

# LEGALFOXES LAW TIMES

## MODERN APPROACH TO CYBER-CRIME LAWS – ENIGMA OR CONUNDRUM

By Nitish Kumar Naveen

### INTRODUCTION

In present times technology has a pivotal role in society. It has for the well being of humans but now it is a bane for humans. It has used for the erroneous purpose either for the personal benefits or for other's benefit which emerges of new time crime i.e. Cybercrime. It is a computer-oriented crime committed using computers or computer networks which takes place over cyber space especially the internet. These include various illegal activities. The term cybercrime is a structure for the classification of multiple criminal acts. Any jurists may describe the above article as cyber-crime victimization. In the execution of a crime, the machine could have been used or it may be the target. "Crimes that arise against individuals or gather people through criminal thought processes to intentionally destroy the victim's reputation or inflict physical or emotional injury or misfortune to the unfortunate person, either directly or roundabout through today's electronic networking networks, for instance, the Internet (networks like but not limited to Chat)".<sup>1</sup>

Clearly stated, the offenses or crimes committed by electronic communications or information systems are defined as "Cyber-crime." These offenses are criminal acts involving a machine and a network. The number of cyber-crime crimes is now that due to the growth of the internet as the physical appearance of the perpetrator is no longer needed when committing a crime. It cannot be described as a single definition. The exceptional characteristic of cyber-crime is the fact that the victim and the perpetrator will never be reached directly. To avoid surveillance and conviction risks, cyber-criminals often opt to work in countries where non-existent or ineffective cybercrime regulations apply. Among the population, there is a belief that cyber-crimes can be

---

<sup>1</sup> Decided by ADD. CMM, Egmore, Chennai on 5/11/2004

committed either over the Internet or cyberspace. Nonetheless, cybercrimes that be conducted without intervention in the cyberspace, the cybercriminal does not stay online.

A modern space called "cyberspace<sup>2</sup>" has been developed with the advent of computer systems and digital telecommunications. The Internet has been the platform for a variety of web-based human exercises. The Internet has, it is real, become today's most eventful spot. Web-based communications, commerce, marketing, banking, and analysis are being increasingly used. There is no human chaos that the internet does not reach. At present, you only have to open a laptop and press on just a button-down, anything can be done on a web-service or online. The intruder harms the individual's rights by using a cyber tool, which is far away from the victim and also uses a benefit of alibi. So, it is stated that "Cyber pen is more harmful than the sword in ancient time".

### Cyber Crime

This abovementioned word was used by Sussman and Heuston since 1995. It has not defined under any acts or by judgments nevertheless it is a combination of acts which has done on the computer or any technology which causes to be wrong done. Although, it has to be stated that those sort of crime in which computer or any electronic medium which is subject of constituting the crime or it may be an amalgamation of both.<sup>3</sup> One of the uncommon things of cybercrime is that the offender who committed the crime has never direct contact with the victim. To take benefit these offender has mostly belonged to wherever those countries which had not stringent cybercrime laws to have fewer chances of detection and prosecution.

In the advent of technology, there are many advantages and disadvantages nevertheless it made ease for the people to connect whomsoever has resided at the distant places. Often viruses are embedded in ostensibly legitimate emails and web advertisements, which attack a device after

---

<sup>2</sup> The word "Cyber Space" was coined by "William Gibson," the Canadian/American science fiction writer who helped define its cyberpunk sub-genre, in 1982 in his novelette "Burning Chrome" in Omni magazine, and in his novel "Neuromancer".

<sup>3</sup> Vishwanath Paranjape, Legal dimension of cyber crimes and preventive laws, Pg no.7, Central Agency, Allahabad, edn, 1<sup>st</sup>, 2010

they have been opened, and then the user can not access their computers. Nevertheless, the approach to encourage open data and communicate over long distances often leads to a worryingly high level of unstable behaviour. The insecurity and health of women are one of the main issues in any criminal and penal legislation, but ladies still have little defense on the Internet. Cybercrime towards women is at an alarming level and may serve as a danger to the health of the victim. Data can be viewed as text, images, graphics, and sound on the World Wide Web. Many accounts of women getting unwelcome emails in recent years have also been pornographic and gross. And the biggest issue is that women will not disclose these issues in general.<sup>4</sup>

The motive behind these offenses is different from any other type of crime. It is not possible to detect the offender, nevertheless who is an employee of the company. The offender had so smart that he had knowledge and understanding about loopholes to commit the offense without leaving any things for busted. In most of cases, cyber offence committed on the women who had to socialize on social networking site, nevertheless, offender is close to someone of the victim, which took for their motive of personal gain, revenge, etc.

