INDIAN JOURNAL OF LAW, POLITY AND ADMINISTRATION

CYBERCRIME IN INDIA: A DETAILED ANALYSIS

***Rimjhim Sharma**

ABSTRACT

This paper examines cybercrime that are routinely undertaken in today's highly networked environment and the need to address such crimes. The central idea and purpose of this paper is that economic and institutional factors facing cyber-criminals and potential victims in the developing world are different from those in the developed world. This paper begins with a discussion on the paradoxical impact of digitalization as a cause that enables cybercrime in the form of malware, escalating organized cybercrime, personal information, data breach, online harassment, and so on but the author emphasizes much on cyber stalking, online harassment identity theft, cyber thread, online defamation which are the major concern in recent times and need of the hour to take preventive measure by the Government of India. According to security software firm Symantec, India ranked third, in the list of countries where the highest number of cyber threats were detected in 2017. After a brief introduction to the issue of digitalization and its insurmountable impact on cybercrime, this research paper attempts to analyse the impact of cybercrime in the society and level of awareness amongst people and what are the cyber security strategies of the Government that has to be taken and whether the information security or data protection is well maintained in the era where privacy is no more unconstitutional in India but a fundamental right adding up what are the precautionary measures taken by the society and the challenges needed for taking up for the transformation in India are also discussed and the suggestions like to build public's trust in a digital world, India will have to bear zero tolerance towards cybercrime. By this research paper the author wants to enlighten the academicians as well as the non tech savvy laymen to have first-hand information and to apply given suggestions to tackle the various cybercrimes.

INTRODUCTION

A crime is an offense that may be prosecuted by the state and sanctioned by law. A cybercrime is a type of crime which uses computers and networks as a target or weapon. Where more than half a billion internet subscribers exist which is increasing rapidly, India is one of the largest and fastest-growing markets for digital consumers. Initiatives like Digital

India and smart cities mission, which are part of technology, have shifted the crime pattern from physical to the digital world. These modern techniques are proliferating towards the oftentimes use of internet activity resulting in creating exploitation, vulnerability making a suitable way to commit a cyber-offence through illegal activity. This digitalization or digital economy which leads to cyber offences in India are broadly discussed in this paper. Cybercrime falls into three categories: Cybercrime against the persons, Cyber Crimes against Business and Non-business organizations and Crimes against the government. If we specifically talk about India then amongst these the biggest scourge is online harassment and Sexual solicitation for youth in recent times who use forms of cyber communication. It may occur on social networking sites or in chat rooms. A teen may be asked to disclose personal information, discuss something sexual or abusive or view pornography online. The author highlights some this kind of plagues in this paper especially in the situation of global pandemic which needs a reality check.

Lack of awareness about cybercrime legislations, Government cyber security strategies and poor digital payment ecosystem are some of the primary reasons that have led to the increment in the number of such cybercrime in the society. Social media such as Facebook, WhatsApp, Messenger, Twitter etc. are used by users as a platform to express themselves without any restrictions which is becoming a major challenge as it may infringe the fundamental right as right to privacy of a human being.

Cybercrime has now become the biggest challenge for all countries in the world. In India it is increasing at an alarming rate and a big concern for the law enforcement agencies (LEAs) to minimize cybercrime occurring in the country and it is a challenge for the web of Cybercrime too that it is becoming by far that perpetrators often located beyond the boundaries of the nation's jurisdiction which is difficult to catch them up.

There is no specific legislation for cybercrime in India but The Information Technology Act (ITA), 2000 Indian Penal Code (IPC), 1868 penalizes a number of cybercrimes. Some rights for the protection of cybercrime are given under the Constitution as well like Art-19 & 21. Increased cybercrime in India has led to the amendment in the Information Technology Amendment Act, 2008, hereunder (The IT Act, 2000).

RESEARCH PROBLEM

My analysis has shed light on the connections between digitalization, social and economic impact of cybercrime. This research problem pertains to critically examining the existing cyber security, lack of awareness in the society and legislative provisions and the challenges that will lead to the transformation in India.

RESEARCH HYPOTHESIS

It is hypothesized that cybercrime exists in many forms in the society. Users are not highly aware about hacking while using the internet. Increased rate in the cases of cybercrime even in the today scenario of globally pandemic, limited existing legislation and scope of jurisdiction clearly depicts the inclusion of comprehensive cyber security law and the essence of awareness in the society.

DIGITALIZATION CAUSING OF INCREMENT IN CYBER CRIME

It is agreed, that with the increasing digitization there is an increment in cybercrime because on the one hand where digitalization has great impact on our daily life by doing online shopping, e-trading, E-banking, E-payment, visually chat and conduct business etc. which goes very smoothly, time consuming, far reaching while on the other hand this digitalization is making India more vulnerable cyber security as people are losing their privacy and disclosing confidential information to internet database and this gives birth to a cybercrime moreover there is a campaign launched by Government of India as Digital India. This is the big step in making India a Digitalization Country which ensures that Government services are made available to citizens electronically and to move the country ahead in technology. "Cyber Crime" can be defined as the crime (as theft, fraud, intellectual property violations, or distribution of child pornography) committed electronically[394]. All developed countries are technologically advanced countries but if we talk about developing countries like India the question arises as to how *much people are secure in terms of hacking and other means of data leakage with the pacing technology*. This digital-advancement is making our life quite easy but we are being exposed to the dark underside of the virtual world. Along with this digital-advancement, Cybercrime is the major concern which reflects the dark side of the advancement. *Recent data from the National Crime Records Bureau (NCRB) shows that*

*IIMT School of Law, GGIPU, New Delhi

[394] Merriam Webster, available at<https://www.merriam-webster.com/dictionary/cybercrime> (last visited on 02.06.2020).

