

# LEGALFOXES LAW TIMES

## Cyber security: a rising question on increase in cyber stalking of women during Pandemic

By: Bhawana Sharma

### ABSTRACT

Modernization in technology and infrastructure has made the life comfortable for the whole world. The rapid development in cyber space has eliminated the limitation of geographical boundaries and connected different countries by providing a platform for virtual communication. This sudden advancement in cyberspace has increased the cyber vulnerability for the entire Globe including India. Also, cybercrimes are adversely affecting the weaker section of the society i.e. women and children. They are the vulnerable parts of the society and are easily trapped by the perpetrators. Recently, it was found that there has been an increase in cybercrimes like stalking, hacking, malware, child pornography, etc. that has raised the question on cyber security of India especially during COVID - 19. Further it was observed that women are psychologically hampered by the offenders and play the role of victimization. Cyber stalking is one of the major problems faced by the women in their day to day life. Moreover, the pandemic situation has clarified that women are facing problem in understanding and controlling their networks. Also, they are continuously being stalked by their colleagues and boss through social media that disrupt the life of the women. Although there are numerous laws framed for the protection and safeguarding of women like that of IT Act 2000, Criminal Amendment Act 2013 and sexual harassment at workplace (Prevention, Prohibition and Redressal) Act 2013. But it is sorrowful to say that the laws are not creating any deterrence in the minds of the criminal. This paper reveals the problem faced by women during Pandemic, need for sensitization of cyber based education, institution of more stringent law along with the effective measure that can help in building the safe and healthy environment for all the citizens including Women and children.

**Keywords:** Cyber security, Cybercrime, COVID - 19, Cyber stalking, NEP 2020.

## **INTRODUCTION**

We are living in a modernize world where more than half of the total population is dependent on Internet. Internet has become an essential need in today`s world as it has made life so comfortable and easy that people can`t think life without it. It has changed the life style and connected people beyond the geographical boundaries. It has organized an effective and virtual ways to communicate people from different parts of the world. The first internet prototype was introduced in late 1960s along with the advanced research project agency network (ARPANET). From the year 1970s the technology started growing and now it has gained huge popularity all around the globe. The development in cyber space has proved to be useful for many people. It has provided a platform to do e - business, online education and has also helped the government agencies to maintain their confidential data. In common parlance “Cyber space” is nothing but a non - physical domain which carries flow of information and communication between networks and computer systems. Cyber space has earned a remarkable progress, but at the same time the cyber vulnerability has become crucial matter for discussion. Due to rapid development in cyberspace the number of cyber crimes has also increased.

Cybercrime are the crimes that are committed through computers and are illegal in nature like hacking, online theft, child pornography, stalking, malware, fraud, obscenity, cyber terrorism etc. It is an attack on all the data and information stored with the government, corporate sectors and also with the individuals. Cyber crime has become a sensitive matter as it can destroy the security of the nation by gaining all the unauthorized data. Cyber crime is imposing an adverse effect on the weaker section of the society i.e. children and women. Cyber stalking against women is the rising issue and has become a matter for dialogue as it causes harm to their dignity and destroys their confidence. Further, it was found in most of the cases that the women are afraid to report cyber crime cases because of the societal stigma on their character. As per the reports it was found that there has been a sudden increase in cybercrimes against women during lockdown. They are several cases of cyber stalking and false accounts on social networking sites which were coming into picture by the cyber security agencies and national commission for women.

Cyber stalking is a crime that involves two persons the attacker and the victim who is consistently harassed and threatened by the attacker over a long period of time through internet or any electronic media. It is a heinous crime against an individual, a group or an organization and mostly the females get victimized and harassed by the stalker. Cyber stalking may encompass identity theft, threats, monitoring, solicitation for sex or gathering of information to threaten the victim. It can be performed with an intention to humiliate, defame or out of anger, jealous, revenge in love etc. Social media applications like instagram, facebook, twitter has become a hunting ground for the users especially for the females. In 2018 National Crime Record Bureau (NCRB) report says that Karnataka (with 5839 cases), Uttar Pradesh (with 6280 cases) and Maharashtra (1262 out of 3511

cases) are the states having huge number of cases related to cyber stalking of women and children<sup>1</sup>. The report clearly demonstrates the power of the stalker and their hands in psychological break down of women in the society. Cyber stalking is consisting of Internet stalking (use of internet to slander and endanger their victim) computer stalking (exploits the working of Internet and windows operating system of the targeted computer) and E - mail stalking (involve unsolicited mails).

