VOLUME 9 ISSN 2456-9704

CYBERCRIME: ARE THE LAWS OUTDATED?

By Bhavya Kaundal
From Symbiosis Law School

ABSTRACT: -
In the present day, people cannot live without the internet because everything from online transaction to online dealing is done on it. Some people use it for wrong purposes and commit crimes like cyber bullying, identity theft, hacking, spreading hate messages etc. To prevent these crimes cyber laws were made. In India, Information Technology Act came into being after the mid-90s when globalization and growth of computerization took place. This Act does not define cybercrime, but S.65 -S.75 describes the offences and punishment for committing these crimes. Also, 2008 amendment in IT act added new sections to protect the people against cybercrime and help the victims that have suffered from it. Thus, Cyber law evolves and has become an important part of protecting our internet lives.

INTRODUCTION:

With the advent of technology, our lives have no doubt become easier, but it has also brought in the problem of cybercrime.

Cybercrime is a type of crime that involves a computer and a network. In simple words, cybercrime is an unlawful act in which a computer is used or where a user/network becomes a target. Cybercrimes involve criminal activities like fraud, identity theft, hacking, distribution of child pornography etc. Cybercrime can be generally be broken into two categories:

- Crimes that target computer networks or devices. These types of crimes include viruses and denial of services (DOS) attacks.
- Crimes that use computer networks to advance other criminal activities. These types of crimes include cyberstalking, phishing and fraud or identity theft.[1]

In cybercrime, there is generally criminal misuse of technologies in the following forms: -

1) Phishing: - means a crime or fraud in which the attacker tries to gain personal information by sending a false email or message as a reputable individual or entity to the victim. E.g.: attacker pretending to be employee of the bank and sending a message on the individuals mobile to get his account details.
2) Identity theft – it basically refers to people who cheat or fraud others by using another person's identity. It involves stealing money or getting benefits by pretending to be someone else.
3) Hacking: - basically means to break into someone's computer system and steals valuable information (data) from the system without any permission. Among all types of cybercrime, it's the most dangerous and serious to the internet and e-commerce.
4) Spreading hate and inciting terrorism- is also a cybercrime because it attacks an individual based on race, religion, sex etc. E.g.: Gender based hate speech on Facebook

[1] *Definition of cybercrime, Technopedia*, (Dec 9, 2018), https://www.techopedia.com/definition/2387/cybercrime

5) Distributing child pornography- Any persons who possess for the purpose of transmitting, distributing, selling, importing etc. or possess, transmits, sells or advertises child pornography is guilty of this cybercrime and is liable to imprisonment for a term not more than 14 years.
6) Grooming: means making sexual advancement to minors

For fighting these crimes Cyber laws were introduced in many countries, Punishments were also laid down.

CYBER LAWS IN UK,US:

In UK many legislations have been made for managing cybercrime such as the Computer Misuse Act (CMA) (1990) , Regulation of Investigatory Powers Act 2000, Data Protection Act 2000,Offences under Fraud Act 2006, S.127 of the Communication Act (2003) makes it an offence to send a message or other material that is 'grossly offensive' or of an indecent , obscene ,menacing character through a public electronic communication network[2] and S.33 of the Criminal Justice and Courts Act 2015 created an offence of disclosing private sexual photos without the consent of an individual with the intent to cause stress to him or her. Serious Crimes Act 2015 amended the Computer Misuse Act 1990 and it ensure life sentence for Cybercriminals if the act has caused loss of life, serious illness, injury, or serious damage to national security.

In US, regulations for cybercrime are the Computer Fraud and Abuse Act, the Wiretap Act, and many other acts.

Cyber Law in India: -

The Information Technology Act 2000 and IT amendment act 2008 have been dealt with in detail regarding electronic offences. Cybercrime has not been defined in the Information Technology Act 2000 or in its amendment Act nor in any legislation in India. Basically, the definition of cybercrime is a combination of crime and computer. offences or crime has been dealt with elaborately listing various acts and punishments for each under IPC 1860 and few other legislations too[3]. Offences against computer or the data itself is the target and where computer is a tool in committing other offence or it provided necessary inputs for that offence therefore it comes under Cybercrime.