India recorded 21,796 cybercrimes in 2017 which has increased 77% from 2016 moreover countrywide, 1.7 cyber-crimes were committed per one lakh population in 2017[395].

Cyber Crimes may include cyber stalking, morphing of pictures and harming rather destroying the dignity of women, hacking, identity theft, Credit/debit card frauds, cyber terrorism cruel and disgusting comments on pictures that have been uploaded, and many more crimes.

Suhas Katti v. Tamil Nadu, decided on 5 November 2004. It was the first case in India where a conviction was held in connection with the posting of obscene messages, defamatory and annoying messages about a divorced woman in the yahoo message group on the internet and he was liable under the controversial section-67 of the Information Technology Act, 2000, 469 and 509 of IPC.[396]

- ***Is the nation ready for Digital Technology: critical analysis***

The law has largely failed to keep pace with this rapid change in the offence committed in different way due to modern change in technology although technology may offer solutions to tackle the very problems it has created but it is also not wrong that One of the difficulties in combating cybercrime is that it is worldwide; victims can be located or found in one country, while the perpetrators are in another.

On the other hand, we should also admit that anything can't be 100% secure and India has accepted digital India but for making digital India successful, the government should build trust in the minds of people by reducing such cybercrime and providing cyber security. As netizens are growing rapidly in developing India then the government should pave the way for making strong electronic infrastructure which should be hacking proof and people can go on digitally without hesitation.

The author doesn't think about growing technology without authorities to be on their toes in safeguarding the data protection or privacy from future unknown hacking techniques, if one wants digital technology. We can see a glaring example of Aadhar being digitized which is linked to vital information sources such as bank accounts and mobile numbers of every

[395] Sumant Sen, "NCRB data: Cyber crimes reached a new high in 2017"<https://www.thehindu.com/data/cyber-crime-cases-in-india-jumped-77-in-2017-compared-to-2016/article29889061.ece>NOVEMBER 05, 2019 (last visited on 22.05.2020).

[396] Advocate Robin Bose, "State of Tamil Nadu Vs Suhas Katti - Cyber law case in India" <https://www.legalserviceindia.com/lawforum/cyber-laws/17/state-of-tamil-nadu-vs-suhas-katti-cyber-law-case-in-india/2238/>, July 30, 2013 (last visited on 25.05.2020).

Indian because *according to the Global Risk Report 2019* released by the World Economic Forum (WEF) shows that India had faced the largest data breach of the Aadhar IDs of more than 1.1 billion citizens in the world due to **"lax cyber security protocols"[397].** In 2019, India had more than 525 million internet users across the country. This is predicted to grow over 660 million users by 2023 this is stipulating a big market potential in internet services for the south Asian country[398].

The growth of cybercrime in the current years indicates a great signal for escalating the issue of data protection and internet governance. It is assumed that in the coming years, citizens will demand greater transparency as well as accountability from the governments and service providers. Taking a cue from Europe's General Data Protection Regulation (GDPR), it is essential for governments and businesses to understand that every data is the asset for an individual and eventually individual's rights can be exercised where a mature regulated environment runs. Hence it is important to have increased data protection and governance culture besides this.

IMPACT OF DIGITALISATION ON CYBERCRIME: ECONOMICALLY AND SOCIALLY

Where digital technology provides aid to many companies in many sectors in the country and delivers products and services in a convenient way on the other hand it has an insurmountable economic and social impact on cybercrimes which constitute challenges that can threaten business operations and stifle growth and innovation. Several challenges must be seen before India becomes truly digitalisation. With the pace of digital payments ecosystem there is a high risk of the chances of getting exposed to cyber security risks like online fraud, information theft, identity theft and malware or virus attacks which leads to economic and social harm to the person. In this scenario, we need to answer some important questions like is there adequate governance mechanism and public policy intellect to cope with the impact of digital or cybercrime?

Conceptually, crime is not considered as static but a dynamic and relative phenomenon and subjected to relative changes like socio-political & economical which takes place in the

[397] *Supra.*

[398] Sanika Diwanji, available at<https://www.statista.com/statistics/255146/number-of-internet-users-in-india/>May 26, 2020 (last visited on 30.05.2020).

existing system of society and digitalization or digital economy is one of the important factors influencing incidences of cybercrimes. The economic impact of cybercrime is monetary losses and the overall monetary losses from cybercrime can be immense. The intrusion of cybercrime on the economy can lead to many factors, like effortless accessibility of tools used to gain access to financial systems, new technologies used to by these criminals, the development of new cybercrime centres, and the extent of intelligence and sophisticated techniques used by cybercriminals. Stolen confidential business information and Intellectual property (IP), online fraud, financial manipulation of publicly traded companies, and the cost of securing networks after hacking is done are some of the most devastating effects to companies right now which have the greatest economic impact for protection against data theft, intellectual property theft, and cyber-attacks.