To avoid cyber crime the government took many initiatives to strengthen the cyber security in India. Cyber security is the procedure and technology to safeguard the data, network and computers from cyber attacks. The ministry of communication and Information Technology provides a strategy outline called the National Cyber Security Policy. The sectors like health care, retail trade, media and energy face Advance Persistent Threat (APT). The growth in data consumption is more than 35% which has raised the issue of a techno - legal nature. The countries have started following different approaches like data localization, data sovereignty, handling fake news, internet governance and international law. The motive of the government body is to safeguard public and private infrastructure against cyber attack. The concept of cyber defense is adopted to address the upcoming challenges such as Cross-Border Privacy Rules (CBPR), EU's General Data Protection Regulation (GDPR) and US` Clarifying Lawful Overseas Use of Data (CLOUD) Act.<sup>2</sup>

In India the authority has created a Cyber Security Policy in 2013 with the aim to maintain safety and security in cyber space. Now in 2020 the authority came up with another cyber security policy which seeks to create a safe, secure, resilient, vibrant and trusted cyber space for the economic progress of India<sup>3</sup>. The government has launched the cyber crime portal [www.cybercrime.gov.in](http://www.cybercrime.gov.in) for filing of complaints<sup>4</sup>. As per the data given by the National Crime Records Bureau (NCRB) there has been 30% jump in cases recorded in 2017 (21796) with 4971 case Uttar Pradesh has the highest number of cyber crimes followed by Maharashtra and Karnataka with 3604 and 3174 respectively. The new crime head was introduced for the cases reported under ATM fraud and online bank fraud. In comparison to 2017 NCRB report, the cases in 2016 were 6% more than the 2015.

In India Cyber Security Policy strengthen the country`s security along with other like the Indian Computer Emergency Response Team (CERT - In), the Cyber Surakshit Bharat held by the Ministry of Electronics & Information Technology (MeitY) and the National Critical Information

---

<sup>1</sup>Jayprakash S Naidu, *Tops in cases of Cyber staking, ATM - related and online frauds*, Hindustan Times, 9 January, 2020.

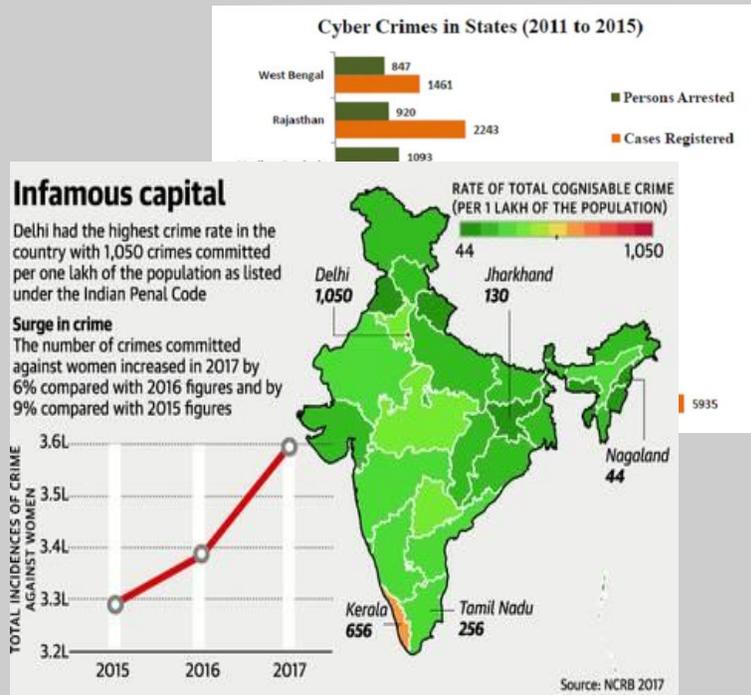
<sup>2</sup>GulshanRai, *Why cyber security should be India's foremost priority*, Economics Time, 31 October, 2019.