### **CATEGORIES OF CYBERCRIME**

The classification of cybercrime is into two heads; Physical and Non-physical cyber crimes. There are certain categories of cybercrime that had embedded in their classification, which has discussed prior to us.<sup>5</sup> Most cybercrimes are not physical since there is no direct contact with communication. Some of the non-physical cyber crimes include cyber invasion, cyber theft, and cyber fraud in which physical contact is not required. However, the subject matter would be different depending on the victims when we speak about the definition of cybercrime, which is simply not depending on the physical essences for instance

---

<sup>4</sup>ShobnaJeet, Cyber Crime Against Women in India: Information Technology Act 2000(12<sup>th</sup> June 2012), Elixir International Journal, [http://www.elixirpublishers.com/articles/1351168842\\_47%20\(2012\)%208891-8895.pdf](http://www.elixirpublishers.com/articles/1351168842_47%20(2012)%208891-8895.pdf) (last accessed on 15<sup>th</sup> April 2020)

<sup>5</sup>DhaweshPahuja, "Cyber Crimes and the Law"(17<sup>th</sup> July 2011), Legal India, <https://www.legalindia.com/cyber-crimes-and-the-law/> (last accessed on 15<sup>th</sup> April, 2020)

1. Cybercrime against individual/person
2. Cybercrime against women
3. Cybercrime against the government by act of terror by harming national integrity of the country
4. Cybercrime against societies at large such as gambling, pornography, trafficking, and cyber financial crisis.

### **Cyber bullying**

To feel lower to the victim in social media like Twitter, Orkut and Facebook cyberbullying can be named a mechanism performed by the wrongdoer of cyber malpractices. There are young people, young children of school age who also pursue cyberbullying as we think about the victims.

The word bullying can be explained as “when a person proceeds when people take appropriate actions against women or other victims to manage them”. Threats may be made and other victims identified. The use of cell phones, e-mails, speech rooms, or informal interactions locally in a wide range is digital bullying, for instance, Facebook and Twitter in a bug, danger, or undermining guy.

Cyberbullying can occur in many different ways at any time of the day, not only at school hours. Like other forms of bullying, cyberbullying can lead to<sup>6</sup> depression, a loss of desire to attend school, issues with self-esteem and can even lead to drug addiction or suicide in serious circumstances.

Due to advancements for easy access to things, digital bullying is being done by kids. In the current scenario these problems have occurred with today's generation due to digitalisation which was not earlier but has been today. This secret aspect makes it impossible to locate the origins and allows the bullies to behave more belligerently than they might in a situation where they have been identified.

---

<sup>6</sup> Dr. Savita Srivastava, Pessimistic Side of Information & Communication Technology: Cyber Bullying & Legislature Laws, International Journal of Advances in Computer Science and Technology 1 (1), November-December 2012, 14-20

## Cyber Stalking

The emotions of women get affected by any person who is sitting in his/her room can be by means of technology. Cyberstalking entails monitoring a person's activities around the Internet by uploading notes (sometimes threatening) to the victim's frequented bulletin boards, accessing the victim's frequented chat rooms, continuously bombarding the victim with letters, etc. For certain instances, we can see that cyberstalking can emerge from actual terms, such as their personal life. Stalking is a matter which is currently known to many people, especially women. So at the stage when the problem arises through the web vehicle is called "Digital Stalking or "Online Harassment". Digital stalking reflects the person concerned with his annoyance, guilt and humiliation. Cyberstalking can destroy the individual personal life by affecting their emotions which is harmed online. Hate, rage, vengeance, envy, obsession and mental illness are the reasons behind cyberstalkers. In 2003, Delhi registered the first case of cybercrime in India. A lady reported in the police station that for several weeks, someone uses her name to harass for such illegality on social media sites. Using her fake name, he was texting to everyone and sending her pictures, addresses and mobile telephone numbers to her friend. Consequently, after getting 70 calls a day from a stranger average day, she becomes mentally disturbed. These calls caused problems in her personal life and thereafter she reported the issue. Eventually, the IP addresses were traced and the accused was arrested based on the complaint by the police. The above-mentioned case was booked under section 509 of the Indian Penal Code (IPC).<sup>7</sup>