However, a recent report given by Cyber security Ventures denominates everyone to be apprehensive about the digital world. The financial loss on a global level is also so galling. According to the report, *A Cybercrime Revelation released by Cyber security Ventures* shows that-"Cybercrime Cost estimates have raised $6 Trillion by 2021 from $400 Billion in early 2015"[399].

Digitalization has social impact as well. Crime is a non-separable part of social existence and it affects our society in a myriad of ways both offline and online. Anything that happens to the individual is a matter of concern for the whole society because it affects the whole society. It should bear in mind that the social concern for high crime rate is not because of its nature, but due to potential disturbance it causes to society. Likewise, the incidents of cyber-crime are on the upturn, and no wonder, it is a result of rising use of technology. In addition, the victims of crime may lose anything that has value. Safety, peace, money, and property are perhaps basic values in society, because they contribute to the satisfaction of many wishes. So, with the pace of new technologies and new users, digitalization will reshape cyber-risks in 2020.

EFFICACY OF CYBERCRIME ON SOCIETY IN RECENT TIME: MAIN REASON OF ITS CAUSE

[399] Robert Herjavec, "Cybercrime Damages $6 Trillion By 2021", *Cybercrime Magazine*, available at<https://cybersecurityventures.com/hackerpocalypse-cybercrime-report-2016/>Oct. 16, 2017 (last visited on 01.06.2020).

Cyber-crime is that type of dimension of the social matrix with the increasing rapid concern towards the destruction of social- well -being and society. Really the demand of the situation is too aware of the people about the terms & consequences of the cyber crimes. Cyber crime destructs the well being of mankind with its technological destructive trappings of hacking, phishing & spamming as well as child pornography& hate and so on. Mainly the teenagers between the ages of 16 to 18 years are under one of the important helping hands of cybercrime as they use their techno- spoiled minds to access someone else's private information of any individual, business organization, educational institutions or schools.

In the leading case of **Jaydeep Vrujlal Depani v State of Gujarat**[400], the Gujarat High Court held that 'the offences, having been committed against individuals or groups of individuals with a criminal intention or motive to loss or cause physical or mental harm, to the victim, whether directly or indirectly or damage the reputation of the victim by using modern telecommunication networks such as Internet networks (but not confined to Chat rooms, notice board, emails, and groups) and mobile phones (Bluetooth/SMS/MMS)'are cybercrime.

Cybercrime affects our society in many ways like **Malware, Phishing, Spear Phishing, Trojans, Denial of Service attack or Distributed Denial of Service Attack (DDoS), Attacks on IOT Devices, Cyber Stalking, Cyber Bullying, Identity Theft, Ransomware etc.**

There is a famous instance where a state of emergency was declared in the state of Louisiana after a ransomware attack on Louisiana government servers in 2019[401].

Wanna Cry Attack 2017- There was a devastating attack in recent history known as WannaCry ransomware attack in 2017. It was a computer worm. In addition to spreading across computer networks using the Windows operating system, WannaCry encrypted files of the host computer and only allowed access to those files after a bitcoin ransom payment was made. Social impact of this attack was such that it infected over 200,000 victims in at least 150 countries. By this attack the society was shattered as the threat was so pervasive and the only option for recovery was to pay the ransom. This incident also affected the systems belonging to the Andhra Pradesh police and state utilities of West Bengal in India.

[400] R/SCR.A/5708/2018 Order.

[401] Available at<https://gov.louisiana.gov/index.cfm/newsroom/detail/2270>November 22, 2019 (last visited on 3.06.2020).

If we see the current situation in the lockdown of the pandemic Covid-19 then there are ample of recent viral cases which show that people are not aware enough about the repercussions of misusing the digital technology and foremost about the cyber laws to take a precautionary step to deal with. If we take recent instances in the current situation then they show a sheer example of lack of awareness of cyber crime in society.

Instances of cyber crime

***"Bois Locker Room"*- "Bois Locker Room" was an Instagram group which is said to be run by teenage boys of Class 11 & 12. Some screenshots were leaked from that group and have gone viral on Indian social media and shared by all users. The screenshots reveal chats between a group of schoolboys in which lurid discussions were going on about underage women's bodies and their private photos were also shared. But there is also an another side of this story on social media where after few days of this incident another story came and According to the Delhi Police's investigation report, a fake account was created by a girl on snap chat to check the reaction of that boy on sexual assault plan. And these two stories got mixed up while in reality the snapchat and the Instagram chat rooms are two different incidents that have been falsely linked with each other[402]. And those school boys were defamed on all over social media for lurid discussions while in reality these two stories were different.

Guwahati Case- It was reported recently that an Instagram account was sending messages to some young women in Guwahati, asking them to indulge in sexually explicit acts in lieu of money[403].

