Cyber Law and its Importance: Case on Social Media and ICICI Bank

Bijal Zaveri and Prashant Amin***

ABSTRACT

The increasing changes in digital technology have initiated many benefits for businesses, and individual consumers worldwide. On the other hand, some people are always looking for new ways of negatively and illegally exploit the weaknesses of digital technology. With many Information technology specialists spread across India, the Cybercrimes and Fraud have been at the highest peak, and frequently experienced in the recent digital era than ever before.

Even if the rate of cybercrimes has increased a lot in the recent era, the government of India has created laws prohibiting such crimes, and imposing heavy punishments for the involved criminals. This article is meant to briefly talk about cybercrimes and assert some of the key cyber laws in India.

Keywords: *Cybercrimes; Cyber laws; Digital technology.*

1.0 Introduction

Normally, criminals are not necessary very educated and skilled people, but for cybercrimes, a criminal has to be incredibly skilled in Information Technology to be a professional hacker. On the other hand, some cybercrimes don't require many skills except the ability to use digital tools and internet. Ranging from simple cybercrimes that can be performed by anyone using internet, to sophisticated bank heists and governments private files illegal access and sharing, cybercrimes are notorious crimes that hurts the society in many ways.

According to Oxford dictionary, cybercrimes are defined as "the criminal activities carried out using a computer and internet" (oxford dictionary, 2018).

According to Techopedia.com, cybercrimes include hacking, and spamming but also represent all criminal offenses done with the use of computer and internet like cyber terrorism, cyber bullying, phishing, child pornography, scams, defamation, identity theft, etc. (Techopedia.com,2018).

On the other hand, Cyber laws are defined as "legal laws that are meant to deal with cyberspace, internet, and all related crimes and issues" (computerhope.com, 2018).

The following is a brief description of cybercrimes, and some key punishments found in the Indian Government IT Act of 2000.

2.0 Literature Review

In the following part of this article, we are going to point out the major forms of cybercrimes.

2.1 Cyber terrorism

According to Techopedia.com, cyberterrorism is defined as the use of internet to conduct premeditated cybercrimes involving deliberate hacking, disruption of IT networks, creating and sending viruses, phishing, web jacking etc. These crimes have to be performed on a large scale, and results in chaos, panic, and disturb the general public order. (Techopedia.com, 2018). Cyber terrorists do so by arrogance or pursuing their own monetary gains and interests,

**Corresponding Author; Dean, Department of Faculty of Management Studies, Parul Institute of Management Research, Parul University, Vadodara, Gujarat, India. (Email: bijal.zaveri@paruluniversity.ac.in)*

***Assistant Professor, Department of Faculty of Commerce, M. S. University, Vadodara, Gujarat, India. (Email: prashantbijalamin@gmail.com)*

and they attack government institutions, banking and financial institutions, hospitals, nonprofit organizations, media corporations, trading and manufacturing corporations etc. Hackers should know that they can become cyber terrorists if whatever they are doing negatively affect many people at a large scale and cause panic and chaos in the society.

On the other hand, even terrorists' organizations are switching their activities on the web because of the easy accessibility, anonymity of terrorists, the large number of people or entities that can be attacked, the chaos that it creates, relatively cheap compared to traditional forms of terrorisms, recruiting, coordination of attacks, worldwide targets etc.

2.2 Cyberattacks

According to Hathaway Oona and her colleagues in their article called "*the Law of Cyber-Attack*", cyber-attacks are defined as deliberately exploiting computer systems, Networks, or systems that uses Technology. (Hathaway et all, 2012)

Cyber-attacks might consist of:

Identity and information theft, privacy invasion: Cybercriminals steal other people's identities; and collect private and personal information for their personal monetary gains. This malpractice starts by violating the victim's privacy, and goes up to the extent of stealing his bank and credit cards details, accessing his email accounts, gaining access to his ATM codes and passwords etc.

Malware, viruses, malicious software, Trojans, phishing, illegal use of web browsing data, instant messaging abuse etc.: cybercriminals also engages themselves in the mentioned crimes and they do so to gain access of the users web history, illegal data collections, login passwords and credentials, etc. phishing consists of deluding victims by using false profiles and ask victims to share their personal details by making them believe that they are dealing with a reputable organization that they know very well. For example, someone can create false E-mail Id, use phone calls, or social media contacts as an Apple company employee, and start to sell false promises to victims.

