

ISSN: 2582 - 2942



# LEX FORTI

---

LEGAL JOURNAL

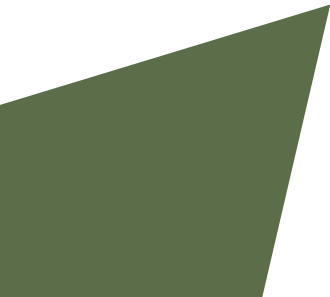
VOL- I ISSUE- V

JUNE 2020

# DISCLAIMER

---

NO PART OF THIS PUBLICATION MAY BE REPRODUCED OR COPIED IN ANY FORM BY ANY MEANS WITHOUT PRIOR WRITTEN PERMISSION OF EDITOR-IN-CHIEF OF LEXFORTI LEGAL JOURNAL. THE EDITORIAL TEAM OF LEXFORTI LEGAL JOURNAL HOLDS THE COPYRIGHT TO ALL ARTICLES CONTRIBUTED TO THIS PUBLICATION. THE VIEWS EXPRESSED IN THIS PUBLICATION ARE PURELY PERSONAL OPINIONS OF THE AUTHORS AND DO NOT REFLECT THE VIEWS OF THE EDITORIAL TEAM OF LEXFORTI. THOUGH ALL EFFORTS ARE MADE TO ENSURE THE ACCURACY AND CORRECTNESS OF THE INFORMATION PUBLISHED, LEXFORTI SHALL NOT BE RESPONSIBLE FOR ANY ERRORS CAUSED DUE TO OVERSIGHT OTHERWISE.



ISSN: 2582 - 2942

# EDITORIAL BOARD

---

EDITOR IN CHIEF

ROHIT PRADHAN

ADVOCATE PRIME DISPUTE

PHONE - +91-8757182705

EMAIL - LEX.FORTII@GMAIL.COM

EDITOR IN CHIEF

MS.SRIDHRUTI CHITRAPU

MEMBER || CHARTED INSTITUTE  
OF ARBITRATORS

PHONE - +91-8500832102

EDITOR

NAGESHWAR RAO

PROFESSOR (BANKING LAW) EXP. 8+ YEARS; 11+ YEARS WORK EXP. AT ICFAI; 28+ YEARS WORK EXPERIENCE IN BANKING SECTOR; CONTENT WRITER FOR BUSINESS TIMES AND ECONOMIC TIMES; EDITED 50+ BOOKS ON MANAGEMENT, ECONOMICS AND BANKING;



ISSN: 2582 - 2942

# EDITORIAL BOARD

---

## EDITOR

DR. RAJANIKANTH M

ASSISTANT PROFESSOR (SYMBIOSIS  
INTERNATIONAL UNIVERSITY) - MARKETING  
MANAGEMENT

## EDITOR

NILIMA PANDA

B.SC LLB., LLM (NLSIU) (SPECIALIZATION  
BUSINESS LAW)

## EDITOR

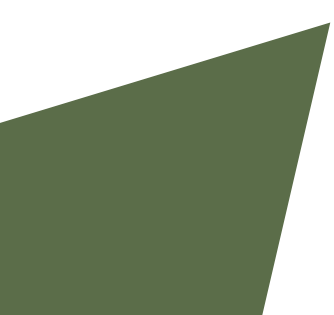
DR. PRIYANKA R. MOHOD

LLB., LLM (SPECIALIZATION CONSTITUTIONAL  
AND ADMINISTRATIVE LAW)., NET (TWICE) AND  
SET (MAH.)