<sup>3</sup>SudhiRanjanSen, *New cyber security policy aims for safe, resilient to boost economic progress*, Hindustan Times, 27 January, 2020.

<sup>4</sup> IANS, *Government taking steps to prevent online frauds: Minister*, Economic Time, 5 February, 2020.

Infrastructure Protection Centre (NCIIPC)<sup>5</sup> to safeguard the confidential data and prevent cyber attack.

Picture - 1 shows the number of cases registered and number of persons arrested from 2011 - 15. Also reflects that the registrations of cases are more than the arrest of the accused.

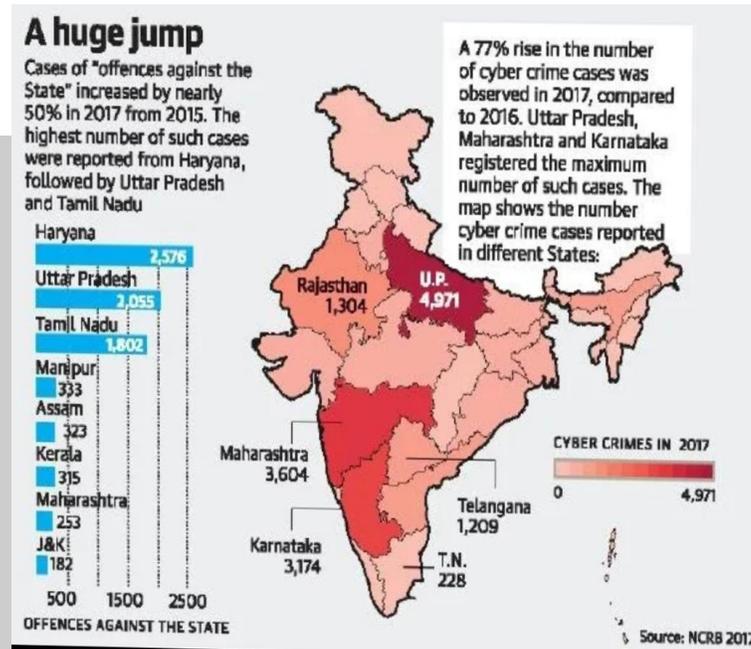


Picture 2 shows the increase in crime against women from 2015 – 2017.



Picture – 3 shows a huge jump in cyber crime in 2017.

<sup>5</sup> ET Government, *Opinion: National Cyber Security Policy needs trans - sectoral synergies*, Economics Times, 15 April, 2020.



## CYBER CRIME DURING PANDEMIC SITUATION

During COVID - 19 pandemic the central government has announced national lockdown and applied DM Act 2005<sup>6</sup> to combat the spread of Coronavirus. The Home Minister along with Prime Minister declared lockdown for maintaining uniformity all over India to deal with COVID- 19. The Ministry has framed certain guidelines to be followed during lockdown such as no mass gathering, work from home etc. These rules are framed by using the DM Act 2005<sup>7</sup> and if anyone disobeys the instructions will be punished under the DM Act 2005<sup>8</sup> and IPC<sup>9</sup>.

Keeping in mind the rules framed by the central government many institutions, government agencies and industries started working from home. This has resulted in increase in demand of internet as people started their operations and meetings online through various online applications like Zoom, Microsoft team, etc. As per the reports on global technology website CNET says that there has been an increase in hacking attempts on system from 15% to 20% from the beginning of the year till the month of March. The recent information from International Criminal Police

<sup>6</sup>The Disaster Management Act No.53 of 2005.

<sup>7</sup> PTI, *Lockdown violators booked under IPC, Disaster Management Act: Home secretary to states*, The Times of India, 2 April, 2020.

<sup>8</sup>Disaster Management Act No.53 of 2005, s.51, s.52, s.53, s.54, s.55, s.56, s.57,s.58, s.59, s.60.

<sup>9</sup>Indian Penal Code Act No.45 of 1860, s.188.

Organization (INTERPOL)<sup>10</sup> stated that the attackers are trying to extract the crucial information from medical institutions and hospitals in 194 countries including India.

