The Cyber World- A Necessary Evil

-Subhiksha Srinivasan & S. Baranitharan

Abstract

Cyber world is dynamic and fast growing and makes almost anything accessible at the click of a button. It has created a lot of opportunities and has made communication easier and people from different corners of the world are able to reach each other instantly. Cyber forums prove to be most unrestricted and accessible.Electronic data is the least secure data today. Ironically, electronic data can prove to be most harmful, when leaked. Cyber law aims at regulating the use and preventing the misuse of electronic data. Cybercrimes and frauds form a huge part of organized crimes, popularly known as 'White collar crimes'. They are very hard to prevent or investigate as the criminals at work are experts in their trade. They are smart, trained and most of the time, educated and make sure they make a clean sweep of the trial.Cybercrimes may have economic, social and political implications. This paper deals with those white-collar crimes and their legal consequences and ways to prevent such crimes and ways to keep cyber data safe and secure.

Cyber Crimes- An Introduction

On churning the ocean of cyber space, cybercrimes come out before the nectar of knowledge and development could come up. A lot of technological development and the increased ease in communication can be attributed to cyber space. However, these gifts do not come without a bitter pill. There is a huge scope for misuse of data and many privacy issues might crop up.

A cybercrime, in a layman's language, constitutes any unauthorized usage of electronic data with criminal intent to cause political, social or economic detriment. A cybercrime could cause any of the three detriments or more than one of them at a time. To quote some, Pornography and obscenity causes social detriment; Banking frauds and black marketing in cyber space causes economic detriment; False propaganda and canvassing about a leader can create political unrest;

Legally speaking, there is no exhaustive definition given to the term in the Information Technology Act, 2000. Anything that falls under the ambit of any of the provisions under the IT Act could be considered a cybercrime. The IPC and CrPC also deal with cybercrimes. Cyberspace is a dynamic area which keeps evolving with time. Therefore, defining cybercrimes and creating borders for the same would not serve the purpose. Cybercrimes need a very liberal definition, capable of accommodating any kind of cyber and electronic data mishaps. Cybercrimes need a definition which would include not only existing crimes, but also crimes which are capable of cropping up in the future, with the development in technology.

Cybercrimes could be broadly classified under three heads:

1. **Crimes against persons:**

   Cybercrimes against persons include stalking, harassment and child pornography, etc. Such crimes aim at attacking the dignity and privacy of people. Cybercrimes in this category also include damage to reputation, status, etc. Pornography and stalking are the most common crimes under this category. They spoil and pollute young minds and instigate crimes of very serious nature.

2. **Crimes against property**

The crimes under this category include trespassing through cyberspace, computer vandalism, transmission of harmful programmes and unauthorized possession of computerized information. Cracking and hacking are among the gravest of the lot. No system or hardware or software is fool proof. There is no system that cannot be hacked or trespassed or misused. Stealing of information and data is a theft by itself. Banking frauds, misuse of company secrets, misuse of financial statements, etc. are some of the many crimes under this category.

3. **Crimes against government**

This category of crimes proves to be most hazardous to the entire nation.Cyber crimes against government threaten the security of the country. Defense secrets are at stake. Important and confidential information are subject to risk. Cyber terrorism is the most vicious in this category.Cyber terrorism is when an individual hacks into government websites or gets his hand into confidential government data.

The Government And Cyber Crimes

E Government is the process of using Information Technology Information and Communication Technology for rendering Government services and managing administration.

E Government consists of:

1. G2C interactions (Government to Citizen)

2. G2B interactions (Government to Business)

3. G2E interactions (Government to Employees)

4. G2G interactions (Government to Government)

The internet is used to convey information to the public regarding general holidays, public hearing schedules and to issue briefs, notifications, etc. and to perform regulatory functions. There is a two-way communication between the citizens and the government, enabling the citizens to post comments, make request to government agencies and avail other services from the government authorities. Lodging tax returns is also done online. E Governance turns the citizens form passive spectators to active participants in governance.