2.3 Invading financial institutions its systems

Cyber criminals have been also targeting financial institutions and trying to steal as much money as they can, or at least disturb and confuse their system. they hack into baking data storage and steal personal client information, changes the codes and move money to ghost accounts, etc. they also steal information regarding bank debit and credit cards, and steal from the card owners. On the other hands, banks and financial institutions have understood that they need to reinforce their system's security and protect their client's private and confidential information maximally to avoid cyber-attacks.

2.4 E-commerce cybercrimes, frauds and trafficking

Even though E-commerce has provided an opportunity for different business across the globe, some individuals hide themselves behind the unregulated selling platform, and make false claims about the products and services they pretend to sell. Once they have got customers, who pays online for the inexistent products, the business is nowhere to find and criminals get away with large sums of stolen customers money. Many of them also have become experts in tax evasion, whereby, they sell products and services but do not pay taxes, by using unregistered companies, misrepresentations and manipulation of prices, fake documents and bills etc. traffickers also have found a safe haven with digital technology. They can traffic different illegal products like, weapons, drugs, elephant teeth, precious minerals and even human beings.

Many of the digital businesses in E-commerce fail to protect their client's personal data, or misuse it for their personal gains, spamming, etc.

2.5 Copyrights, trademark infringements and piracy

It is also a crime to illegally use someone else's trademarks or violate copyrights on his products and services. Cybercriminals take advantage of the anonymity, and lack of vigorous control of online markets, and sell different products and services illegally developed or acquired without owner's consent. Examples here include downloading and selling music movies, books duplicating someone else's products, brands imitation, etc. Piracy is also another crime that is manifesting itself in this recent digital era, and it largely includes software piracy, duplicating digital tools, stealing devices technology, etc.

2.6 Defamation and cyber stalking

Many people hidebehind the unanimity of internet and use it wrongfully by demeaning other people. They do so by making false claims that are meant to make someone loose dignity and credibility in the eyes of the society.

The victim is falsely accused on the web and social medias, and not only he is embarrassed in front of his family and friends, coworkers, people in the neighborhood, he might lose credibility national wide, but if he cannot properly defend himself, he loses his good image.

This also goes along with people sending threatening messages, emails, or phone calls, following someone's movement, or openly criticizing or demeaning him.

2.7 Child sexual abuse, adult pornography and sexual content

Even though some countries tolerate adult pornography; child pornography is strictly prohibited in many countries, and punishable by the law. This doesn't stop cyber criminals, to produce, distribute and sell child pornography on internet. This goes along with illegal production and sharing of sexual content to different users of the internet even if they didn't sign up for it. In the past many people have experienced the anonymous hackers who randomly posted nude photos and pornography videos on random people's Facebook accounts.

Pornography and sexual cybercrime are popular among the youth and different cyberspace users, where they immorally use its content to disturb the public and ethical order of the society. In India, it is strictly prohibited to share such content, and failure to do so is highly punishable by the law.

The list of cybercrimes is long, but above are just some common crimes, and the following part explains what shall be done by the users to minimize the risks of being attacked.

3.0 Cyberspace User's Safety

Cyberspace users shall be informed about the dangers that they face since cyber criminals always work hard to find the next victim. The following are some of the important strategies that users might adopt to minimize the risks of becoming cybercrimes victims.

The following are some of the tips for better cyber security:

Strong password and codes: some people use short and easy password that can be easily hacked. They use their birthdates, parts of their names or children's names, pets etc.

Instead of having short and easy password, it is always advised to have long passwords, and must include capital letters, symbols and signs to make it stronger. In addition to that, users shall never share their passwords to friends or family, or allow different website to save password if they are not sure about their security features. A stronger password or bank card code is very hard to hack.

System updates*:* cyber users should be advised that they better update their computer systems and anti-viruses regularly. Hackers and cyber criminals are always trying to find new ways of invading people's privacy, but they reach a dead end if your system is highly protected

***Avoid visiting unsecured or untrusted websites*:** with the internet widely available and used by many people around, some users find themselves visiting untrusted websites, with popups that install viruses in thickener system and make it vulnerable for cyber-attacks.

These untrusted websites include pornography websites, online movie streaming websites, online gambling and lottery websites, dating websites, etc. cyberspace users should avoid clicking on pop-ups, suspicious banners and unclear external links since most of them contain viruses and malicious software that can make them vulnerable to cyber attacks

Purchase from trusted online retailers only*:* well-known and reputable online retailers have developed security measures that allow them to protect their client's data against cyber-attacks. If one has to make online payments, they shall do so only on the trusted websites, to avoid any identity theft or their payment details to be stolen. They can also consider using online payments special methods like PayPal to minimize the risks or choosing the cash on delivery option whenever applicable.