As per the Business leaders and other decision makers there are high chances of losing confidential data during the COVID - 19. The cyber attackers are targeting the citizens` wallets and also their personal data. There has been growth in financial cyber crimes including frauds using cards and e - wallet. The government is taking various steps to strengthen the surveillance and legal frameworks against the attackers during Pandemic situation. In this, common people are easily getting exploited by the perpetrators as they are not aware about cyber related crimes. According to the report of National Cyber Security Coordinator (NCSC) the cyber criminals have introduced thousands of “fraud portals” on Coronavirus. These sites have tempted thousands of Indians eager to donate and give their contribution to fight against Coronavirus. The government is taking steps to put a control over online frauds. According to the Union Minister of State for Home Affairs G. Krishan Reddy said that the government has constituted an Inter-ministerial committee regarding phone frauds with the stakeholder organization.

The Pandemic situation has also posed lots of challenges for women especially for the professional women`s who are working from home for a long period of time and are harassed by the offender while performing their job. Many women approached to the experts for seeking guidance for reporting complaint of sexual harassment. According to Akancha Srivastava founder of Akancha against Harassment stated that women are playing a role of victim and are harassed in subtle way by their boss and colleagues. Also, women are worried about their job security and are in dilemma as to whether to speak or not. As a result many of them overlook the indecent approach coming towards them and try to make compromise with the situation. The National Commission for Women (NCW) stated that there has been a down fall in the reporting of complaint because many women don`t wish to engage themselves into official complaints and wish to consult what they can do in such issues.<sup>11</sup> Along with this some employee women are facing problem with their colleagues as they are inappropriately dressed up during the virtual communication that makes them feel uncomfortable. According to Vineet Kumar, founder of cyber peace foundation said that during lockdown the cases of “sextortion “has increased. The people are forgetting their securities and easily get connected without thinking on social networking site. Vandana Verma, the founder of InfoSec girls said that when the whole country is working from home the cyber criminals have become craftier and innovative in the technologies. Also, there are lots of fake profiles; online stalking and cyber bullying are also intimidating.

---

<sup>10</sup>Puniti Pandey, *Massive shift to digital space increases the need for cyber security experts*, Times of India, 28 May, 2020.

<sup>11</sup>PTI, *Covid-19 lockdown: working women complain “online” sexual harassment*, The New Indian express, 1 June, 2020.

According to CSC e - Governance Services India that holds the license of providing internet services declared that there has been an increase in data consumption from 2.7 terabyte (TB) to 4.7 TB from 10<sup>th</sup> March till 30<sup>th</sup> March, 2020.<sup>12</sup>

### **LACK OF AWARENESS: A MAJOR PROBLEM**

The main problem of increase in cyber crime is due to lack of public awareness related to internet. In today`s world People are dependent on internet for various purposes like online shopping, online payments, e - business and online studies etc. Modernization has improved the technology but also increased the level of risk for the common public. Cyber vulnerabilities have become a sensitive and a matter of concern for the world. People take internet for grant and never think before giving their personal data to any application. Sometimes these applications grasp all the confidential data and use it maliciously.

Cyber stalking is one of the major problems that a female face in her life and in most of the cases they never approach to the police or court for getting justice. As per the reports there has been a significant increase in complaints related to cybercrime against children and women during lockdown. According to Rekha Sharma, chairperson of National Commission for Women (NCW) said that there is a lack of awareness among the women about where to reach out and about the safety measures that needs to be considered in order to be safe and secure on cyber space. She advised that women should not upload any personal detail or pictures on social media.<sup>13</sup> Also, the cyber experts mentioned that the cases are just “the tips of iceberg” as most of the women are afraid of reporting. Cyber stalking is a shameful act against the society and also towards the humanity that disrupts or can cause profound harm on the physical and mental condition of the women. This issue is not restricted only to India but it`s a global problem that gives rise to injustice towards the women as they are the vulnerable part of the society.

Moreover, there are many other cybercrimes that are creating destruction and making an unsafe environment for the citizens like hacking, malware, phishing etc. Further, it was noticed that the hackers steal money and send it to other hacked digital wallets so that they can`t be traced back easily. There are many links or unknown applications which contains malware that gives the attacker an access to hack the device and access to control. Generally, people have a misconception that the applications available at Google or Apple store are secured however that`s not necessary. As it was found recently that there are many applications on play store which have malware and were using to steal all the confidential information. Even in many cafes the Wi - fi facilities are

<sup>12</sup> PTI, *Significant increase in cyber crime against women during lockdown: Experts*, Economic Times, 2 May, 2020.