The citizens are more informed, participative and aware of their rights and duties. The government offices can be controlled and regulated better. Scope for corruption and bribery is reduced. A considerable amount of the country's funds are saved. E Governance creates a lot of employment opportunities for the educated and unemployed youth.

The disadvantages of e governance are:

1. Lack of access to theinternet to a large chunk of the population.
2. The information on the web is not always reliable.
3. Public opinion may be manipulated if internet is overused.
4. Political motives can create unrest in the society and the internet may have a big hand in this.
5. Misuse of governmental electronic data can prove to be dangerous.
6. Government officials might turn out to have more power than they ought to, which can be fatal.
7. A new scope for corruption might crop up, which will be through the hands of trained, educated and informed people.
8. Initial investments may prove to be high.
9. Privacy issues might crop up as the government has more information about the citizens than earlier.
10. A separate agency is required with expertise, to link the cyber crime with the cyber criminal.
11. Collection of electronic evidence is challenging.
12. The Judiciary also requires technical knowledge and expertise to achieve the ends of justice.
13. Innocents may be penalized for no wrong of theirs due to misuse of identity and proving misuse of identity is a herculean task.

Cyber Security And E Governance

Cyber-attacks on governmental data can disrupt the security of the country. It can disturb the social and political peace in the country and can cause devastating economic effects. Espionage and hacking are no small threats to e governance. Cyber criminals are offered information on a

golden platter. Enemy nations also do not find it difficult to access information. Defense sector becomes weaker when the enemy nation gets more information. Intellectual property is not very secure anymore. Cyber criminals may steal information either for their personal benefits or they may act as agents to a government.

The wikileaks case showed how destructive cyber criminals could prove to be. Wikileaks obtained information which was supposed to be confidential. Wikileaks was founded in 2006 by Julian Assange, a computer programmer and hacker. Chelsea Manning was a former Army intelligence analyst, who provided Wikileaks with classified documents and was convicted under the Espionage Act, 2013, and was sentenced to 35 years of imprisonment. Her sentence was later commuted by President Barack Obama on 17th May, 2017. Wikileaks threatened the security of the United States and there could not be a better example for what harm a cyber crime could cause.

Cyber terrorism is a distinct crime under cyber crimes against government. Cyber terrorism is when an individual cracks into a government or military website to disrupt the peace and security of the country. This shows that the internet and cyberspace can be used by a small group of individuals to actually instill terror in citizens and to threaten powerful governments. Cyber terrorism relies more on the brain than brawn. All plans and attacks made by cyber terrorists are fool proof and difficult to establish guilt. These attacks cause the most destruction as there are no preventive measures taken. The Twin Tower is a living example for this fact. Post September 11, 2001, Cyber terrorism was taken seriously by the European Union and some other countries. A treaty called International Cybercrime Treaty was formulated.

Section 66F of Information Technology Act defines Cyber Terrorism and provides for the punishment for the same.Section 66F (1)(A) says that any misuse or abuse of cyber data and computer resources with and intention to spoil the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people and thereby death or injury to person or property or disruption of services provided.Section 66F(1)(B) says that any access to information that is kept confidential for the purpose of security or foreign relations amounts to cyber terrorism. Punishment for cyber terrorism may extend upto life imprisonment.

Cyber Crimes Against People

The provisions of Information Technology Act which cover cyber crimesagainst people are 66A, 66C, 66D, 66E, 67, 67A, 67B. Section 66A provides for the punishment for sending offensive messages through communications services, etc. Section 66C provides for about punishment for identity theft. Section 66D for punishment for cheating by personating by using computer resource. Section 66E provides for punishment for violation of privacy. Section 67 provides for punishment for publishing or transmitting obscene material in electronic form. Section 67A provides for punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form. Section 67B provides for punishment for publishing or transmitting material depicting children in sexually explicit act, etc. in electronic form.