Delhi Nizamuddin Case-Three persons were arrested on 1st April, 2020 for allegedly posting obscene content on social media in connection with the COVID-19 pandemic and the Markaz gathering at Nizamuddin in New Delhi. In a reference to the media, the accused had posted a video of a woman and her child who were walking on the road, the caption of the video was written as an obscene slur and asked the media to report such news rather than covering only the Nizamuddin incident. The cognizance of the video was taken by the cyber crime cell. He was liable under the relevant sections of the IT act along with IPC sections 153, 295 and 505

[402] Sravya M.G, "Boys Locker Room: Yet Again, Trolls Divert Focus from Real Issues", available at <https://www.thequint.com/voices/blogs/boys-locker-room-yet-again-trolls-divert-focus-from-real-issues>, May, 14 2020 (last visited on 29.05.2020).

[403] Anirban Choudhury, "There's nothing social about social media anymore", available at<https://www.eastmojo.com/opinion/2019/06/28/theres-nothing-social-about-social-media-anymore >Jun 28, 2019 (last visited on 29.05.2020).

for promoting enmity between different groups on grounds of religion, defiling a place of worship with intent to insult and mischief[404].

Gurugram Suicide Case 2020- A story went viral. A complaint has been registered in the suicide case of Manav Singh. He was student of class 12th in Gurugram who took his life after being accused of sexual abuse on social media by the girl who made the accusations but had no proof for the same. This incident came into light when Rishi (His elder brother) wrote the truth behind that suicide case on social media. He said that Manav tried to convince them who had accused him that he was innocent and did nothing to that girl but he couldn't handle the constant threats and believed that his side of the story would not be heard and he got suicide[405].

Even in the pandemic of covid-19, hackers are utilising the popularity of video conferencing platform zoom, targeting the platform with cyber-attack by which the government has to make some privacy changes in the app.

In addition, there are many more glaring instances of cybercrime and there are millions being created every year. One of the biggest reasons is the bounded awareness of the impact and importance of cyber security in society. Even if society is aware then the other main reason is the fatal drawbacks of the Act that the cases have been going unreported. One obvious reason is that the police force is non-cooperative. The police are a powerful authority today which can prevent cybercrime by playing an influential role. At the same time, it can also end up harassing innocent people, preventing them from running their normal cyber business but nothing seems to have happened like this. A cooperative police force is required for complete realization of the provisions of this Act.

India has no specific cybercrime legislation. The IT Act, 2000 and Penal Code, 1860 cover cyber-crimes punishable in India. However, there are several laws which include provisions for controlling such crimes which are as follows:

i. **The Indian Penal Code, 1887.**

ii. **Information Technology Act, 2000.**

iii. **Prevention of Children from Sexual Offence (POCSO) Act, 2012.**

[404] "Three arrested for posting 'obscene' content over Nizamuddin event", *The Indian Express,* available at <https://indianexpress.com/article/cities/ahmedabad/three-arrested-for-posting-obscene-content-over-nizamuddin-event-6350403/>April 6, 2020 (last visited on 29.05.2020).

[405] Available at <https://www.opindia.com/2020/05/manav-singh-suicide-gurugram-bois-locker-room-sexual-abuse-mens-rights/> May 8, 2020 (lat visited on 29.05.2020).

iv. **The Young Persons (Harmful Publications) Act, 1956.**

v. **The Indecent Representation of Women (Prohibition) Act, 1986.**

vi. **National Cyber Crime Reporting Portal.**

vii. **The Young Persons (Harmful Publications) Act, 1956.**

Despite the presence of such laws there are some rules as well but still the cyber-crime rate is on a high. People must be aware of these laws so that they might be aware of their rights and restrictions. According to the *2019 NortonLifeLock Cyber Safety Insights Report*, 63% Indians don't have any idea what they will do in case of identities being stolen, albeit 70% are worried that identities will be stolen and 4 in 10 consumers in India have experienced identity theft[406].

If we talk about identity theft, another instance came into light when Microsoft filed a case against two Noida based call centres recently. Both call centres employed approximately 500 staff and when a call is dialled to any member for support from the US, the caller would be asked to distantly entrust the control of his or her laptop to the employee. Having control of the laptop the call centre staff would give a speculative reason for its malfunctioning and ask for $300 to $400 dollars for repairing it. When the CBI got involved, its owners were arrested including between 400-500 call centre employees. This is just one recent example of organized cybercrime, there are innumerable others and many such crimes never appear in the day[407].

PRECAUTIONARY MEASURES TAKEN BY THE GOVERNMENT

Some of Precautionary measures undertaken by the Government are following-

- In April 2017, the MEITY had issued measures to curb Child Sexual Abuse Material (CSAM) in India.
- An app named "*Samvid*" was introduced by the Government. It is a desktop based Application Whitelisting solution for Windows operating systems. It allows only pre-approved sets of executable files for execution and protects desktops from suspicious applications from running.

[406] Riju Mehta, "Cyber criminals stole Rs 1.2 trillion from Indians in 2019: Survey", *The Economic Times, Apr 13, 2020,* available at <https://economictimes.indiatimes.com/topic/report-cyber-crime> (last visited on 28.05.2020.).