Through the technology cyber-stalking has a direct attack on the victim rather than indirectly. In all cases, the law needs a reasonable danger to the unfortunate victims of law in some jurisdictions. "Digital stalking is defined as using the Internet or email, or specific communication methods to harass or threaten another person<sup>8</sup> as other researchers represented digital media explicitly simply by the disconnected criminality of stalking". Not generally

---

<sup>7</sup>Vishwanath Paranjape, Legal dimensions of cyber crime and preventive laws, Pg no.33, Central Law Agency, Allahabad, edn., 1st, 2010

<sup>8</sup> Naomi Harlin Goodno, Cyber Stalking a New Crime: Evaluating the Current State and Federal Laws, 72 MO. SREV. 125, 126 (2007); see also Shonah Richard Shafritiz, A survey of Cyber stalking Legislation, 32 UWLA

described otherwise as actions of participation or recurrent sexual harassment. The stalker's main purpose is to get a more threatening online fear of the victim than the physical terms.

### **Cyber harassment**

In reality cyber harassment in the real world, digital badgering should be limited to concentrating on people, for example, race or sexual orientation, through uprightness in their registered assured class. On the internet, as in the non-online world, the refinements between tormenting and badgering will usually haze directly that has been represented as digital bullying involves mobbing activity that has gone for hushing ladies and ethnic minorities, which seems to go too far between bullying and badgering. If there is an organized secure class, mobbing is characteristic of tormenting, and the point of driving marginalized gatherings disconnected tends to be more powerful than ownership — normal qualities of tormenting rather than badgering. In the light of the discrepancies between the tormenting and the bullying and the refinements between them, it might be necessary, in any case in the good 'old days' electronic guidance, to fix the physical harm all over and to emphasize the credentials afterward. There may indeed be new refinements among classes that are more suitable in advanced age than in established qualifications. Controllers can, for example, select from an individual and general exchange correspondence specifically arranged around a single person that the previous lead would be even quicker to compromise or unnerve the individual in question. Direct correspondences involve risks and may be harder to regulate by legislation than general virtual interchanges.

### **CYBER VICTIMIZATION**

Technological innovations provide perpetrators with different methodologies, but they don't produce new crimes. The clear distinguishing factor between new and conventional crimes is the use of digital technologies. Nevertheless, technology alone cannot adequately differentiate between the worlds of criminal activity. The fact that a criminal needs no technical tool to do what he is doing best, crime is extraordinary in this regard. Crimes such as, inter alia, fraud, child pornography and IP conflicts before the 'cyber' prefix is connected to it. Internet cyber-crime

inclusion is essentially an extension of conventional crimes that have occurred in the illicit criminal area of existence.

Cyber-crime is commonly an assault on the data of the persons, including but not limited to corporations, governments, organizations and individuals. While these attacks do not impact the individual's physical body, they disturb the life of the individual. Therefore, the significance of a person's virtual identity in this day and age is paramount, but they also reduce them to the government's digital data records. Cybercrime, among other items, stresses the fragile existence of such centralized records, which contain closely related identity information.

The main goal of cybercrime is to remove the above anomalies as they are listed therein, raising significant domestic, national or even international issues, international treaties must be drawn up, ratified and/or incorporated into the essential domain of the legal structures of the nations, to curb the disaster, at UN level, in the light of the imminent cyber breach.

Types of Child Victimization in cyberspace:

The key features of child victimization in cyberspace below are included: high 'Dark Number Victimization' of many people by crime; easy child victimization by virtual environments.<sup>9</sup>

### **SEXUAL TOURISM THROUGH THE INTERNET CHILDREN:**

Sexual tourism, including child trafficking, is another form of torturing the victims, in major cities around the world and especially in India for the child. The phraseology 'sex Tourism' means sexual abuse by tourists<sup>10</sup>, as they defy both the human rights and the inherent inalienable rights of the victim, which are only enabled by social media and virtual spaces.