Section 66A says that communication of any message which is offensive in character and which, known to be false is transmitted with ulterior motives, including those messages sent through mail or mail messages. This provision was declared unconstitutional by the Supreme Court in Shreya Singhal vs, Union of India[1]. The Supreme Court held that the provision was beyond the reasonable restrictions[2] of freedom of speech and expression[3]. The misuse of this provision in many instances led to filing the said Public Interest Litigation. The PIL was filed by Ms. Shreya Singhal when two girls, namely ShaheenDhada and Rinu Srinivasan were arrested under section 66A of IT Act for commenting on the shut down in Mumbai on Shiv Sena leader Bal Thackeray's death. One of girls posted the comment and the other 'liked' it.

There are many other instances where this provision was misused. To name a few, Ambikesh Mahapatra was arrested for posting cartoons on the Chief Minister of West Bengal, Mamata Banerjee in 2012, Mayank Sharma and K.V. Rao were arrested for allegedly posting offensive comments against political leaders in their facebook group, Businessman Ravi Srinivasan was also arrested allegedly for tweeting that Karti Chidambaram, son of Union Minister P. Chidambaram was 'Corrupt', three youngsters from Kishtwar district namely Kishori Sharma, Bansi Lal and Moti Lal Sharma were kept in confinement for 40 days for being tagged in an allegedly blasphemous video posted on Facebook. One of them had commented on the video.

[1] AIR 2015 SC 1523
[2] Article 19(2) of Constitution of India
[3] Article 19(1)(a) of Constitution of India

They were charged for inciting communal violence and for desecrating religious symbols using Information Technology, a tourist officer in Varanasi was arrested for uploading 'objectionable' pictures of Samajwadi Party Leader Mulayam Singh Yadav.

Section 66C deals with identity theft. Identity theft refers to misuse or abuse of another person's identity. A person's identity lies in their signature, passwords or any other unique identification feature. Punishment for identity theft is imprisonment upto three years and fine upto Rs. 1,00,000/-. Identity theft could be done with monetary or other motives. Identity thief can use the information to fraudulently apply for credit, file taxes or get medical services.Even if the misuse of communication devices is not explicitly mentioned, it will be covered under this provision. However, the term 'Unique Identification Feature' is not defined under the Information Technology Act. This phrase could mean anything and everything that a person uses to access his or her personal information. With development of technology and communication, defining this phrase will not serve the purpose.

Section 66D deals with punishment for cheating by personationby using computer resource. Cheating by personation and identity theft are very similar to each other. Cheating by personation refers to misrepresentation. Identity theft refers only to misuse of personal information or access to personal information. However, the effect is the same in both these cases. Cheating by personation is punishable with a maximum of three years and fine upto Rupees One Lakh.

This offence is not new to the Indian Legal system. Section 416 of Indian Penal Code defines the same offence and section 419 provides for the punishment for the same. The essential ingredients of this offence are:

a) Pretending to be some other person
b) Knowingly substituting one person from another person
c) Representing that he is a person other than he really is
d) Representing that any other person is a person other than such other person really is.

All or any of these acts must be done with an intention to cheat or defraud. The person represented may be real or imaginary.

There are many instances of these two offences right from the 50's[1], even before Information Technology Act came into force. These crimes are generally charged as conspiracies as they are done as a team and seldom individually. Recently, in October, 2017, a house maid in Singapore had used her employer's identity to book a hotel and spa without his knowledge. She was sentenced to 45 months' jail. Even faking a Facebook ID and using it to threaten the victim and her family would also be considered an offence under Section 66C and 66D[2].

Section 66E provides for the punishment for violation of privacy. Capturing and transmitting images which would tragress the limits of decency and violate the privacy of any person would amount to an offence under this provision and is punishable with a maximum of 3 years' imprisonment or fine upto Rs. 2,00,000/- or both. Violating privacy includes capturing pictures of the sensitive parts of people when they do not expect that any picture or videos of theirs is captured.