Origin of Information Technology legislation in India: - mid 90s India saw a dire need to come up with a legislation due to globalization and growth of computerization in many nations and for e-commerce. Before lot of transactions use to take place through post and telegraph only. United Nations Commission on International Trade Law (UNICITRAL) made a model law on e-commerce and recommended all the States to enact and revise their laws keeping the model law in consideration. The Indian Government enacted the Information Technology Act in June 2000. The act mainly deals with legal recognition of electronic documents, legal recognition of

[2] *Cybercrime – prosecution guidance, Legal guidance*, (Dec 10, 2018), https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance

[3] *Cyber-Laws -Chapter in Legal-aspects-book*, (Dec 15,2018), http://www.iibf.org.in/documents/Cyber-Laws-chapter-in-Legal-Aspects-Book.pdf

Digital Signatures, Offences and Contraventions, Justice Dispensation Systems for cybercrimes [4] .

Applicability of IT Act: -
IT Act 2000 is applicable to everything except: -

- Negotiable Instruments
- Power of Attorney, 1882
- Indian Trusts Act, 1882
- Indian Succession (Will) Act,1925
- Any contract for the sale or conveyance of immovable property or any interest in such property.

Provisions in IT ACT relating to cybercrimes: -S.65 to 75 deals with cybercrime and punishments related to those crimes.

S.65- Tampering with the computer source documents: -Whoever conceals, destroys or alters any computer source code used for computer network, computer program, computer network knowingly or intentionally shall be punishable with imprisonment up to three years or fine that may extend up to Rs.2 lakhs or with both. This section is cognizable and bailable.
Case laws:Sayed Asifuddin case[5]: - in this case the Tata Indicom employees were arrested for manipulation of the electronic 32- bit number (ESN) programmed into cell phones that were exclusively franchised to reliance infocom. Held: The court held that such manipulation amounted to tampering with computer source code as described in s.65 of the Information Technology,2000.

s.66-hacking with computer system, data alteration etc.– (Computer related offences) whoever with the intent causes or likely to cause wrongful loss or damage knowingly to the public or destroys, deletes, alters any person's information residing in a computer resource or diminishes it value, utility or affects it injuriously by any means, commits hacking. It can be read with S.43 (a) cause of S.77 which explains that a compensation, confiscation or penalty for not to interfere with other punishment which came after 2008 amendment.

- Hacking incidents in India: -

Atm System hacked In Kolkata[6]: -A Canara bank atm servers was hacked by fraudsters On July 2018 and wiped off almost 20 lakh rupees from different bank accounts. The number of victims was over 50 and it was believed that they were holding the account details of more than 300 Atm users across India. On 5th August 2018, two men were arrested in New Delhi who was working with an international gang that used skimming activities to extract details of bank account.

Zomato (2017) [7] :- The Restaurant app Zomato was hacked and suffered when data of some 17 million users were stolen.

[4] Lionel Faleiro, *IT Act 2000-penalties, Offences with Case studies*(Dec17,2018), https://niiconsulting.com/checkmate/2014/06/it-act-2000-penalties-offences-with-case-studies/

[5] Rahul Deo, *Offences Under IT Act, 2000,* (Dec 22, 2018) https://www.lawctopus.com/academike/offences-act-2000/

[6] *Major Cyber Attacks in India (2018),* (Dec 22, 2018),https://www.testbytes.net/blog/cyber-attacks-on-india-2018/

[7] *8 big global attacks that affected India*, (Dec 23,2018), https://www.gadgetsnow.com/slideshows/8-big-global-hacking-attacks-that-affected-india/photolist/63720530.cms

Hackeread.com claimed that a user by the name of 'nclay' claimed to have hacked Zomato and was offering data of some 17 million registered Zomato users on dark web marketplace. Zomato had acknowledged the hacking attack, however, claimed that no payment information or credit card data was stolen / leaked.

S.66A – Sending offensive messages through any communication services: -

Any electronic mail or email sent with the end goal of causing anger, difficulty or mislead or to deceive or sending any information that's not true with the end goal of annoying, causing inconvenience, danger, insult, obstruction, hatred, ill will. The person could be sentenced up to 3years of imprisonment along with fine.

Case laws: -

Nikhil Chacko Sam V. State of Kerala (July 9th, 2012) –The accused was with the complainant in Chennai because it was a college reunion and all of them took photos one of the friends had their boss with them. So, the accused later transmitted the photos and depicted the complainant in a bad light through internet which lost him his job. The Kerala Court charged the accused under S.66-A, ITA and was imprisoned.