Mostly industrially rich countries have been increasing the sexual abuses of children whose age of 10 years old with the passage of time according to UNICEF records, and also facilitate sex trafficking at a whole different level.<sup>11</sup> Not only child abuse is accessible in an efficient manner

---

<sup>9</sup>Bastani, 1383,p.124

<sup>10</sup>Abachi, 1380, p. 89

<sup>11</sup>Beigi, 2005, p. 252

on the internet for availing sex tourism, but also there is online sharing of such illegal and uncanny content.<sup>12</sup>

### **Child pornography**

Pornography means literally: any text, sound or image containing sexual items that do not have any moral, artistic, political or scientific value at all.<sup>13</sup> According to Section C of Article 1 "Optional Protocol of the Children's Rights Convention on children's sale, prostitution and pornography adopted in 2000," imply any kind of display by children engaged in real or artificial sex, or any representation of children's sexual organ for primarily sexual purposes, through texts and pornographic images of children.<sup>14</sup> It should also be noted that child abuse of this nature has to be aimed towards sexual activity. The picture of the child during bathing is not called child pornography subjects, but laws contain only (Obscene) documentation of the sexual organs of an infant during sexual activity.<sup>15</sup>

Any visual demonstration showing a child or individual as an object or as a subject in sexual activity, that appears to be a child irrespective of the conditions in which female sex or baby's anus for sexual pleasure are demonstrated. Any audio presentation represents, provides, motivates or consults unlawful sexual interaction with children, irrespective of the manner or nature of the device suggesting criminal behavior, without prejudice against performance, such as the showing of computer graphics cases or the use of mechanical or electronic devices.<sup>16</sup>

### **Cybercrime against women in India**

A lady in India regularly assures that they are a victim of digital infringement, and the online stage is currently a new stage in which dignity, security and safety are being challenged continuously every minute. Digital worlds are common in Trolling, bullying, cheating, stalking,

---

<sup>12</sup>Beigi, 1384, p. 254

<sup>13</sup>Bastani, 2007, p. 50

<sup>14</sup>Beigi, 2005, p. 237

<sup>15</sup>Rahimimoghadam, 2009, p. 23

<sup>16</sup>Daziani, 1385, p.56



voyeurism, body shame, stigmatizing, advertising, malicious pornography. The objects of laws have given assurance for ladies' security which is more on physical than mental mischief if there is a digital violation is committed against ladies. The details confer that the National Crime Records Bureau (NCRB) has no digital infringement records for women. Technology means that some criminals are used to insult women by sending obscene Whatsapp messages, emails, and harassing ladies by making explicit recordings, which are usually without their permission, saturating texts, transforming photos to obscenities by using various virtual products that are available on the web. Indian women aren't prepared to report digital criminal actions promptly, whether they're not aware of where to report these violations or because of social embarrassment they want to stop disclosing what they do. Their mentality must broaden, and they must become the whip to restrain these culprits nearby so that they feel free to object promptly.<sup>17</sup>

### 1. Cyber pornography

Today a woman is still under the fear of cyber pornography. Cyber porn is a crime in India that spreads rapidly throughout the world. When an inquiry is performed approximately 40% online, obscene content is used. Porn videos can easily be viewed online or offline via hard disk and DVD. Digital technology is not just an extension of documents, pictures and clips to be considered.<sup>18</sup>

The most recent example is of Delhi Metro CCTV video leakage case<sup>19</sup>, the video has been leaked on the Internet recorded by police security cameras where the couple was intimated in metro stations etc. The special case of Cyber Pornography protected in some way by Section 67 of the IT Law 2000 was dealt with under the IT Act 2000. In compliance with the IT Act, the offender can be prosecuted under different provisions of the IPC (Section 290 for causing public disruption, Section 292 for selling pornographic

---

<sup>17</sup>Dhruti M Kapadia, "Cyber Crimes Against women and laws in India", Live Law(21<sup>st</sup> Nov,2018,11:36AM),<https://www.livelaw.in/cyber-crimes-against-women-and-laws-in-india>(last accessed on 15<sup>th</sup> April, 2020)

<sup>18</sup> Agrawal Nidhi and Dr.kaushikNemaj, cyber crimes women retrieved from [www.publishingindia.com/Getbroucher.aspx?quer y...](http://www.publishingindia.com/Getbroucher.aspx?quer y...)(last accessed on April 15, 2020)

<sup>19</sup>"Porn MMs from Delhi Metro CCTV Footage", Zee News(10<sup>th</sup> July 2013,00:17AM),[http://zeenews.india.com/news/nation/porn-mmses-from-delhi-metro-cctv-footage\\_860933.html](http://zeenews.india.com/news/nation/porn-mmses-from-delhi-metro-cctv-footage_860933.html)(last accessed on 15<sup>th</sup> April,2020)

books, etc., and Section 292A for printing or publishing grossly lewd or scurrilous content or information intended for extortion, Section 293 for selling pornographic items to young people, and Section 294 for producing or reading, recording, etc.