<sup>13</sup> PTI, *Significant increase in cyber crime against women during lockdown: Experts*, Economic Times, 2 May, 2020.

used by the customers that are not safe as there are high chances of hacking because they are not properly equipped in terms of security.<sup>14</sup>

There are around more than 60 Crore internet users in India out of which 29 Crore are in rural areas. However, the people who are living in urban and developed areas are much aware of cybercrime than the rural area. In rural areas people are not much educated to handle and understand the criticalness of cybercrime. As a result, they are trapped by the attackers and sometimes finds difficult to recover.

Keeping in mind the interest of the general public the government has framed various laws for the protection of the citizen`s especially for the weaker ones and is trying to create sensitization on cybercrime and cyber security. Along with this, people should also take all the effective and protective measures on social networking sites especially before accepting any friend request from unknown. Moreover, it should be the duty of the women to not to overlook any attack by the offender that can cause harm to them.

### **STRINGENT CYBER SECURITY LAWS: AN EMERGING NEED**

Due to advancement in cyber space the cyber vulnerabilities have gathered the attention of whole world. As per the reports India comes on second rank in most cyber attacked countries in the world. Recently it was observed that there are numerous cyber related crimes committed by the offenders during COVID - 19 like child pornography, cyber stalking, hacking, identity theft, online scams etc. These malicious practices are creating an anxiety or threat for the citizen`s especially for the woman who suffers humiliation and harassment on cyber space. The crimes like cyber stalking and bullying can be committed through sending, sharing insensitive or posting malicious content against women and causes a severe mental health issue. Cybercrime has become a huddle in the development and security of any nation as it hampers the individual privacy and rights. Cybercrime against women and children such as pornography, stalking, harassment has become a matter of concern. Child pornography is a heinous crime as it destroys the dignity and raises question on the safety and security of children below the age of 18years. During lockdown the research on child pornography was done by the Indian Child Protection Fund (ICPF) shows that there has been increase in demand for “child porn”, “teen sex video”.<sup>15</sup> Moreover Nivedita Ahuja, spoke person for ICPF said that the pornographic websites are playing hide and seek game with the Law and Indian Judiciary by changing their URLs.<sup>16</sup> To protect the children the government is trying to reach them and also provide security. According to RakshitTandon, cyber security expert and consultant in panel discussion at Amity University on challenges in cyberspace said that most of the cyber crimes are committed by the youth and college students. Now a child of class 6 also

<sup>14</sup>Ankush Johar, *This is how hackers can comprise your mobile wallet*, Economics Time, 3 November, 2017.

<sup>15</sup> Express New Service, *Demand for child porn increases during lockdown*, The New Indian Express, 14 April, 2020.

<sup>16</sup>AmbikaPandit, *ICPF report warns of sharp raise in demand for online child pornography during lockdown*, Times of India, 14 April, 2020.

knows how to hack Wi-fi password but mostly offender claims it to be ethical hacker, although there is nothing ethical hacker in the laws.<sup>17</sup>

To maintain cyber security the government came up with IT Act 2000 on 17th October, 2000. The act was introduced with the motive to deal with cybercrimes and electronic commerce and is applicable to whole India. Later on, Amendment was made in 2008 to provide a strong data protection regime and also provided security of critical infrastructure. The act covers offences like hacking, data theft, illegal tampering, and denial of service.<sup>18</sup> Under IT Act amendment 2008 the protection was given against cheating by impersonating online,<sup>19</sup> identity theft.<sup>20</sup> The victims of porn can file their case in both IT Act<sup>21</sup> and Penal Code.<sup>22</sup> Under IPC there is provision for wrongful loss and gains or fraudulent acts,<sup>23</sup> outraging modesty of women,<sup>24</sup> assault or criminal force on women to outrage her modesty,<sup>25</sup> stalking,<sup>26</sup> word or gesture or act to humiliate the modesty of the women.<sup>27</sup>