[407] *Supra.*

- On July 6, 2017, a notification was issued by RBI regarding Customer Protection in Unauthorized Electronic Banking Transactions by giving them a Limiting Liability.
- In February 2017, Computer Emergency Response Team (CERT-in), established by the Government of India, launched '*Cyber Swachhta Kendra*' (Botnet Cleaning and Malware Analysis Centre), a new desktop and mobile security solution for cyber security.
- In 2019 The Ministry of Home Affairs inaugurated the Indian Cyber Crime Coordination Centre (I4C) that will enable citizens to raise cybercrimes complaints online and by this they can assist and coordinate electronic investigations of cybercrime and law enforcement agencies in criminal investigation etc[408].

Authorities responsible for enforcing cyber security

In accordance with the IT Act, the Ministry of Communication and Information Technology established the Computer Emergency Response Team (CERT), which acts as the principal agency for resolving cyber security incidents and to raise security awareness among Indian cyber community in India. It is in charge of scanning cyberspace for cyber security vulnerabilities, unauthorized access and malicious activity and can block web pages and websites.

In India there are also some additional agencies regulated by the Indian Government for protection of the people's information security as follows-

National Cyber Security Policy, 2013

This policy was formalized by the Indian Government in 2013. It was taken as a step to prevent cybercrime. It recommended creating a secure cyber ecosystem and strengthening laws, and creating mechanisms for the early warning of security threats, vulnerability management and the response to security threats. The policy provides an initial approach on cyber security from the perspective of protecting data of enterprises and individuals. It referenced protection of strategic digital assets and critical information infrastructure, without significant details of implementation. This policy is supposed to be updated in 2020. The policy states that education and training programmes are required for reducing the cybercrime rate. The policy is planning to set on various national awareness programs across the country with a view to increase cybercrime awareness.

[408] S.S.Rana & Co. Advocates, "Is Cyber Crime Spreading like a Spider Web in India"<https://www.mondaq.com/india/it-and-internet/785120/is-cyber-crime-spreading-like-a-spider-web-in-india>27 February 2019 (last visited on 30.05.2020).

Botnet Cleaning and Malware Analysis Centre (Cyber Swachhta Kendra)

Under the initiative of Digital India, this was set up by the Ministry of Electronics and Information Technology (MeitY), operated by CERT-In under provisions of Section 70B of the Information Technology Act, 2000, working with internet service providers and product or antivirus companies to provide information, to detect malicious programmes and provide free tools to remove such programmes. Similar proactive measures are placed by sector-specific regulators from time to time.

These policies, incentives by the government are rolled out to improve their cyber security as the Public Procurement (Preference to Make in India) Order 2018[409], wherein government procurement agencies will give preference to domestically manufactured or produced cyber security products.

PROPER CHECK ON INFORMATION SECURITY AND ROLE OF SERVICE PROVIDER AGENCIES

Security on cybercrimes is one such problem that we have not been able to achieve. Although there are several laws to prevent and control cybercrime regardless the cybercrime rate is on a high. *A Symantec (an acknowledged leader in cyber security) report* published in January 2019 reveals that 76% of Indians have been victims of some form of cybercrime and 60% have been excruciating or victimized because of computer viruses and malware[410].Over the last 5 years, there has been a 457% increment in cybercrime in India[411]. *According to security software firm Symantec, in 2017*, India ranked third in the list of countries in which the highest number of cyber threats was detected, and second in terms of targeted attacks[412].

[409] Aprajita Rana and Rohan Bagai, "Cybersecurity in India", <https://www.lexology.com/library/detail.aspx?g=4cd0bdb1-da7d-4a04-bd9c-30881dd3eadf>February 24 2020 (last visited on 26.05.2020).

[410] Dinesh Jotwani "The Growing Issue of Cyber Crime in the Technological Age"<http://bwcio.businessworld.in/article/The-Growing-Issue-of-Cyber-Crime-in-the-Technological-Age-/08-07-2019-172939/>, 08.July.2019 (last visited on 26.05.2020).

[411] Ibid.

[412] " India ranks 3rd among nations facing most cyber threats: Symantec" *The Economic Times,* available at< https://economictimes.indiatimes.com/tech/internet/india-ranks-3rd-among-nations-facing-most-cyber-threats-symantec/articleshow/63616106.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst >April,04, 2018, (last viewed on 03.06.2020).

According to the Global Risk Report 2019 released by the World Economic Forum (WEF), India is ranked 15th in the world in terms of cyber security. The number one rank was the least secure country and 60 the most[413].

Role of Internet Service Providers

In order to restrict the harassing behaviour of the stalker, few steps have been taken by the Internet Service Providers. Some provide the opportunity to report abuses. For example, Facebook has certain privacy policies whereby we can restrict strangers from sending messages containing obscene content and abusive behaviour[414]. Internet Service Providers take control measures by sending unwanted emails to spam folders.

Another step towards user security is implementing a strong password policy which should be at least six characters long, and contain alphas, numeric, and special characters.