## 2. **Cyber Morphing**

Morphing edits the original image so that it looks entirely or substantially different. Many immoral elements in the virtual environment steal photos of girls from places like Facebook and then create another one in a risky position to prove that women are involved in these practices. The next move after this is always to intimidate certain people by threatening to release distorted photographs and undermine certain woman's status in society.

A 19-year-old girl from Haryana's Fatehabad town has been in severe distress when she posted images on social networking site facebook after a youth whom the name is Gautam Kumar belongs from Sirsa downloaded one of her photographs and morphed it. Consequently, she was abducted by GautamKumar and his friends Sonu and Raju. The case was booked under various sections of IPC after filing a complaint against him.

The latest case which was recorded in India is Air Force Balbharati School case (Delhi)<sup>20</sup> A student of the school was teased by all his classmates to have a pocket facial by himself in this group. He who is sick of the mean jokes wanted to come back to his persecutors and scan the images of his classmates and teachers and places them on the website of a free hosting company. The father of one of the girls on the platform identifies about this and filed a report with the police.

## 3. **Cyber defamation**

It is not entirely different from Sec 499 of IPC. Defamation is called non-physical damage in terms of which another person's reputation is affected. Cyber defamation is carried out by publishing the third person false information on the internet. Defamation has done through libel or slander. Cyber defamation may not only be committed by women, but the crime rate is more applicable to women.

---

<sup>20</sup>AbhimanyuBehera, "Cyber Crimes and Law In India," XXXI,IJCC 19 (2010)

There was a case that was recorded 1<sup>st</sup> time in India is SMC Pneumatics (India) Pvt. Ltd. v. JogeshKwatra-JogeshKwatra-There was an employee who sent defamatory and obscene emails related to Managing Director. The e-mails were anonymous and sent to several of their corporate partners to tarnish the plaintiff company's reputation and goodwill. With the help of a private computer expert, the complainant was able to locate the defendant and brought the High Court in Delhi. The Court issued a restraining injunction and prohibited the employee from e-mailing, publication and transmission of defamatory or derogatory messages to the claimants.

The above-mentioned actions against women demonstrate that a serious threat to our women in the country has arisen from the boom in technology.

### **JUDICIAL CASES OF CYBER CRIME AGAINST WOMEN**

#### **RituKohli Case<sup>21</sup>**

This is the leading case of cyber-stalking and the reason for the amendment of IT-Act. The culprit Manish who was used name, mobile no and photographs of the victim and made a profile on social networking site and started the chat by her name. Before it police have not deal with this type of matter which has lodged by any person in the society, henceforth they have to be vigilant and unique in their investigation process. The intent to act by Manish had mentally disturbed the victim, due to she got night call by the third person and asking for a spend night with them. Consequently, she went to the police station to register an FIR. As a result, over the next three straight days, she started receiving nearly 40 lewd phone calls at odd hours of the night. This required her to write to the police in Delhi. As soon as the complaint was lodged the FIR at the police station, the team of investigators began gathering evidence to identify the Manish after successfully traced IP address and arrested Kathuria under the IPC provisions but mainly because of there is no existence of legislation i.e. IT Act 2000 on that time when the case was lodged. It was when the law was introduced to prevent cyberstalking in India and then Section 66-A was amended by a parliament. That has been the case. Then the case is registered, and the IP address and arrest of MR. Kathuria is traced by Delhi police in compliance with Section 509 of the Indian Penal Code, under the proper investigation. The main thing was that the IT Act was not

---

<sup>21</sup>RituKohli v. Manish Kathuria, 9 RMLNLUJ (2017) 175

included when the case was registered because no changes were made. Therefore, it is obvious from this case that legislators have to be wake up and think of statutory provisions to deal with such a matter in any ongoing proceedings. Afterwards the 66-A was adopted in 2008. As a result, cases under this section are still registered as opposed to Section 509 of the Indian Penal Code, as was the case in Goa when a university student was harassing a woman under the above clause by establishing a false profile on social network and posting an image on it and proclaimed her to be his wife. Initially, email harassment, cyber-stalking is governed through prevailing cyber laws in India. The offender may be charged remotely for infringement of confidentiality and privacy only under sec 72 of the IT Act. The perpetrator can also be convicted of a criminal offense under section 441 of the IPC and section 509 of the IPC of outrage of female modesty. Therefore the victim has hoped to favour the decision.<sup>22</sup>