In order to protect and prevent such heinous crimes on internet the government came up with many laws and amendments under IT Act 2000, Criminal Law (Amendment) Act 2013, POCSO Act 2012<sup>28</sup> and sexual harassment of women at workplace (Prevention, Prohibition and Redressal) Act 2013. These laws are enacted to safeguard the interest of the women and children. Under POCSO act special care and attention was given against child pornography so that the children can develop and grow in safe environment. The famous recent case of “Bois Locker Room” had 22 members out of which 2 are college students. In this case the boys were planning to commit a gang rape of a classmate and have photos of school girls posted on Instagram multiple of screenshots were shared on social networking sites before the police took cognizance and register case under IPC and IT Act 2000. According to the reports the minors were booked under the Juvenile Justice Act.<sup>29</sup>

Further During the lockdown many women have complained regarding the indecent messages, pictures and inappropriately dressed up male employees in the virtual meetings that make them feel uncomfortable in the discussion. Also, they are been called up by their boss at midnight for small works that can be easily handled through mail. These offences make them mentally and emotional disturbed and sometimes they lose their confidence on social media. According to National Commission for Women (NCW), 54 complaints were received in the month of April

<sup>17</sup> PTI, *One cyber crime takes place every 10 minutes in NCR: Experts*, Economics Times, 1 September, 2017.

<sup>18</sup> Information Technology Act No. 2000, s.66; s.43.

<sup>19</sup> Information Technology Act No.2000, s.66C.

<sup>20</sup> Information Technology Act No.2000,s.66D.

<sup>21</sup> Information Technology Act No. 2000,s.66E; s.67; s.67A.

<sup>22</sup> Indian Penal Code Act No.45 of 1860, s.67A;s.67B.

<sup>23</sup> Indian Penal Code Act No.45 of 1860 , s.463; s.464; s.465; s.466; s.467; s.468; s.469; s.470; s.471.

<sup>24</sup> Indian Penal Code Act No.45 of 1860, s.354.

<sup>25</sup> Indian Penal Code Act No.45 of 1860, s.354(A).

<sup>26</sup> Indian Penal Code Act No.45 of 1860, s.354(D).

<sup>27</sup> Indian Penal Code Act No.45 of 1860, s.509.

<sup>28</sup> The Protection of Children from Sexual Offence Act, (32 of 2012).

<sup>29</sup> HT Correspondent , *20 boys from 4 reputed Delhi –NCR school part of lewd chat club*, 6 May, 2020.

while 34 and 21 were reported in the month of March and February respectively. The cyber expert mentioned that around 412 genuine complaints were filled on cyber abuse from March till April. Out of which there are 396 complaints are serious in nature like unsolicited obscene pictures, indecent exposure, ransom demand, malicious email claiming their accounts are hacked, blackmailing related etc.<sup>30</sup>

But the question which comes into picture is that “Are the laws really creating any deterrence in the minds of cyber attackers?”

### **NEED FOR EFFECTIVE REPORTING BY POLICE**

Police are the source of maintaining peace and harmony in the society by taking harsh and necessary steps to reduce the crime rate within the territory of India as per the law. They are the public servants whose aim is to implement and play a proactive role in detecting the cases along with its investigation. It should be the duty of the police officer to report the cases and take all the effective measures in providing Justice. However, it was observed that sometimes the women are harassed by the police officers or face hostility and are given alternative options to avoid reporting. Moreover, women sometimes feel that complaint against police personnel is very difficult as these officers are in powerful position to negotiate and because of this reason they prefer not to approach to them. Hence, it is essential to sensitize the police officers and also monitor their work so that the victim should not suffer misbehavior from the officer side. And in case if the police neglects to report or investigate then the strict action should be taken to ensure that such acts won't happen in future. Also, it should be the duty of the police officers to guide the victims about not to make any delay in reporting the case as it becomes harder to prove the commencement of crime. According to NCRB 2018 data, there are 12,947 cases of stalking were reported out of which 9,438 were new and rest 3,505 cases are from previous years. Hence, it is urgent to aware both police and public to raise voice against any sexual assault or harassment.