## EDITOR

MS.NANDITA REDDY

ADVOCATE PRIME DISPUTE



# ABOUT US

---

LEXFORTI IS A FREE OPEN ACCESS PEER-REVIEWED JOURNAL, WHICH GIVES INSIGHT UPON BROAD AND DYNAMIC LEGAL ISSUES. THE VERY OBJECTIVE OF THE LEXFORTI IS TO PROVIDE OPEN AND FREE ACCESS TO KNOWLEDGE TO EVERYONE. LEXFORTI IS HIGHLY COMMITTED TO HELPING LAW STUDENTS TO GET THEIR RESEARCH ARTICLES PUBLISHED AND AN AVENUE TO THE ASPIRING STUDENTS, TEACHERS AND SCHOLARS TO MAKE A CONTRIBUTION IN THE LEGAL SPHERE. LEXFORTI REVOLVES AROUND THE FIRMAMENT OF LEGAL ISSUES; CONSISTING OF CORPORATE LAW, FAMILY LAW, CONTRACT LAW, TAXATION, ALTERNATIVE DISPUTE RESOLUTION, IP LAWS, CRIMINAL LAWS AND VARIOUS OTHER CIVIL ISSUES.

**Modern Crimes of Modern Age**

**Deepankar Chugh**

## INTRODUCTION

---

So, if we talk about crimes there are certain things we came across or things that came is theft or looting a bank, or robbery and certain other things as these things are not enough as in the modern age there is another thing that has been originating in the **21<sup>st</sup> century** is the growth of **cyber crimes because most of the times we only get to know about the crimes that are happening physically and we get to safe from those kind of crimes without taking care of crimes that are virtual in nature as these kind of crimes are more dangerous as it will lead to more harm to a person as physical crimes can be taken care but the crimes that are virtual in nature is hard to take care as for these sought of crimes because there are certain technicalities that are hard to catch or to take review of those kind of activities.** In **21<sup>st</sup>** century there are certain kind of criminals activities which are hard to get for police if we talk about Indian police as our country is at a developing stage so, for us right now it is quite difficult to get at that stage of development where we could easily catch the crime because due to lack of resources there are certain problems are there for are police system in India but it is not just like that there are certain developments as if we look at the coming of the cyber cells that are considered to be the development in the police system of the country as now days cyber cells are active for 24 hrs in the country. **As if we look at the 21<sup>st</sup> century there are certain things on the internet that are considered to illegal in nature the first thing that comes to ou mind is the use of Dark-net, illegal trafficking and much more as the internet we use as a public is around 5% but the original internet that are mostly used by the criminals or hackers is around 95% most of the criminals are mostly found on these type of networks there are certain cases where there has been hacked accounts which cause public lot of problem but now days if we look at these system after getting advanced with the day to day activities of the criminals the police are active 24x7 on these kind of network which create problem for these kind of criminals but still there are certain crimes which are hard to get because there are basically certain type of **hash system or the assymetric cypto system these two system are basically used for generating the evidence for digital signature that has been defined under Section 3(2) of the Information technology Act 2000,** as technology is getting so advanced there are certain cases related to forgery now if we look at **forgery** the first thing that came to our mind that how forgery has been conducted on digital matters as more use of computer has created problem towards public as it is good that the technological development is good for the society but there are many hindrances to that kind of development forgery is basically **conducted through copying those digital signature due to which the legality of that signature get hampered that has been defined clearly under section 5 of those electronic signature.** As the concept of **signature** is just an**

**example** how there has been development around the world due to which the crime has also been increasing with the change in time there has been change in the criminal activities for that one example has been taken above as the use of electronic record signature and its authentication will be discussed in the following document in proper manner. As in the age of technology the crime rate has been increasing so looking at those things the following paper will look at those modern crimes and their remedies in India as well as around the world.

## **CYBER CRIMES AND FORENSICS:**

---

### **CYBER CRIMES**

As with the increase in technology the aspect of cybercrimes has been increasing, basically there are certain types of crimes that are catch-able through police investigation but some might do not come even close through investigation and sometimes the IP (internet protocols) show different address due to which it gets difficult for the police to arrest the said criminal or the group of criminals. So, there are following types of crimes that have been generating in this cyber age:

1. Phishing
2. Misusing personal information
3. Hacking
4. Spreading hate and terrorism
5. Distribution of Child pornography
6. Grooming; making sexual advances to minors
7. Cyber stalking
8. Denial of service attacks
9. Software piracy
10. Virus attacks
11. Salami attacks
12. Sale of illegal articles
13. Online gambling
14. Email spoofing