### **VinuPriya Case<sup>23</sup>**

This case is based on cybercrime against women who completed her graduation at the age of 21 yrs. She was upset when she told her parents that On June 23, her image suddenly appeared on the internet for the first time. The police officers' failure or inattention to apprehend the perpetrator using morphological images was deceitful. The victim's dad was told to jail him for up to 2 weeks, which was surprising to his family. The cyber-crime cell of Tamil Nada doesn't understand the agony that the family of the victim is experiencing during these days. Cyber-crime officials demanded bribe taken as mobile phone whose cost is Rs 2000. Afterwards the case has not solved by cybercrime cells on June 26, consequently, another obscene pictures were posted on facebook by the perpetrator. Police officials are not carrying out their duties properly and thought that somebody is given pictures by the girl and are now released. This investigative act by officers telling Vinupriya those photographs had been sent by her to a boyfriend in the

---

<sup>22</sup>[Aravinthbalakrishnan](http://www.legalserviceindia.com/legal/article-214-cyber-stalking-challenges-in-regulating-cyberstalking-at-the-cyber-space.html), "Cyber Stalking: Challenges In Regulating Cyber stalking At The Cyber Space", Legal Service India, <http://www.legalserviceindia.com/legal/article-214-cyber-stalking-challenges-in-regulating-cyberstalking-at-the-cyber-space.html> (last accessed on 7<sup>th</sup> April 2018)

<sup>23</sup>Palanisamy v. State of Tamil Nadu, HC No. 1956/2016

past and is now being downloaded by him. She killed herself<sup>24</sup> while she was alone in her home on 27th June, because police were unable to find true fault.

### **Karan Girotra v.State<sup>25</sup>**

The filling of an application under section 498 for anticipatory is the only resort on cybercrime to attain justice by the court. In this case the lady whose name was ShivaniSaxena had filed the petition of divorce for annulment of marriage. Accidentally, a guy had met on the internet with her and had a long time chatting with him, and he told her that he wanted to marry her. The guy said to her that he wants you to meet his dad, so you come to dinner and she's happy to take part in the meal. Finally, the man sexually harassed her at dinner and took her lewd pictures and menaced her that the photos would be published on the internet if she did not allow her to marry.And the ceremony was carried out by two of them. Today, girls have no choice but to complain to a guy about such an immoral act under the IT Act 2000. The boy was subsequently arrested under the IT Act, which involved a serious custodial investigation, and he submitted the appeal that was dismissed by the courts because of an indecent image of a girl circulated and released on social media. This case has been affected by a delay in FIR filling.<sup>26</sup>

Provision under IT Act 2000 dealings with Cyber Crime:

1. **Section 67:**It deals specifically with obscene or offensive content on any electronic device is anoffence.
2. **Section 66A:**Punishment for the transmission of offensive messages through electronic Device to person

---

<sup>24</sup> The Hindu newspaper, Madras Edition, dated on 01-07-2016

<sup>25</sup> Karan Girotra v. State, VAD (Delhi) 483

<sup>26</sup>Legal Crystal,<https://www.legalcrystal.com/cases/search/name:information-technology-act-section-66/page:2>(last accessed on 15<sup>th</sup> April 2020)

3. **Section 66B:** It deals specifically with the person who dishonestly stole any data from a computer or electronic device with punishment up to three years or one lakh rupees as fine or both.
4. **Section 66C:** It deals specifically that person use of identity or electronic signature of another person through fraud and dishonest have punishment up to three years and also liable to fine up to one lakh rupees.
5. **Section 66D:** Punishment for cheating through computer resources or electronic devices by impersonation.
6. **Section 66E:** It deals specifically for violation of privacy done by person without consent to have punishment up to three years or fine up to two lakh rupees or both.
7. **Section 66F:** It deals specifically with to endanger India's unity, dignity, protection or sovereignty or to terrorize the citizens or some part of the population.
8. **Section 75:** Jurisdiction related to cybercrime in India.
  - 1.) In pursuit of the provisions of sub-section (2),the provisions of this Act shall also extend to any crime or contravention of anyone, regardless of his / her nationality, committed outside India.
  - 2.) For sub-section (1),The Act refers to an offence or contravention committed by any individual outside India where the violation or conduct involves a computer<sup>27</sup>, computer-system<sup>28</sup> computer network<sup>29</sup>.