Many ISPs keep logs of information, as from which IP address the user was connected and at what time. If all activity is consistently logged by the ISP on their servers, it can allow them to watch for trends in the logs. For example, if the logs showed a large number of connection attempts on an unused port, this might alert the administrator that someone was scanning the server, or trying to compromise it. Also, if a dial-up user continually tries to log in with several different passwords, it could mean that someone is trying to guess a password[415].

For all these securities there is a requirement of cooperation between Internet Service Providers and the enforcement agencies when it comes to tracking down the stalker. However, the need for legislative provisions cannot be ignored in the light of taking precautions.

Some legislation related to information security under the IT Act 2000

India does not have a dedicated cyber security law though, The Information Technology Act 2000 (the IT Act) along with the rules and regulations framed there under deals with cyber security and the cybercrimes.

Even the Constitution of India specifically deals with restriction on sharing of cyber threat information. In the case of **Justice K S Puttaswamy & Anr. Vs. Union of India and Ors**[416]

[413] Nikhil Rampal, "India's cyber security a joke for hackers, ranks among worst in the world"<https://www.indiatoday.in/india/story/india-cybersecurity-privacy-data-breach-crypto-hackers-aadhaar-1450572-2019-02-07> February 7, 2019 (last visited on 26.05.2020).

[414] Available at<https://newsroom.fb.com> (last visited on 29.05.2020).

[415] Available at<https://www.giac.org/paper/gsec/1950/user-security-internet-service-provider/103393> (last visited on 29.05.2020).

[416] Writ Petition (Civil) No.494 of 2012.

The constitutional bench of the Hon'ble Supreme Court held in this landmark case that Right to Privacy is a fundamental right, and that is protected as an intrinsic part of the right to life and personal liberty under Art 21 of the Constitution of India, as a part of the freedoms guaranteed by Part III of the Constitution. Also, it must be read with the other existing fundamental rights. However, these Fundamental Rights are not absolute, but are subject to reasonable restrictions given under Art 19(2) of the Constitution of India that may be restricted by the State.

Besides this the offences like hacking, data theft, damage or disruption to computer, virus attacks, denial of service attacks, illegal tampering with source codes including ransom ware attacks could be prosecuted under Sec-66 read with Sec-43 of the IT Act.

Addition to this, The IT Act after amendment in 2008, protected against identity theft (S.66C) or cheating by impersonating online (S.66D), Victims of revenge porn may register complaints for violation of their privacy under S.66E as also under S.67 and S.67A. Sec-67A provides for prosecution of pornography and Sec-67B child pornography respectively. In case of the child pornography, the Prevention of Children from Sexual Offences Act, 2012 (POCSO) may also be invoked.

Moreover sec-69 provides Powers to issue directions if there is any interception or monitoring or decryption of any information through any computer resource and sec-72 imposes a penalty, where any person holding any power discloses records, book, register and information accessed in the course of his or her duties without the consent of the concerned person[417]. Apart from this, Sec-46 of IT Act also provides for remedies against data theft, hacking, virus attacks and financial frauds covered under Chapter IX (S.43 to S.45) of IT Act, 2000.

There are many more provisions under IT Act, 2000 dealing with cybercrimes but besides this, some Indian penal code, 1860 also deals with data protection law like Cases of forging any electronic record, credit or debit card, or even cloning a mobile SIM with malicious or fraudulent intention to cause wrongful loss or gain could be prosecuted under (S.463 to S.471 IPC, as applicable), Sec-419 for cheating of personation, and Sec-409 for criminal breach of trust[418].

[417] The Information Technology Act, 2000, No. 21, Act of Parliament, 2000.
[418] Indian Penal Code, 1860, No.45, Acts of Parliament, 1860.

In the landmark case of **CBI vs. Arif Azim**[419], sony India Private Limited operated a website enabling NRIs to send sony products to their friends/relatives in India after paying for it online. An individual gained access to the credit card number belongs to an American National and ordered Sony products by using her identity. He was convicted under sec-419 of IPC, 1860.

FAIRNESS OF PUNISHMENT IN THE CONSTITUTION OF INDIA: A CRITICAL EXAMINATION

There have been two recent radical changes to the privacy framework. First, on August 24 2017, the S.C of India held that the right to privacy is a fundamental right guaranteed under the Constitution of India[420].The right is procurable to the residents of India against the state and the government. Second, In December 2019, The Personal Data Protection Bill, 2019 presented by the government, in the parliament, by which there would be possibility of creating the first cross sectoral legal structure for data protection in India[421]. Therefore, it seems likely the enactment of extensive privacy legislation will come into force in India next year.

But meanwhile the offender/stalker must be charged for Article 21of Indian Constitution[422] because his actions are violative of this article and India has not yet enacted specific legislation on data protection. However, The Indian legislature included Section -43A and Section -72A in The Information Technology (IT) Act, 2000, after amendment in 2008, which gave a right to compensation for improper disclosure of personal information. The stalker aims at entering into the private space of the victim by that means ruining his/her right to privacy and right to personal liberty. The stalker always tries to monitor each and every move of the victim by following the victim on social networking sites, e-mails, messages or through telephone calls or through any other mode. This causes distress and a sense of threat in the mind of the victim. The victim cannot enjoy his personal space. So, it is not justifiable to the victim under the constitution of India.