Shreya Singhal case: It's a landmark case which led to the deletion of S.66 from the IT Act. In this case two girls posted their comments on Facebook describing the displeasure of the bandh called in the wake of Shiv Bal Thackery's death and later were arrested for it by Mumbai Police. The arrested women were released later on and it was decided to close the criminal case against them but the arrest had already attracted widespread protest. There were a lot of petitions to the Supreme Court that 66A was against the constitution because it was vague, ambiguous and was being misused by law enforcement authorities. It was also contended that S.66A violates freedom of speech and expression. Supreme Court held that s.66A is unconstitutional cause it violates Article 19(1)(a) freedom of speech and is ambiguous thus was struck down entirely.

Exception of this section is that it is applicable to the Non- citizens of India cause its struck down only for citizens of India. If Non-citizens commit this crime as described above they will be charged under S.66A.

S.66B-Receiving stolen computer resource or communication device: -

Whoever receives or retains any stolen computer resource or communication device dishonestly knowingly or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment with the term extending to three years or with fine extending to Rs.1lakh or with both.

S.66C- Identity Theft: -

Whoever uses the electronic signature, password or any other unique identification of another person fraudulently or dishonestly will be punished with maximum three-year imprisonment and also a fine up to RS.1lakh.

S.66D- Cheating by personation by using computer resource: -

Whoever, cheats by personating through any communication device or computer resource; shall be punished with a term extending to three years and also a fine extending to Rs.1lakh.

Examples –
Woman in Gurgaon deceived into giving Rs.30 lakh to 'Ukrainian' she met on matrimonial site(25th May 2017)- the complainant told the city police that she created a profile on a matrimonial site last year in February and got response by a person who identified himself as Deepak Frank Rich ,Ukrainian. A case was then registered under S.66D Of IT Act and S.420 of Indian Penal Code[8].
Student detained for cheating in exam (Thane, July, 2017) [9] - the accused was caught copying while he was writing his 10-math paper as his friend helped him by sending him photos of the answers through WhatsApp. The accused friend was also booked. The case was booked under S.66D of Information Technology Act.

S.66E – Punishment for violation of privacy: - (voyeurism)
Whoever, publishes or transmits the image of a private area intentionally or knowingly of any person without his or her consent violates the privacy of that person. Punishment is imprisonment extending to three years or with fine not exceeding Rs.2lakh rupees, or with both.
Example: -

1) Hidden cameras were found in the changing rooms by HRD minister Smriti Rani in Fab India store in Goa.
2) Jawaharlal Nehru University MMS Scandal [10] - In this prestigious institute, a pornographic MMS clip was made in the campus by the two accused studentswho initially tried to extort money from the girl in the video but when they failed the accused put the video out on mobile phones, on the internet and even sold it as a CD in the blue film market. This would come under S.66E cause the transmitted this video intentionally violating her privacy.

S.66F- Cyber terrorism: -
Whoever denies or cause the denial of access, attempts to penetrate or access a computer resource without hisor herconsent, introduces or causes to introduce any Computer Contaminant with the intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people. This section is cognizable and non-bailable. Anyone who commits or conspires to commit cyber terrorism will be punishable with imprisonment which may extend to life imprisonment.

S.67 - Publishing or transmitting obscene material in electronic form: -
Anyone who publishes or transmitsor causes any material which is indecent or appeals to the or prurient interest to be published in the electronic form, or if its effects is such as to tend to deprave and corrupt persons who are likely , to read, see, or hear the matter contained or embodied in it shall be punished with imprisonment of term extending to two three years in first

[8] *S.66D Punishment for cheating by personation by using computer resource*, (Dec 24, 2018) http://www.itlaw.in/section-66d-punishment-for-cheating-by-personation-by-using-computer-resource/

[9] *Boy Detained for Copying During School Exam*, (Dec 24 ,2018), https://www.indiatoday.in/pti-feed/story/boy-detained-for-copying-during-school-exam-1003031-2017-07-23

[10] Lionel Faleiro, *IT Act 2000-penalties, Offences with Case studies*Supra

conviction with fine extending to five lakh rupees. In the second or subsequent conviction with imprisonment of either for a term extending to five years and also with fine extending to ten lakh rupees. Cyber Pornography: - S.67, S.67B are provisions applicable for preventing this crime.