15. Cyber defamation
16. Forgery
17. E-mail bombing
18. Data diddling
19. E-commerce investment fraud <sup>1</sup>

So these are cybercrimes that are certainly considered to popular in the world of cyber crimes and looking at the criminal activities the particular crimes will be defined in the popular manner which might create a sense of attention towards public that if they might come across such situation through certain definition they get to know about those crimes generally the countries are concern with the growing rate of cyber crime and they have adopted two basic strategies (1. to approach computer crime both as traditional crime by/on high tech computers,2. Crime that is unique in nature requiring new legal framework).<sup>2</sup> As there has been phenomenal growth of Internet has provided result in several types of computer crimes. As according to a survey it has shown that around 70% reported a variety of computer crimes through viruses that affect laptop or net abuse, basically the abuse of net has been there and been increasing with the change in time usually there has been more abuse of internet as it has been described above that more report of net abuse has been recorded with the growing of time. Responding several survey it has shown that there are several companies that cause great loss due to these kind of privacy hacking's or kind of Identity theft these activities has cause great amount of loss to these companies and might affect their goodwill in the market as it has been recorded that around 1 million dollars<sup>3</sup> that occur throughout computer leaked data. As another thing that affects is piracy as this industry has been earning with change in time basically the work of piracy is getting the original content and getting that thing in the market at low rate that will considered as the piracy usually the pirated content has been more in the market and consumers are forged to buy that kind of product as they lure the customers this kind of things has been growing at the E-commerce platform usually the platforms like Amazon, Snapdeal these are the two platforms that have been reported that there have been more use of the pirated products as the complaint has been recorded under Intellectual and information

---

<sup>1</sup><http://www.helpline.law.com/employment-criminal-and-labour/CCII/cyber-crimes-in-india-what-is-types-web-hijacking-cyber-stalking.html>

<sup>2</sup>In America 31 states have passed new legislation to deal with computer related crimes whereas others have amended the definition of larceny to include electronic media. Michael D. Rostorker et al. Computer Jurisprudence, also covered under IT Act 2000

<sup>3</sup>Peter H. Lewis "losses from computer breaches are on the rise of a study according to new York Times 1995"

technology act, basically it has been recorded **around 2.8 billion dollars per year income, as a cellular phone companies lost around 650 million dollars in the year 1996 as due to certain sought of change has been seen in the company's software**<sup>4</sup> basically this shows that how the technology has been growing at that period but this show's with the change in time there has been change in technology and crime rate has been increasing in cyber world whether we talk about dark net or dark web there as most of the product which we called as the 1<sup>st</sup> copy of different branded has been sell at that particular site and usually that sites can be visited through **Tor browser as most of the web traffic has been recorded there because the web we use is around 5-10% of the total internet as most of the internet is the use of the dark web.** As in the new generation of crimes has been summed and several other crimes has also been generated different crimes which have been discussed above as these crimes are not enough the crimes are emerging more and more with the change in time and technology both are major part in the growing of the cybercrimes around the world, as it is not only about the normal public but the major companies are getting affected through cybercrimes. Basically there are certain crimes that have been described above as if we looked at those names they certainly technical in terms as for a prudent person those names are technical and to provide knowledge through my paper it will be in certain manner will be helpful for the people to have a kind of knowledge regarding those terms as if they feel certain kind of disturbance or minor disturbance they will get to know that what has happened to their data and with that they can easily make complaint to the police station. So, some crimes will be explained as it to provide quite knowledge about the topic, following are these crimes:

## **PHISHING**

---

So the concept of phishing is basically getting one's information received by 3<sup>rd</sup> party as they send e-mail messages through unknown sources and gets sensitive information like details related password PIN of credit card or debit card. So, it is important for the public to keep their password safe and as the password of the social media platforms should strong enough by the people. As with concept of phishing has been governed under certain laws:

- **Information Technology Act 2000:**
  - **Section 66:** Hacking with computer System
- **Information technology Act 2000 (After amendment of 2008):**
  - **Section 43(i):** Diminishing the value/utility of the information or affects information injuriously (I.e. hacking)