This is a huge issue today and women are predominantly subject to harassment and torture through this crime. There are cases where women are threatened with such videos and photographs and are forced to accede to the demands of the criminals. Such kind of illicit photos and videos are the ones which give rise to pornography and other indecent videos. With the unlimited amount of freedom and exposure given to the youth, such photos and videos are treated as a source of entertainment, giving scant regard to the dignity and reputation of the victim. The worst part is, the Indian society blames and secludes the victim herself and doesn't care to punish the criminal.

Right to privacy by itself is a part of Right to Life and Personal Liberty[3]. Right to life includes right to live with dignity and such dignity will be lost if privacy is lost. There are a number of decisions which reiterate this point. To name a few, R. Rajagopal vs. State of Tamilnadu[4], Kharakh Singh vs. State of Uttar Pradesh[5], People's Union for Civil Liberties vs. Union of India[6] were landmark judgments of the Apex Court in India. The victim and her family are forced to

[1] DurgadassTulsiramSood vs. State AIR 1955 Bom 82
[2] Manish Singla vs. UT of Chandigarh
[3] Article 21 of the Constitution of India
[4] AIR 1995 SC 264
[5] AIR 1963 SC 1295
[6] AIR 1997 SC 568

withdraw their cases against the culprits and the Court also quashes the FIR, considering the future of the victim[1].

The other problem with this provision is that it deals only with obscene or indecent photographs and not with photographs taken by force and photographs misused in other manners. If the photograph or video does not project any private or sensitive part of the body, such a photograph or video will not fall under this section even if it was taken without the consent of the victim or was misused in other undesirable manners[2].

Section 67 provides for the punishment for publishing or transmitting of obscene material in electronic form. The punishment for this offence is two-fold. On first conviction, the punishment is three years' punishment with fine upto three lakhs. On subsequent convictions, the punishment is five years' imprisonment with fine upto ten lakhs. This provision has a wide scope. The word obscene material is subject to judicial interpretation. The word must necessarily be given a wide meaning as it is subject to technological development and introduction of new communication devices. This provision also covers publication in social media. There is difficulty in effective implementation of this provision because the victims go in for compromise easily. Here the victims are not only those who publish and transmit the videos but also those who feature in the video by force or without knowledge. The definition given Webster's Third New International Dictionary for the word 'lascivious' was accepted by the Gujarat High Court[3]. Electronic form is defined under section 2(r) of Information Technology Act. It includes mobile phones, CDs, etc.[4]

The Indian Penal Code also deals with this offence[5]. It deals with the same essentials as that of section 67 of IT Act. It covers every mode of publication other than electronic media. Even the seller of such obscene books and publications is liable to be punished, even if the seller does not know of the book's contents or of the ban on the book[6].

In Chandrakant KalyandasKakodkar vs. State of Maharashtra, the Supreme Court held that the standards of obscenity would differ from country to country depending on the standards of

[1] Sunny Dhiman vs. State of Punjab
[2] Lakshmi Prathapan vs. State of Kerala
[3] Mohammed vs. State
[4] Union Of India vs. Prafulla Kumar
[5] Section 292 of the Indian Penal Code
[6] Ranjit D Udeshi vs. State

morals of contemporary society[1]. The test for obscenity was laid down in Regina vs. Hicklin. The test is whether the tendency of the matter charged as obscene is to be deprived and corrupt those, whose minds are open to such immoral influences, and into whose hands a publication of this sort may fall[2]. The word obscenity was interpreted differently by various High Courts and the Apex Court.

What could be and could not be considered obscene still remains a million dollar question left to the discretion of the judiciary. This could pose problems in delivering justice as the concept of obscenity differs from person to person and when decided by Divisional Benches, would create discrepancies. However, giving one air-tight definition to the term 'obscenity' is next to impossible. It would also result in grave injustice as many acts of indecency or obscenity are prone to be excluded and would prove to be loop holes to the law. The only solution to this is to give an interpretation commonly accepted and fairly justified and that which would facilitate in providing justice to the victim as well as the accused. Easier said, this would prove to be a herculean task as generation gaps and other social stigmas would prove to great hurdles to the effective implementation of these provisions.