### **CYBER BASED EDUCATION: TO STRENGTHEN THE CYBER SECURITY**

Cyber security is the urgent and crucial need of the hour for the nation in order to eliminate or eradicate the cybercrime. The issues related to cybercrime can only be handled through spreading and creating sensitization on cyber related education, crimes and judicial mechanism introduced by the established laws. As per the data there is a scarcity of professional in the field of cyber security in India where the government is trying to digitalize everything. The cyber security is an important and crucial call for the nation as through this we can secure our personal data from any attack. These cyber security professionals are the persons who protect the servers, networks and other hardware and data from any cyber - attack. They identify risk and conduct ethical hacking to test for vulnerability or do research on new type of cyber crime. These cyber security professionals

---

<sup>30</sup> PTI, *Significant increase in cyber crime against women during lockdown: Experts*, Economic Times, 2 May, 2020.

help the government and organizations to develop solution and secure their data.<sup>31</sup> Further the women who are facing the issues related to cybercrime can take the help and consultation from National Commission for Women (NCW).

With this growing fear the institutions and various coaching institutions started providing courses for the students and professionals on cyber security. The Indian Institute of Technology (IIT) has organized a comprehensive cyber security course to safeguard public interest. The students who are interested to make their career in cyber security must have a good understanding of programming and networking. They should be motivated to pursue a career in this field and should carefully choose the courses along with universities. It is important for the government and universities to train the student by exposing them to the real-life situations through projects, internships etc. This will enhance their learning and also encourage them to find the solutions of such problems. Moreover, it will help many organizations and government to move toward digitalization of India by safeguarding the information in cyber space. There are five top free courses available during lockdown for the students who are interested and want to explore a career in cyber space are- springboard: foundation of cyber security, IT fundamental for cyber security, great learning academy: introduction to Information security, Stanford school of engineering: introduction to web security, ex.: introduction to cyber security.<sup>32</sup>

Further, there has been an exponential growth in cyber security training and the government has released the first National cyber security policy directing to raise the number of cyber security officials. As per the data the number of cyber security professionals has increased from five Lakh to 35- 40 Lakhs in 2020. And recently after 34 years the Ministry of Education has introduced New Education Policy 2020 with more holistic way of learning for the students. The policy has introduced coding classes from class 6 onwards for the students to observe, analyze, question and record everything that can enhance the creativity and innovation skills. Coding will increase the curiosity, along with logical analytical thinking. This will push the students to stand forefront and will help the country to develop in terms of technology.<sup>33</sup>

Although the NEP 2020 has a great benefit in future and help to provide a high level of security in cyber space but at the same time it is completely on the government execution because framing policy won't help. This policy requires proper funding and training for the teachers and students to understand this paradigm shift

## **CONCLUSION**

Cyber crime is a major threat for the whole world including India. As India is the second largest country having highest data consumption requirement. Due to rapid development in the cyber

---

<sup>31</sup>Latika Duhan, *Emerging courses: Digital India's growing need for cyber security experts and how to be one*, 22 May, 2020

<sup>32</sup> India Today Web Desk, *5 free cyber security courses to pursue during lockdown*, 7 May, 2020.

<sup>33</sup> Anurag Gupta and Rajeev Tiwari, *New Education Policy 2020: Integration of coding and analytical thinking from the school level*, Hindustan Times, 13 August, 2020.

space, the cyber vulnerabilities have become a serious matter. The government has introduced many laws and policies for strengthening the cyber security in India. Many amendments were also made but in spite of having so much protective measures the cyber crimes are increasing especially during lockdown. There are many cases which came up related to fraud, stalking, hacking, Child pornography etc. It has hampered the safety and security terms of the citizen`s especially the women. This shows that we are still lacking behind in terms of cyber security.