---

<sup>4</sup> Ruth Larson, Secret service nabs 259 on Cellular phone fraud "cloned phones seized" June 18 Times 1996

- **Section 66A:** Sending offensive messages through communication services
- **Section 66C:** Punishment for identity theft
- **Section 66D:** Punishment for cheating by Personation (using other person identity with intent to deceive) by using computer resource
- **Section 70B:** Indian CERT (computer emergence response Team) to serve as national agency for incident response
- **Indian Penal Code 1860**
- **Section 416:** Cheating by Personation
- **Section 464 :** Making False document
- **Indian Copyright Act 1957**
- **Section 51 :** Infringement of copyrights
- **Section 63 :** Offence of Infringement of Copyright or rights that are conferred by this Act
- **The trademarks Act 1989**
- **Section 27 :** Passing off
- **Section 29 :** Infringement of registered Trademarks

So, these are certain acts their sections that are dealing with the concept of phishing under Indian laws. As if we write about phishing and do not talk about Jamtara it would be slightly unfair as in 2015 this has been one of the biggest scams that have been registered by the police as some local gangs have been try call people by changing voice tone and ask for the bank card details or some sought of messages will be received from certain unknown no. asking for bank details as this case is considered to be India's biggest phishing case<sup>5</sup> as after this awareness programs has been started by the government for not giving any kind of sensitive details in the public place or not providing any bank details to any other person or sending to any third person as this might create chaos for the public. As another case that has provided the Definition of term "**Phishing**" **Nasscom v.Ajay Sood & ors.**<sup>6</sup>. So, still there are cases related to particular concept but with citizens getting more aware still the crime rate can get low.

## CYBER STALKING

As we are clear with concept of stalking in physical terms but there are large section of the society that are not clear with the terms of cyber stalking. So, cyber stalking basically means criminal usually means when the particular person anonymously follows other person over social media and post something that has been inappropriate and that particular activity has been done over

<sup>5</sup><https://indianexpress.com/article/india/india-news-india/phishing-in-jamtara-what-does-it-take-to-carry-out-online-fraud/>

<sup>6</sup>119 (2005) DLT 596, 2005 (30) PTC 437 Del

several other social media platforms and that would be considered as **Cyber-stalking**. As cyber-stalking is basically new form of cyber-crime which has been increasing with change in time there are technologies i.e. introduction of social media in the life of the people whether we talk about Facebook or any other kind of social media platform basically the cyber-stalking is taking new place in the form of cyber-stalking. As cyber-stalkers always think that they are anonymous and can hide without knowing their **IP address** as they use certain things such as the use of **Virtual private network (VPN)** with these things usually the location of the person gets hidden easily the particular person's location and not only the VPN but there are several other software that can be used to hide the location of the person as the use of VPN is basically temporary because sometimes these software's are not reliable. As all these things are basically helped by the cyber experts as these experts usually hired by the police officials under **section 45 of Indian evidence act 1872** and those materials will be given to the cyber forensics department as the department basically helps in decoding those software's and get to know about the criminal's location or his information and to retrieve certain more information related to cyber-stalkers or other kind of Cyber-criminals in the cyber space.

As the biggest strength of these cyber criminals is their anonymity as it has been described above that most of the cyber-stalkers remain hidden throughout their whole criminal activity and this is a problem for the society because it is impossible for a person who has not any sought of information regarding these cyber activities that who has been stalking as in case of physical stalking it can be seen that who is that person what is the purpose of those activities but in case of cyber-stalking the purpose and the motive is really impossible to know but still there are following motives that are mostly recorded in certain cases :

- **Revenge and Hate**
- **Jealousy**
- **Obsession**
- **Sexual harassment**

As these are certain motives recorded in recent years as per certain websites it has shown behavior that has been recorded in past 10 years.<sup>7</sup> As there have been different sections which have been dealing with the cyber-stalking across the country and there are different legislations such as **Indian Penal Code 1860** and **Information technology Act 2000**. As if we talk about the Information Technology Act as section 67 and 66 are talking about obscene and offensive messages basically under cyber-stalking both the things i.e. obscene and offensive at the same time and there are different

---

<sup>7</sup> [https://cyber.harvard.edu/vaw00/cyberstalking\\_problem.html](https://cyber.harvard.edu/vaw00/cyberstalking_problem.html)

section under Indian Penal Code i.e. (354D,292,507&509) as these section have been applied as in one way or another.