Section 67A provides for the punishment for publication and transmission of sexually explicit acts though electronic media. The punishment is imprisonment for five years and fine upto Ten Lakh Rupees. On subsequent repetition of the same offence, the imprisonment is upto seven years and the fine amount remains the same. The interpretation to the term 'sexually explicit act or conduct' is also subject to judicial interpretation.

Child pornography and publication and transmission of electronic data depicting children in sexually explicit acts is an offence punishable under section 67B of Information Technology Act with imprisonment for five years and fine upto Ten Lakh Rupees. On subsequent repetition of the same offence, the imprisonment is upto seven years and the fine amount remains the same. Arjika case was a landmark judgment in this regard, which came before the commencement of the Information Technology Act, which was regarding online child pornography.

[1] AIR 1970 SC 1390
[2] 3 LR QB 360 (1868)

Section 67, 67A and 67B of the IT Act does not apply to publications which are[1]:

1. For public good
2. For bona fide heritage or religious purposes

The terms 'public good' and 'bona fide' are also interpreted by various Courts. The Supreme Court has given two differentinterpretations in two different decisions for the term 'public good'. In Superintendent Central prison, Fatehgarh vs. Dr. Ram Manohar Lohia[2], the Supreme Court held that public order is synonymous to public safety and public tranquility and the lack of disorder, which could include National upheavals such as revolution, civil strife, war, affecting the security of the state. In Municipal Corporation, Raipur vs. State of Madhya Pradesh the same Court removed the negative part of the definition and held that Public order means public safety and tranquility[3].

The intermediaries are mandated to exercise due diligence and care in placing their rules, regulations and conditions of user agreement, which informs the users not to upload, transmit any indecent, undesirable or obscene data. On receipt of any information about such content, the intermediaries shall take immediate action, failing which they would liable under section 67B as co conspirators and abettors.[4]

Section 67C says that intermediaries shall retain information until such time the Central Government directs them to do so. Else they are liable to be punished with imprisonment upto 3 years and fine.

Cyber Crimes Against Property

Section 65 of IT Act deals with tampering computer resources, codes and documents. Intentional tampering, concealing, alteration or destruction of electronic data would attract punishment of imprisonment upto three years or fine upto two lakhs or both. This provision mandates the existence of mens rea to constitute the crime. Cyber crimes against people and government do not give much importance to mens rea. Tampering of police records is also an offence under this

[1]Provisio to Section 67B
[2] AIR 1960 SC 633
[3] AIR 1970 SC 1923
[4] Rule 3 of IT Rules, 2011

provision[1]. Even if the misused data or code is sold to an international client outside the boundaries of India, the accused will be triable in India[2].

Section 66 is a very general provision and covers all computer-related offences. Section 66 provides for the punishment for any for any of the acts mentioned in section 43 of IT Act. The punishment is three years' imprisonment or fine upto Five Lakh rupees or both. Section 43 defines the offence and section 66 is the charging section. Mens rea is an essential component to prove an offence under this provision also.

Section 43 elaborates on the kinds of damages to the computer system. This provision covers the following situations:

i. Unauthorized access
ii. Unauthorized procurement of data or documents
iii. Induction of computer contaminant or viruses
iv. Damage to the hardware
v. Disruption or crashing of computer network or programme
vi. Denial of authorized usage
vii. Abetment or assistance to commit offences under the IT Act
viii. Online payment frauds
ix. Destruction or alteration to any essential information
x. Theft of electronic data or documents

Section 43 uses the words 'fraudulently' and 'dishonestly'. Their definition was adopted from section 23 and section 25 of IPC. However, these words were given more than one interpretation by the Apex Court as well as the various High Courts.