Case law: -

1)Suhas Katti case- in this case the accused started harassing a divorcee lady through false email account opened by him in her name. These emails contained obscene defamatory and annoying messages which resulted in annoying phone calls to the victim. On her complaint the accused was charged and found guilty of offences under S.469 and S.509 of IPC and S.67 of IT Act 2000. He was sentenced to two years of imprisonment and fine of four thousand rupees. This was the first case of conviction under S.67 of IT act 2000.

2) Chennai techie jailed under S.67[11]: - Srinath Nambudiria software engineer was working in TCS, Siruseri (Tamil Nadu). He was attracted to a colleague and expressed his love to her. When she rejected him, he started sending several obscene and derogatory emails to her in 2011. She had gone for trip then Nambudiri send a morphed nude picture of the woman to her brother. He continued to stalk and eve tease the women electronically for several months. After returning to Chennai she filed a complaint against him with cyber wing of CBCID. It was only then the police registered a case against Nambudiri and SC held him guilty under S.67 of ITAct,S.506 and S.509 of IPC along with S.4 of Tamil Nadu Prohibition of harassment of women Act ,1998. The court convicted him and slapped with fine of Rs.20,000.

S.67(A) is similar to S.67 just that the person will be imprisoned for 5 to 7 years and fined up to 10 lakhs. Both S.67 and 67(A) does not extend to any book, pamphlet, writing, drawing, representation or figure in electronic form.

S.67(B) Publishing or Transmitting of material depicting children in sexually explicit act, etc.in electronic form (Child Pornography): -

Whoever publishes or transmits, creates text or digital images, cultivates or entices or induces children to online relationship, facilitates abusing children online or records in any electronic form of others pertaining to sexually explicit act with children.Any person who commits this crime for the first time will be imprisoned for a term extending to five years with fine up to 10lakhs. Second conviction criminals could be sentenced for a term that could extend to 7 years along with fine up to 10 lakhs. This is a positive change as this section makes even browsing and collecting of child pornography a punishable offence.

The difference between S.66E and S.67 is that in one its fine if it's done with consent and in the latter prohibits transmission and publication of obscene and sexually explicit material.

S.69-Power to issue direction for monitor, decryption or interception of any information through computers resources: -

[11]Manish Raj, *After 66A is Scrapped, Sec 67 of Same Act Lands Chennai Techie in Jail*, (Dec 26, 2018), https://timesofindia.indiatimes.com/india/After-66A-is-scrapped-Sec-67-of-same-Act-lands-Chennai-techie-in-jail/articleshow/46695301.cms

This provision gives power to authorities for giving direction for monitor, decryption or interception of any information through computers resourcesif there is threat to integrity, security, sovereignty or defense of the country or state or to prevent any cognizable offence related to the above situation. The power is subject to the condition that authorized officer records reasons in writing. The power includes directing, intermediaries, subscribers or individuals to assist in providing access to the computer and also in decrypting, intercepting or monitoring or intercepting the concerned information.

S.69A- Power to issue directions for blocking for the public access of any information through any computer resource: -
It vests with the central government or any of its officers with the powers to issue directions forblocking for public access for any information, through any computer sourceif there is threat to integrity, security, sovereignty or defense of the country or state or to prevent any cognizable offence related to the above situation.

S.69B- Power to authorize to monitor and collect traffic data or information through any computer resource: -The central government vests the power to authorize to monitor and collect traffic data or information to enhance Cyber Security and for identification, analysis and prevention of any intrusion or spread of computer contaminant in the country.

There are few more important sections in IT Act ,2000: -

- S.70- Unauthorized access to protected systems
- S.71-Penalty for misrepresentation
- S.72-Breach of confidentiality and Privacy
- S.73-Publishing false digital signature certificates
- S.74-Publication for fraudulent purpose
- S.75- Act to apply for contravention or offence that is committed outside India
- S.77- Compensation, Confiscation or penalties for not to interfere with other punishment

Information Amendment ACT, 2008: - This act came due to some of the sections in the original Act being criticized for being draconian and others stating it to be diluted and lenient. The Act came into force in 2009. So, it introduced many changes to the existing IT Act which added several cyber offences. The eight new cyber offences added are as follows-

1) Identity Theft (S.66C)
2) Sending offensive messages through mobile phone or computer (S.66A)
3) Receiving stolen computer resource or communication device (S.66B)
4) Punishment for cheating by personation using Computer source (S.66C)
5) Cyber Terrorism (S.66F)
6) Punishment for violating privacy or video voyeurism (S.66E)
7) Child Pornography (S.67B)
8) Publishing or transmitting material in electronic form containing sexually explicit act (S.67A)