### **Section 354D-stalking**

### **Section 292-Obscenity defined**

### **Section 507- Criminal intimidation through anonymous communication messages**

### **Section 509- Violating modesty of women**

As the concept of both type of stalking has been inserted in **Criminal Amendment 2013 after the Delhi Gang Rape Case**. As both are in the need to be included as the cases related to physical stalking are having less situation but nowadays as there has been growing technology and case related to cyber-stalking has been increasing as according to a data by **NCW (national Commission for woman) as in this lockdown around 54 cases have been recorded** this shows that how the technology has been increasing but in a wrong way. As there certain section in IT Act 2000 deals with the Cyber-stalking and has been inserted in the **2008 amendment of the Act**, following are the section:

### **Section 67A: Part of cyber stalking**

**Section 67B: Punishment for publishing or transmitting of material depicting children in sexual explicit act etc. in electronic form** (As this section basically targets children that are below 18)

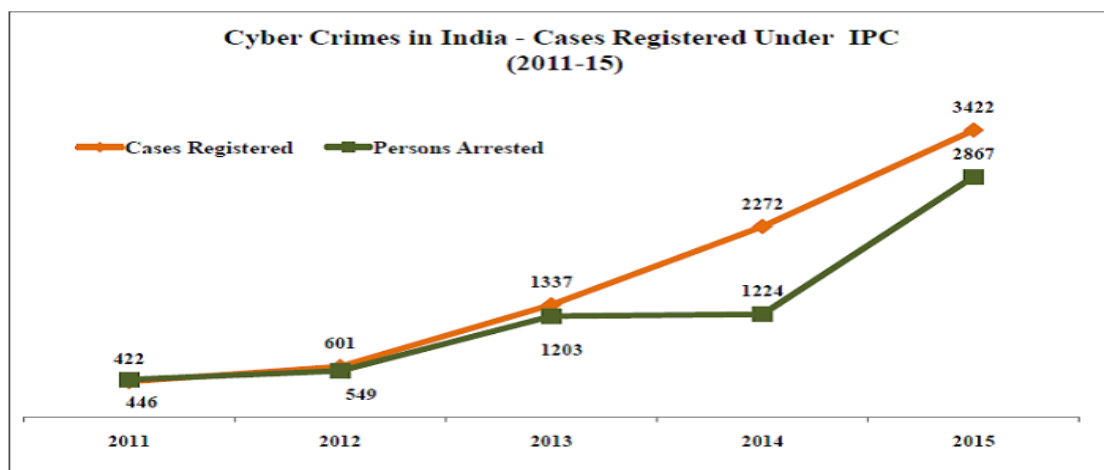
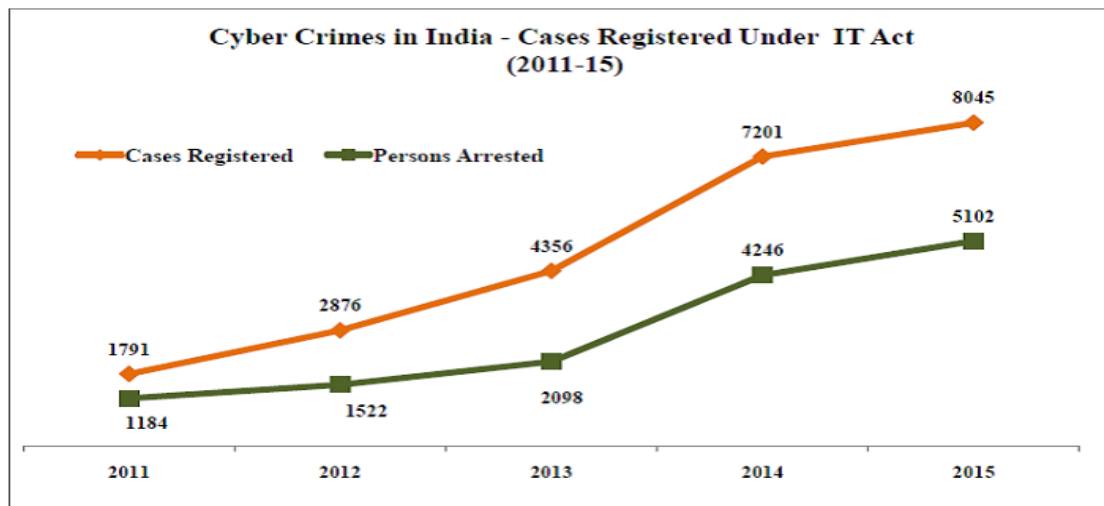
### **Section 66E: Punishment for Cyber terrorism**