[419] 2003 (IT ACT, 2000)

[420] Justice K S Puttaswamy (Retd.) & Anr. Vs. Union of India and Ors, Writ Petition (Civil) No. 494 of 2012.

[421] "Personal Data Protection bill, 2019", Pub. L. No. 373 of 2019, accessed on 03.06.2020, http://164.100.47.4/BillsTexts/LSBillTexts/Asintroduced/373_2019_LS_Eng.pdf.

[422] INDIA CONST. Art- 21 which says "No person shall be deprived of his life or personal liberty except according to procedure established by law.

The Indian Constitution under Art-14 states equality before law. We can see that our Constitution gives guarantees for Equality but when we read the legislative provisions, it shows that there is too much gender inequality. In India, the laws are gender biased as there are ample legislations which show that the law-makers considered women as the weaker section of the society hence, every statute revolves around protecting women. However, such gender inequality doesn't hold good when it comes to the present scenario.

Section 509 of Indian Penal Code, 1860 addresses the issue of offending the modesty of a woman. This section should also be reframed by the term "any person" in place of "woman". A female stalker can also offend the modesty of a man through sending obscene materials on the internet or e-mails or messages. Thus, the lawmakers should make an effort to promote the welfare of both man and woman and not just the woman from the deficient-effects of cyber stalking.

Section 354D of Indian Penal Code is at present the only provision that has some proximate relation to the crime of cyber stalking. It is evident from the provision that it solely protects women. This violates Art-14 of the Indian Constitution. However, it is true that this Section was added recently through Criminal Amendment Act 2013 after the very famous Delhi gang rape case took place. This section should be reframed using the term "anyone" or "any person" to make it non violative of Article 14.

Section 354C of Indian Penal Code, 1860 is concerned with voyeurism. This section is also gender biased as it protects only women. It reads as: Any man who watches, or captures the image of a woman….[423]

One of the features of cyber stalking is the anonymous identity of the stalker. There has been a suggestion to put restrictions to keep the identity anonymous. This, however, appeared to be a debatable topic as almost the laws of every country ensure Freedom of Speech and putting restrictions on anonymous identity would be violative of this freedom. **In Sahara India Real Estate Corp. Ltd. v. Securities & Exchange Board of India**[424] the court held that the freedom of speech and expression as provided under Article 19(1) (a) is not an absolute right. It means there are some reasonable restrictions on the freedom of speech and expression. But increment in the number of cases in recent time, it shows that Art-19(1) (a) is followed often without restrictions and this is not justifiable under the Indian Constitution.

[423] Indian Penal Code, 1860, No.45, Acts of Parliament, 1860.

[424] Media Guidelines Case, C.A. No. 9813 of 2011, decided on Sept. 11, 2012.

SUGGESTION FOR CYBERCRIME PREVENTION

The author thinks that it may not be possible to completely eradicate cybercrime and ensure complete internet security even businesses cannot reduce their exposure to it by maintaining an effective cyber security strategy by using a defence-in-depth approach to secure systems, networks and data. Even in every instance of cybercrime it is not possible to completely rely on the police, national security departments, and commercial cyber security firms for getting protection from the wrong doers. No wonder legislation provisions are there to provide punishment for the offence. However, for the average computer user, it's quite hard to go up against a cyber-crook or wait for deterrent punishment after the incident. So the best approach is to follow some common best practices to protect ones from such cybercrime which are follows-

1. Protect the computer system from internet security suite- Use any security which provides real-time protection against existing and emerging malware including ransom ware and viruses which helps to protect private and financial information when one goes online.

2. Use strong passwords- Do not keep the same passwords for various social media accounts, passwords must be a mixture of words and special characters. Use the strongest one and don't give any social media an authority to keep that password strong like Google, chrome. Everyone must Log out every time from the device that is unfamiliar to or not in use.

3. Always keep the software updated- Always use the latest and update antivirus software to guard against virus attacks and always keep backup volumes or data of everything so that one may not suffer any data loss in case of virus contamination.

4. Strengthen home network- It's the best to use a VPN whenever using a public Wi-Fi network whether it's in a library, café, hotel, or in an airport. A VPN encrypts all information as soon as it leaves devices. It means hackers will only be able to intercept nearly impossible to decipher traffic and if cybercriminals manage to hack your communication line, they won't clog anything but encrypted data.

5.Social media settings- Cybercriminals may only need a few bits of personal information for instance the name of one's pet to clear security questions, if someone posts one's pet's name or reveals one's mother's maiden name then he/she might expose the answers to two common security questions. So keep it safely and share as little as possible.

6. Aware the young ones- keep them aware about the consequences of using strong and different passwords for every online account. They have to assist others from accessing their personal information and let them know about the updating of security software to protect their family against scammers, hackers, and other online threats that can compromise their computer system.