Non-bailable Offences: - In IT act 2000 all of the acts were cognizable and bailable but after the amendment in 2008 any offence punishable with death, life imprisonment or imprisonment for more than 7 yrs. And if an offence is punishable with more than three years but less than 7 yrs. These are cognizable and non-bailable offences. Sections which are non-bailable is S.66F because punishment is life imprisonment, S.67because punishment is imprisonment extending to five years, S.67A and S.67Bbecausepunishment is imprisonment exceeding five years and 7years, S.69 and S.69Abecausepunishment is imprisonment for seven years.

IPC Code 1860: -

Information Technology does not cover all aspects of cybercrime and therefore Indian Penal Code is applicable. Therefore, after the enactment of information Technology the law makers amended IPC to include offences involving electronic record.

Most of the cybercrime come under the category of fraud but Information Technology Act has not defined the concept of fraud thus lot of the offences come under the preview of Indian Penal Code.S.25 of IPC defines fraud and element of intent to defraud must be present and defraud implies deceit and injury to the person deceived. In IT Act 66B talks about dishonest intention which is not defined in the IT Act then one can refer to IPC[12] . When cyber fraud is committed it is cheating in real sense thus s.145 of IPC can also be applied. Apart from this S.345C deals with voyeurism and S.345 stalking are acts of IPC which are made for the internet and communication devices. Cyber defamation is not too different from the defamation in S.499 of IPC because it just means writing any derogatory statement, which is intended to injure a person's business or reputation on the internet like writing defamatory matter about someone or sending an email containing defamatory material. Financial Crimes are also punishable under IPC and IT Act and these include cheating, money laundering, credit card frauds etc.Web Jacking comes under S.383 of IPC and the comes from the word hijacking. It means when a website is web jacked the owner of the site loses all control over it. The person gaining such kind of access is called hacker who may alter or destroy any information on the site[13]. As it is one kind of hacking and IT cannot cover all kinds of hacking therefore IPC is generally applicable to such kind of unauthorized access.

These offences are subject to Indian Penal Code and without the general principles of criminal law, Cyber law cannot work in India.

Conclusion-

India is a fast-growing internet user country. Today users are able to access internet at any time and from anywhere. Data Communication by way of emails and mobile applications have increased many folds. This brings progress but at the same

[12] *Chapter III: The Law Relating to Cybercrime in India*, (DEC 18, 2018),http://shodhganga.inflibnet.ac.in/bitstream/10603/203654/8/08_chapter%203.pdf

[13] **Rajkumar Dubey,** ***India: Cyber Crimes "an unlawful act where in the computer is either a tool or a target or both",*** (Dec 19, 2018),http://www.mondaq.com/india/x/28603/technology/

time makes the country vulnerable to different kinds of cybercrimes that is explained above. To counter the threats, India has implemented digital India project which attempts to minimize connectivity. In the past years, more than 50,300 cyber security incidents have been reported to Indian authorities - including denial of service attacks, web site infiltrations and, especially phishing[14]. In 2017 alone 4,035 cybercrime cases were registered under IT Act. Cybercrime against women and children are also on the rise. One recent example is the online game -Blue whale. Most cities in India have a cybercrime cell where citizens can file a cybercrime complaint like online harassment, stalking, pornography etc. If there is no cyber cell in any place then FIR can be filed in a local police station. There is also an initiative by the government to start an online portal (www.cybercelldehi.in).

The law is not outdated as amendments were also made. The law helps control cybercrime but still there is a need to follow best practices and guidelines to minimize security risks of cybercrime. There is also need to review international law in this field. Cyber law needs to change and evolve constantly so the authorities are step ahead of the hackers and criminals. The law does deal with challenges of cyberterrorism but it may require additional security measures and strengthen criminal liability rules in the law. Law must also ensure that a proper balance is maintained between protecting the nation and its citizens while ensuring that their privacy and rights aren't infringed. India has taken lot of steps to control cybercrime but we cannot be complacent in our vigilance and need to ensure that the laws keep evolving with time and technological advancement.

*****

[14]Vanita Pandey, *Inside India's Cybercrime Boom*, https://www.threatmetrix.com/digital-identity-blog/cybercrime/inside-indias-cybercrime-boom/ (Dec, 27 2018)