If we look at different section of IPC there are certain kinds of section which shows that there are loopholes in **Section 354D of Indian Penal Code so, following are loopholes:**

- So, it ignores the fact that the men can be the victim of cyber stalking but the particular section focuses only on women and ignores the fact that the cyber-stalking is a gender neutral crime as through cyber crime there can certain things that can even happen to men. So, both the aspect should be inserted.
- Another thing that has been considered as a loophole under this section is that the method of communication

So, these are certain loopholes that are need to be looked at as this might be considered as a gate for the cyber criminals to get away. Similarly there is **Section 509 of IPC** that is also having same kind of problem that is being gender neutral i.e. only focuses on the women and men has been kept aside. As this section requires that words, sounds, gestures, heard and seen respectively. Thus cyber-stalkers can easily escape the penalty under this section as word cannot be spoken,

gestures cannot be seen and sound cannot be heard on Internet.<sup>8</sup> So these are certain section that need to be seen and addressed by the victim of the cyber-stalking and most of the time they are not familiar with jurisdiction that where they need to report the case as for that cyber cells has been made in India in different states . As there is graphical representation for cyber crime cases that has been recorded in IPC in past years:<sup>9</sup>



So, the graphical representation above shows when the case got registered under IPC and Information technology Act but the representation clearly shows that when registered under IPC criminals are more arrested this clearly shows that legislation is weak and there has been loopholes under certain sections as loopholes under IPC has been discussed above as not only IPC but the IT Act 2000 also need to change with the time and the laws need to be made more stricter, and the procedure for filling complaint against those crimes need to be made hassle free so that if any

<sup>8</sup>P.Duggal, India's first Cyber-stalking Case- Some Cyber-law perspectives, [https:// cyberlaws.net/ cyberindia/ 2CYBER27.htm](https://cyberlaws.net/cyberindia/2CYBER27.htm) (May 13,2017)

<sup>9</sup>[https://factly.in/wp-content/uploads//2015/03/cyber-crimes-in-india\\_cyber-crimes-registered-under-it-act.png](https://factly.in/wp-content/uploads//2015/03/cyber-crimes-in-india_cyber-crimes-registered-under-it-act.png)

kind of problem seen or any kind disturbance feel from the side of the victim he/she can easily file the complaint before the problem gets worse.

Similarly there are different types of cyber crime that has been discussed above similarly there has been cyber terrorism which has been increasing as this crime has been related to the cyber stalking as there has been inclusion of the **Section 66E which basically talks about the punishment of the cyber terrorism** , most of the times the cyber stalkers are mostly involved under cyber terrorism basically they uses victim data in such a way that would lead him to trouble and the chances of getting caught under the charges of Cyber terrorism are very less as they work by keeping their information anonymous basically it can be regarded as their biggest weapon or considered to be the only weapon.