LEGAL FOXES

"OUR MISSION YOUR SUCCESS"

---

<sup>27</sup> 'computer' means any electronic, magnetic, optical or other high-speed data processing device or system which performs logical, arithmetic and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software or communication facilities which are connected or related to the computer in a computer

<sup>28</sup> computer network' means the interconnection of one or more computers through - (i) the use of satellite, microwave, terrestrial line or other communication media; and (ii) terminals or a complex consisting of two or more files.

<sup>29</sup> 'computer system' means a device or collection of devices, including input or output support devices and excluding calculators which are not programmable and capable of being used in conjunction with external

## **WAY FORWARD**

In the light of the foregoing proposal set out in this paper, the above-mentioned chapters may be concluded as set out below. It would be extremely fascinating to believe that cybercrime can be combated and ended without significantly altering the country's IT legislation. Therefore, with a view, among other things, to new, diverse and up-to-date cyber mishappenings, the author would like to suggest that the IT Act, 2000, be interpreted by all judicial authorities taking into consideration of new, varied and updated cyber mishappenings without proper implementation take place.

The Case like that of the Ritu Kohli (supra)<sup>30</sup> has also shown a significant yet alarming light on the deficiencies of the existing cybercrime legal framework when adjudicating an issue that has turned out to be an initial one in India. It is a big concern. However, it should not be wrong to accept the criticisms of the above-mentioned flaws in the Indian demographic situation, including, but not limited to rational analysis, appreciating Indian technological developments and the IT jurisprudence that has been established, primarily from the Indian scenarios. The author assumes that the government, in addition to recognizing possible situational adjustments in its approach, is cautious in introducing more mature legislation, which appreciates the current situation. It's just a time test about what's happening and how.

---

<sup>30</sup>Supra Note 28

## **Bibliography**

### **LEGISLATIONS REFERRED:**

- Information Technology Act, 2000
- Constitution of India

### **CASE LAWS REFERRED:**

- Karan Girotra v. State, VAD (Delhi) 483
- Palanisamy v. State of Tamil Nadu, HC No. 1956/2016
- RituKohli v. Manish Kathuria, 9 RMLNLUJ (2017) 175

### **WEB SOURCES REFERRED:**

- <https://www.legalcrystal.com/cases/search/name:information-technology-act-section-66/page:2>
- <http://www.legalserviceindia.com/legal/article-214-cyber-stalking-challenges-in-regulating-cyberstalking-at-the-cyber-space.html>
- <http://imrfjournals.in/pdf/MATHS/SSIRJ-VOLUME-2-ISSUE-1-2016/91.pdf>
- [http://www.elixirpublishers.com/articles/1351168842\\_47%20\(2012\)%208891-8895.pdf](http://www.elixirpublishers.com/articles/1351168842_47%20(2012)%208891-8895.pdf)
- <https://www.legalindia.com/cyber-crimes-and-the-law/>
- <https://www.livelaw.in/cyber-crimes-against-women-and-laws-in-india/>

### **OTHER SOURCES REFERRED:**

- The Hindu newspaper, Madras Edition
- Agarwal Nidhi and Dr. KaushikNemaj, cyber crimes against women
- Daziani, 1385
- Rahimimoghadam, 2009
- Beigi, 2005



- Bastani, 2007
- Beigi, 1384
- Abachi, 1380
- Bastani, 1383
- VishwanathParanjape, Legal dimensions of cybercrimes and preventive laws, Pg no.7, Central law Agency, Allahabad, edn.,1st ,2010
- Citron, Cyber Civil Rights, at 4 (discussing "the growth of anonymous online mobs that attack women, people of color, religious minorities, gay and lesbians"
- See Bullying: What Is It?, (describing "gang" or "group" bullying, known as "mobbing")
- Presentation, Erica Merritt, Workplace Bullying (Case Western Reserve Univ., 18, 2010)
- Naomi HarlinGoodno, Cyber stalking, a New Crime: Evaluating the Current State and Federal Laws, 72 Mo. REV.125, 126 (2007)
- Shonah Richard Shafritz, A Survey of Cyber stalking Legislation, 32 UCLA



• LEGAL FOXES •

"OUR MISSION YOUR SUCCESS"