7. Identity theft can happen anywhere- It is smart to know how to protect identity even when travelling or going outside. There are a lot of things that can help the criminals out from getting one's private information on the road so always keep travel plans off social media and use a VPN when accessing the internet over hotel's Wi-Fi network**.**

8. Know what to do if one becomes the victim of cybercrime- If one believes that he/she becomes a victim of a cybercrime, one need to inform the local police and, in some cases, the FBI for the purpose of obtaining assistance. This is utmost important even if the crime seems minor. One's report may assist authorities in their investigations or may help to deter the criminals from taking advantage of other people in the future and even now citizens can report cybercrimes online on The Indian Cyber Crime Coordination Centre (I4C), launched in 2019.

9. Talk to children about the internet- parents can teach to the kids about acceptable use of the internet and what they post on the net about other people and the consequences of those posts. Also, the parent must have a talk with their child. Let them know that they can come to them if they're experiencing any kind of online harassment, stalking, or bullying.

10. Protection against data theft, intellectual property theft, and cyber-attacks- Cyber insurance will protect against data theft, intellectual property theft, and cyber-attacks. If a person purchases cyber insurance they will be compensated when they ever are victim to cybercrime. This need has been proposed by DSCI (Data Security Council of India)[425].

- ***Cyber security challenges needed for transformation in India***

One of the greatest lacunae in the field of Cyber Crime is the Jurisdiction in India. It is the most debatable issue on the maintainability of any suits. In India, the Information Technology Act, 2000 concerned the "extraterritorial jurisdiction" under Sec-75. This section makes it clear that whether an offence is committed outside or in India, the offender shall be governed by the provisions of the Information Technology Act irrespective of the fact whether he is a

[425] Policy Bazaar, "cyber Security Insurance" available at <https://www.policybazaar.com/commercial-insurance/cyber-insurance/>, 08.05.2020 (viewed on 03.06.2020)

citizen of India or not but such an offence to know that the S.C now struck down the curb on crypto currency trade in India and guided legislators to make regulatory authorities on this.

India has to take steps to set up its cyber defence such as establishing effective cyber security groups at the defence ministry in order to cooperate with other countries as well. India should strengthen its domestic cooperation through information sharing like Japan is concerning IT become one of the safest places in the world and have slowed its development of cyber security in 2020.

India should have its own investigating branch like the **National Security Branch (NSB) to investigate cybercrime.** The United States of America was the first who used to investigate the crime and for that, a number of laws have been passed in recent years by the USA. There is also utmost need for Exhaustive and continuous training in cybercrime investigations and forensics to organize quantity investigations in states as well as central law enforcement departments.

There is also a lack of cooperation and collaboration between Law Enforcement Agencies and Central agencies to cope with cybercrime investigation and also deficiency of a platform where different state police units can collaborate or assist investigation officers in cybercrime cases.

Sharing Information -The Indian government is responsible for explaining to its citizens the necessity of sharing information on the methodology of cyber-attacks and alerts the public on the current threats so that India can minimize in a timely manner. The United States introduced a law called "Cyber Security Information Sharing Act 2014(C.I.S.A)" they have enhanced sharing of information about cyber security threats to improve cyber security in the country. Such laws are required in India as well to share threat information among citizens or netizens.

To reduce the decade's sized gap in its cyber strategy, the Indian government should work on a number of policy changes. There should be new partnerships between the government and technology leaders in the private sector which would help India to rapidly augment its digital security capabilities like Japan is the good example who is proving that partnerships between the government, large organizations, and technology companies can overcome decades of policy inaction and create an example for other countries to follow even the existing Information as well.

India is also lacking national cyber security architecture. The architecture provides a framework for designated agencies to assess the nature of any threat and tackle them effectively, to monitor, certify and fortify India's networks in accordance with the law but there must be concerned with the computer systems, or network that is situated in India. Thus, the solution provided by Indian laws is limited as there is limited enforcement for the same and there is also a need of cooperation between the countries so that extradition policies may come into picture when there is a jurisdictional issue amongst the countries.

The Technology Act does not have adequate provisions for cyber security so there is a need of the hour for implementing new provisions and comprehensive cyber security law. In addition, laws pertaining to cybercrime may become obsolete in India like currently, there has been no law defining crypto currencies and fake news. At the time of writing this paper, the author got

is a long way to go before India has the necessary structure in place. However, to assess the nature of cyber threats and respond to them effectively there must be a National Cyber Security Agency (NCSA) as some analysts have also recommended for the same.

CONCLUSION

This research paper has striated many apropos and the cyber-frontier perspective with a view to highlight pitfalls pertaining to security and development assistance. Legal measures certainly play a vital role in combating crime and in a country like India where population remains enormously and technological advancement make it impossible to reduce cybercrime offence; the legislators should also address different areas like encompassing jurisdictional issues of Cybercrime as well. To confront the challenges of potential cybercrimes in 2020, there is a need to overcome the obsolete model of dealing with the situation and build a new model that is effective and efficient like we have seen the precautionary measures taken by the government and rules & policies which are neither known to most of the people in the society because these measures have limited implementation nor effective much. The need for effective legislation was also required. This paper tried to give effective suggestions to the people to tackle cybercrime on its own way and cyber security challenges to the government, needed for transformation in India. It is expected that this research will make known, raise awareness and motivate others to further look into the effective measures needed to be taken and the interaction between cyber security and cognitive factors