### **SERVICE PROVIDER LIABILITY FOR COPYRIGHT INFRINGEMENT AND PORNOGRAPHY:**

---

As if we look at this there has been another crime that has been increasing in recent times there has been cases related to cyber pornography and at various places it has been discussed that intermediary are considered to be liable for any kind of mishappening as some of the experts thinks that intermediaries are considered to be the gateway for entering the cyberspace. As it provides online access to individuals, educationalist and government agencies. As the concept of intermediary has been defined under **Section 2(1)(w) of the information technology act 2000 “intermediary”, with respect to any sought of electronic records which means any person who on behalf of any other person receives stores or any kind of service related to that record.** For example Paytm can be termed as an intermediary because through its software pays certain bills to the service providers so it work as an intermediary as per the definition that has been described in the **section 2(1) (w) of the IT Act 2000.** As these service providers usually engage in commercial and non-commercial activities to connect the users from the world of Internet. As service providers thus include originator of the information flows from the access provider who possibly makes access to certain information across the cyberspace as for the intermediaries as to whom that service has been provided they are basically termed as the “**digital consumers**” as they usually take information from one place and provide that information to the end user. **As the question usually raise towards the working of intermediaries is that whether they are liable for any sought of copyright infringement or any kind of cyber crime?** So, the answer regarding the working of intermediary has been given under **Section 79 of the information technology Act 2000.** As to answer the question described above we have to talk about the liability of the network service provider/intermediaries, as for that it is necessary to

describe the **section 67 of the information technology act i.e. Punishment for publishing or transmitting obscene material in electronic form** which can also be considered as cyber pornography. As the word “**causes**” to be published in the electronic form any obscene material are rather broad to cover all prominent causes to the publishing of electronic obscene material. As the words are unqualified and the law can be applied to a spectrum of immediate activities that can be alleged as causes of publishing electronic form. So, u/s 67 is covered under the penal statute. As **Mens rea is required to prove before the said offence is required to be proved before**. Basically the offence of obscenity has been applied on the principle of “**Strict liability**” but it has to consider that Mens rea or the concept of guilty mind will play a minimal role. As the **internet service provider (ISP) telecom service provider (TSP)** as they are purely content provider and they have nothing to do with the content transmitted through their networks and they would not be covered under section 67 as causing transmission of obscene material is not an offence.

### **POSITION OF ISP IN INDIA**

---

As position of ISP liability in India is same as prevailing in other countries. As with the 2008 amendment of the Information technology act certain additional grounds were added as intermediary will not be liable for any third party information data or communication link made available or hosted by him if the function of the intermediary is limited to providing access to a communication.

**(Liable only if): As section 79 of the information technology act basically talks about “exemption from liability of intermediary in certain cases”** but it will be considered only if found that they have done any kind of conspiracy or aided or induced whether by threats or in commission of unlawful act.

**As Article 19(1) of the constitution basically talks about right of freedom of speech and expression but if we look at another clause i.e. 19(2) of the constitution it has basically said that there has to be certain reasonable restriction should be imposed** as that has to be imposed on the intermediaries as they are granted with the freedom of speech and expression but there has to be certain reasonable restriction which intermediaries need to follow i.e. intermediaries guidelines rules 2011 as these guidelines are need to be followed by the intermediaries as anything which is infringing any kind of copyright trademark or content is illegal in nature that content has to be taken down in 36 hrs but that has been criticized as after that clarification has been issued by government on 18 march ,2013 and the time has been increased to 30 days to redress such complaints from receipt of complaints.



## SUPREME COURT AND IT ACT

---

As there certain cases and the judgment has been given by the supreme court but back in **October 2000** the IT act is basically controversial piece of legislation as from back then the act has managed to draw considerable criticism from the legal community and the general public. As matter has become worse by introducing the infamous (**Section 66A: Punishment for sending obscene message in communication services**) basically the main problem with this particular section is that the “**vagueness of what is offensive in nature**” because if we look at the word “**offensiveness**” as the interpretation of this word can be different as for one person it can be offensive but for other it can be normal. So following are the cases in which supreme court has laid down different landmark cases:

**1. Shreyas Singhal v. Union of India<sup>10</sup>**

As in this particularly case as the entire section 66A of the IT Act was struck down in its entirety for being in violation of **Article 19(1)(a)** and it has not been following under the scope of the (**Reasonable restriction**) as per the constitution of India.