### **SUGGESTION**

Cyber crime has become a menace for the society and nation`s safety and security. It is important for the person to maintain some security while using internet. They should think before installing or responding to e-mail or giving any confidential data. It is essential for the women to think before accepting friend request, giving personal information or sending picture to another person. Every person should keep on changing their passwords and think before installing any application. Never open the bank page in the phone because if the phone is already compromised, then it would be easier for the hacker to steal the financial transactions along with OTP. It is important for the humans to understand the sensitivity of the internet along with this the police should also take some effective steps against criminals. Moreover, it is important for the government to keep a check over cyber criminals and make stringent laws against them. The government should also take the initiative to create more stringent laws and ensure awareness in the public regard cyber law and types of cyber crimes. Apart from awareness programme there is an urgent need to establish cyber related courses in the institutions as India requires more minds to tackle such problems and also help in boosting the nation`s security. Although the government has recently announced NEP 2020 that covers coding from class 6 onwards in the schools. But again, the question comes on its execution then only it will be impactful and will lead to growth in technology. Otherwise simply framing won`t work for that there should be proper funding is required in education area along with training. It is required from the female to come out of patriarchal thinking and report against cyber stalking by take the help from National Commission of Women.

### **REFERENCE**

<https://www.thehindu.com/news/national/Amended-IT-Act-to-prevent-cyber-crime-comes-into-effect/article16888817.ece>

<https://www.hindustantimes.com/mumbai-news/cyber-police-issues-advisory-on-cyber-crimes-amid-lockdown/story-0tDnAdHq4u5w7fAcDsUz0O.html>

<https://m.economictimes.com/tech/ites/only-cyber-security-jobs-at-it-firms-are-covid-19-virus-proof/articleshow/75707342.cms>

<https://www.thehindu.com/sci-tech/technology/december-2019-tips-from-india-cybercrime-experts-on-security-social-media-phishing-privacy/article30379212.ece>

<https://www.toppr.com/guides/business-laws-cs/cyber-laws/cyber-appellate-tribunal/>

<https://indianexpress.com/article/cities/pune/in-maharashtra-400-cyber-crime-cases-filed-on-covid-issues-most-on-hate-speech-communal-accusations-6419881/>

<https://www.hindustantimes.com/cities/37-cybercrime-cases-registered-in-pune-region-during-lockdown-period/story-3aw80FX4bUSOBSKzrGsn7M.html>

<https://www.thehindu.com/news/national/andhra-pradesh/state-firm-on-ending-cybercrime-against-women-says-sucharita/article30040624.ece>

<https://m.economictimes.com/tech/internet/sc-seeks-centres-reply-on-plea-for-ban-on-zoom-app-until-appropriate-legislation-is-put-in-place/articleshow/75891148.cms>

<https://www.thehindu.com/news/cities/mumbai/sexual-harassment-what-the-police-want-you-to-know/article17763619.ece>

<https://www.hindustantimes.com/delhi-news/no-conviction-in-150-sexual-harassment-complaints-against-delhi-police-staff/story-fA1Az18vxegU9KI72TIGgI.html>

<https://indianexpress.com/article/cities/mumbai/mumbai-senior-official-of-top-media-house-booked-on-charges-of-sexual-harassment-6575611/>

<https://www.thehindu.com/opinion/Readers-Editor/cyberbullying-must-stop/article32254166.ece>

<https://lexlife.in/2020/05/21/law-regarding-cyber-bullying-in-india/>

<https://www.hindustantimes.com/more-lifestyle/coronavirus-pandemic-as-work-has-moved-home-so-has-bullying-harassment/story-5Z0HCEVwLWuIvAWyighAIM.html>

<https://www.newindianexpress.com/nation/2020/jun/01/covid-19-lockdown-working-women-complain-of-online-sexual-harassment-say-experts-2150824.html>

<https://www.newindianexpress.com/cities/kochi/2020/jun/05/odd-hours-cyber-stalking-teachers-struggle-to-cope-with-online-classes-2152384.html>

<https://www.thequint.com/voices/opinion/the-dark-world-of-cyberstalking-and-how-the-law-cant-protect-us>

<https://www.hindustantimes.com/mumbai-news/tops-in-cases-of-cyber-stalking-atm-related-and-online-frauds/story-86vRas325NWRcADmCZILuJ.html>

<https://timesofindia.indiatimes.com/city/hyderabad/victims-of-cyber-stalking-mostly-minors/articleshow/64823238.cms>

<https://timesofindia.indiatimes.com/city/coimbatore/plan-to-revive-panel-on-sexual-harassment/articleshow/74233367.cms>



• LEGAL FOXES •

"OUR MISSION YOUR SUCCESS"