In Kishan Kumar vs. Union Of India, the Supreme Court held that wrongful gain includes wrongful retention and wrongful loss includes being kept out of the property as well as being wrongfully deprived of property[3]. Thus, the expressions get a wider meaning and since it is an

[1] State of Maharashtra vs. Anand Ashok Khare
[2] State of Uttar Pradesh vs Saket Singhania
[3] AIR 1959 SC 1390

inclusive definition, scope for interpretation is also wider.In many other instances, the Supreme Court has accepted the definitions given in IPC for these words.[1]

Section 70 gives the Central Government the power to declare certain computer systems or electronic systems which affects Critical Information Infrastructure as 'protected systems'. Critical Information Infrastructure would include computer resources that, if tampered with, will affect National security, economy, public health and safety. Such systems cannot be accessed without authorization by the Central Government, in writing, through a notification. Any unauthorized access or attempt to unauthorized access to protected systems would attract punishment of imprisonment upto 10 years and fine. In this provision the punishment for the attempt and the commission of the offence is the same.

The Kerala High Court, in Firos vs. State of Kerala[2], has held that section 70 of IT Act is subject to the provisions of the Copyrights Act. The Court said that computer resources can be declared as protected systems only when they are government works as defined under section 2(k) of Copyrights Act. The Government can thus claim copyrights under section 17(d) of Copyrights Act and declare the said software as a 'protected system'. Thus Section 70 will not be in contradiction to the Copyrights Act, but will be subject to the provisions of the Copyrights Act.

Section 71 of IT Act provides for the penalty for misrepresentation. Misrepresentation or suppression of material facts from the Controller or the Certifying Authority for obtaining any licnese or electronic signature certificate is an offence under this provision and is punishablewith imprisonment upto two years or with fine upto one lakh rupees or with both. The Certifying authority may be punished under this provision if he commits this offence against the Controller.

Section 72 provides for the penalty for breach of confidentiality and privacy. Disclosure of information without the consent of the concerned person is an offence under this section punishable with imprisonment upto two years and fine upto one lakh rupees or both.

Section 72A deals with punishment for disclosure of information in breach of lawful contract. When information is given as a part of lawful contract it is supposed to be kept confidential and

[1] B. Suresh Yadav vs. Sharifa Bee, AIR 2008 SC 210; Abdul Fazal Siddiqui vs FatehchandHirawat; (1996) 6 SCC 32
[2] AIR 2006 ker 279

disclosure of such confidential information or trade secrets would attract punishment of imprisonment upto three years or fine upto five lakh rupees or both.

Publishing an electronic signature certificate with false particulars is an offence under section 73. This offence is punishable with imprisonment upto two years or fine upto one lakh rupees or both. False details about the certifying authority, false information about the acceptance by the subscriber and non disclosure of the suspension or revocation of the signature are covered under this provision.

Publication of electronic signature certificates for fraudulent purposes is also an offence under section 74 with the same punishment as provided under section 73.

Conclusion

Cyber world poses a lot of risks to persons and property. Much as it makes life easier and transactions simpler, it also puts personal information and details at risk. Misuse of such information would prove to be harmful even without our knowledge. Protection and security of the public is in the hands of the public.

Legislations can help only when the criminal is caught, which seldom happens. Protecting information is the responsibility of the people themselves. This will go a long way in preventing cybercrimes. Avoid giving phone numbers a long way in preventing cybercrimes. ATM PIN numbers should not be shared with anybody. Unnecessary calls asking for personal details, account details, etc must be ignored. Posting pictures and whereabouts in social media must be avoided to the maximum. Since Facebook, Instagram, etc are public forums, information posted there can reach anybody in the world. Passwords and user names are given for a purpose They are not meant to be shared.

Phone numbers and e mail ids must not be shared in any public forum as far as possible. Installing unnecessary applications and allowing them to access mobile contacts and galleries can also prove to be dangerous. The people who use the information and trade this information are hard to trace. The only way to stay safe is to prevent information from leaking. Once information stops leaking, cybercrimes will reduce. Cyber security will increase and the cyber world will only be used for the right purposes.

Volume 2 | Issue 2 | December, 2018 | ISBN 978-93-5311-594-4