**2. Rajeev Chandrasekhar v. Union of India<sup>11</sup>**

As per this case it has been laid down that **section 66A** is ambiguous in its terms similarly intermediaries guidelines rules are similarly ambiguous and require private intermediaries to subjectively asses objectionable content. As per this case it has been laid down that **section 66A** is violative of **Article 14, 19 and 21** of the constitution.

**3. Common Cause v. Union Of India**

**4. People Union for Civil Liberties v. Union India**

So, these two case have shown the same thing that both the cases have similar thing that **section 66A** is violative of **Article 19(2) of the constitution** As the process of blocking the website is entirely secret and fail to meet the safeguards of natural justice but it has to be considered that it is right because if the notice are issued there are more criminal activities will be increased or any kind of activity can be done. So, after having a clear view about the liabilities of the intermediary and under section 79 how they can be exempted but if we look in the normal sense intermediaries are the third party that basically help in providing the services as they can be only considered to be liable if they found in any kind of conspiracy or aided in any kind of unlawful activity.

---

<sup>10</sup>(2013) 12 SCC 73

<sup>11</sup>W.P.(C) NO. 23/2013

## INCREASING OF CYBER CRIMES IN PANDEMIC

As in the pandemic of COVID-19 the chances of cyber crime gets increases and in modern era this modern age crime has causing problems more than the physical crimes as the physical crimes get caught easily we get to know the name of the person but in case of these crimes the name of the person are chances has been used wrong as these criminals use most of the times wrong names to get away from the crime as it become helpful for those criminals. As in this pandemic all the citizens in the country are in their home in lockdown try to get safe from the corona virus but how will they get safe from virus of cyber criminals and their different attacks that has been described above, as per Google reports in January there are 149k active phishing websites and in the February websites doubled their rates to 239k and in march that number has increased to 539k- a 350% increase since January.<sup>12</sup>



As another thing that has to be kept into mind is that the children are at home in this lockdown amid COVID-19 so they might not get indulge into pornography activities as there are certain sites that are harmful for the children and the crime rate for cyber pornography get increases as those sites are most trafficked sites on the internet as per some records in the recent years India has been at 3<sup>rd</sup> position in the world watching the pornographic content which has resulted some sought of cyber attacks<sup>13</sup>

As the income source has been reduced for the people and the cyber criminals take advantage of this time and send certain sought of e-mails claiming that by filling this survey or playing any kind of quiz the individual might be able to win certain cash prize as these are generally e-mail attacks as people who not familiar with this kind of stuff will get fall into it. So, the people should look

<sup>12</sup> [http://www.unicri.it/news/article/covid19\\_cyber\\_crime#anchor18](http://www.unicri.it/news/article/covid19_cyber_crime#anchor18)

<sup>13</sup> <https://www.menshealth.com.au/coronavirus-pornhub-spike-in-traffic-free-premium-membership>.

for such kind of emails and do not fall for these kind of stuff as these e-mails are of such luring nature that the person get fall into it or they take information through your e-mail accounts as most of the people have link their e-mail accounts with phone and usually all the data get sync with the e-mail id.<sup>14</sup> So, these are certain data that is showing that how the cybercrime has been increasing or at increasing rate amid corona virus.

## CONCLUSION

---

So the following article shows that how the liability of the following section arise in the society and types of cyber crimes and whether intermediary are liable for modern age crimes but if we look at the growing rate of cyber crime it cannot be stopped by the government or any kind of foreign officials but the citizen themselves have to become much more engaged and informative with the society at large, so that the growing rate of these crimes will gradually becomes slow. As time when these crimes were realized by the public is when the **Sony pictures got hack or the Bangladesh bank heist** these are considered to be the famous cases where the officials were not known about the attack basically they get to know after all the action but till then it is considered to too late. So, it is important that the government start spreading awareness regarding these crimes especially in developing countries like India where half of the population lies in the urban areas as when the citizen themselves get informative they can easily dealt with the problem as all the procedures should tell by the officials regarding these crimes.

---

<sup>14</sup><https://www.reuters.com/article/us-cognizant-tech-cyber/cognizant-hit-by-maze-ransomware-attack-idUSKBN2200YA>