the Indian subcontinent lacks the data and the cyber laws specifically owing to the contemporary issue of the digital environment. Also when these payment gateways and platforms as the Internet service providers get intruded by the malicious software fabricated by the hackers, the company or the organization raises multiple questions regarding their accountability for safeguarding the database of the citizenry that also the vacuum created by the lack of efficient rules and regulations and the most primary, the statutory laws comprising rules, penalties, definitions, and many other aspects in a comprehensive way.

Now coming on to some of the reports published by different agencies and firms, the first among them is the Kaspersky Cyberthreat report of 2020 which said, “45% of the online users in India were targeted by local cyber threats like rootkits and removable tools like malicious USB drives and other offline methods. Brute force attacks on Remote Desktop Protocols (RDPs) also saw a massive increase of 242% globally. The number of detections in India alone went as high as 36 million

---

The nodal indigenous organization for cyber security in India, CERT-In, in 2021, too released a statement related to cyber threats which read, "The Indian Computer Emergency Response Team (CERT-In) has observed more than 6.07 lakh cybersecurity incidents in the first six months of 2021, of which about 12,000 were related to government organizations. A total of 6,07,220 cybersecurity incidents were observed during 2021 up to June of the same year."

The National Crime Records Bureau (NCRB) also releases an annual report on various crimes that are committed throughout the territory of India, which is “Crime in India Report, 2020” which mentioned that the incidents of cybercrimes in 2020 alone, stood at 50,035 which saw a huge surge when compared to the incidents in 2018 amounting to 27248, which in percentage terms is a significant increase of 83.6%. Going with the same report, the amount of charge-sheet filing stood at 47.5%, which depicts that a whopping amount of 52.5% cases went unaccounted.

Thus, going by these reports and press releases and also broadly with the cyber threat incidents mentioned above, one can gauge that the cyber environment in India is filled with many loopholes and witnesses various problems- Firstly, There is no adequate and comprehensive statutory law related to cybercrimes barring the IT Act of 2000 which has become archaic owing to the contemporary digital phase; Secondly, the lackadaisical attitude of the Parliamentarians in bringing the required rules and regulations for mandating different entities to safeguard the privacy and the database of the citizenry; Thirdly, there is inadequate coordination between different cyber security enforcement agencies which creates a vacuum in terms of vigilance and when a catastrophic condition occurs, the said agencies start playing ‘passing the parcel’ in blaming others; Fourthly and the foremost lacuna is that the data localizers tend to commit negligent acts owing to the lack of sufficient and modern equipments and resources or largely lack of security infrastructure ailes such agencies due to which, the problem of data breaching occurs; Lastly, inadequate awareness among the citizenry regarding different cybercrimes also facilitates the act of breaching of their data by the perpetrators of such acts.

India, which has a mammoth population and a vast level of deep Internet penetration among the users, needs to have the above-mentioned loopholes corrected by reformatory measures and fill the vacuum which exists only because of the lack of effective and holistic laws that need to be brought into effect for the betterment of the


cyber rights of the citizenry. So, certain corrective measures can be taken by the incumbent government to make the already existing complexities in the cyber and digital society by reforming them. Firstly, adequate, effective, comprehensive, and holistic laws need to be brought by the legislators to bring them into implementation as soon as possible; Secondly, proper research and development and proper studies need to be done on various aspects of cyber security and cyber threats to gauge the areas where more improvement is needed by the lawmakers and the law enforcement agencies; Thirdly, proper training needs to be given to various officials and the outfits of the law and cyber enforcement agencies for proper vigilance and effective output given by them during the performance of vigilance and reporting activities; Fourthly, certain awareness campaigns and various training centers need to be brought for the citizenry like the Cyber Surakshit Bharat Initiative, Cyber Swatchh Kendra and many more. Lastly, Toolkits related to cyber security and cyber threats and some programs like the mock drills need to be done in a targeted manner and certain areas of the country.

Though according to the International Telecommunication Union’s “Global Cybersecurity Index of 2020”, India has moved up 37 places, secured the 10th position and the 4th position in the Asia-Pacific region^43, it is not in toto, a promising figure, and even then, the nation needs to work upon many complex problems and emerge as a global super leader in terms of cyber security and work towards mitigating such cyber threat incidents and also come up with various promising mitigation strategies to safeguard the rights and freedoms of the citizenry in ‘Digital India’.