Only share necessary information*:* cyber users shall be advised that they must consider sharing necessary rather than sensitive information. Sharing all information creates vulnerability and once found in wrong hands, that information can be wrongly used to harm someone in many ways. People should learn to be reserved, and avoid sharing anything and everything online even when they have been guaranteed the security.

4.0 Some Cyber Laws, and Corresponding Punishment in India

According to computerhope.com, cyber law is created to protect cyber users from cyber criminals. (Computerhope.com, 2018). This is meant to protect people from the consequence of improper use of digital technology by cybercriminals, and just like any other law, impose punishments for committed crimes. It serves as guidelines and disseminates what practices are morally and ethical acceptable, and set the boundaries by which cyber users shouldn't cross. The following are some of the key paragraphs on cyber law in India, commonly known as Information Technology ACT, passed in 2000.

Hacking with computer system: As described in section 65 of the Indian IT act, anyone found guilty can be sentenced up to 3 years imprisonment or/ and be fined up to 500,000₹.

Cheating using a computer resource*:* found in the 65D section of the Indian IT act, anyone found guilty can be jailed up to 3 years or/and pay a fine of up to 100,000₹

***Publishing private Images of others*:** found in the section 66E of the Indian IT act, it includes taking, distributing and sharing other people's private parts. Once found guilty, a criminal can be jailed up to 3 years or/and imposed a fine of up to 200,000₹

***Cyber terrorism*:** found in the section 66F, it includes anyone who deliberately performs a cyber-act that threatens the unity, integrity serenity and security of the government of India. Once found guilty, one can be jailed for life.

Causing or publishing obscene information in an electronic form: Found in the section 67 of Indian IT act, and anyone found guilty can face 5 years imprisonment or/ and up to 1,000,000₹of fines.

Publication of sexual images and videos: found in the section 67A of the Indian IT act, anyone found guilty can be imprisoned for 7 years or/ and 1,000,000₹ of fines and penalties

Predating minors online, creating or publishing child pornography: as found in the section 67B of the Indian IT act, a guilty criminal will face 5 years imprisonment or/and up to 1,000,000₹ in fines for the first time, and if he does it again, he can face 7 years imprisonment or/and up to 1,000,000₹ in fines and penalties

Wrongly Using someone else's password: as found in in section 66C of the Indian IT act, it includes stealing and using his identity, online signature etc. the guilty criminal might face up to 3 years imprisonment or/ and up to 100,000₹offines and penalties.

Tampering with computer source documents: as found in the section 65 of Indian IT act, it includes concealing, destroying or altering computer source code, computer system, or computer networked. guilty criminal can face up to 3 years imprisonment or/and up to 200,000₹ in fines and penalties

Receiving stolen computer or digital device: As found in the section 66B of the Indian IT act, anyone found guilty can face up to 3 years imprisonment or/and up to 100,000₹ in fines and penalties.

5.0 Case Studies

5.1 Phishing attack against ICICI bank

ICICI bank profile: According to ICICI Bank website, ICICI is the largest private bank in India, with over 4,867 branches and 14,367 ATMs nationwide. Founded in 1994, this bank is very profitable with consolidated assets valued at ₹11,242.81 billions, Which is approximately $172.5 billion, and last year, this bank made a net profit of ₹66.77 billions, which is approximately $1 billion. (icici.com, 2018)

Description of the phishing case: Cyber criminals targeted this bank and its customers by sending fake E-mails but disguised as official bank Employees, and sent E-mails to the Bank customers. In those Emails, they were asking the customers of this bank to update their banking details and their personal financial information.

According to www.blog.comodo.com, they were sending E-mails to the victims, containing links that they had to follow and fill their banking details pretending to be operated by ICICI bank. (www.blog.comodo.com, 2018). After clicking to the link, they were redirected to another page that looked genuine, and they were supposed to fill the required information as they were asked.

They were asked to share their bank card details, pin numbers, transaction passwords, email ID, etc.it is obvious that by revelling such sensitive and private financial information, the victims though that they are dealing with their bank, but in reality, with a bunch of cybercriminals ready to misuse the received information and steal from many victims as they possibly could. (www.Indiaforensic.com,2018)

Bank official comments: Luckily, ICICI bank has strong security features. According to www.blog.comodo.com, ICIC bank have a multi-level security system which is designed to prevent cybercrimes including phishing. They assured their clients that even though there has been this attack, they shouldn't worry since their accounts are secure, and that they have efficiently solved the issue. They urged the customers to be vigilant and report any suspicious Email information update requests, and assured them that ICIC bank doesn't conduct or ask any personal or banking information via email. They advised their clients to never share with anyone their banking, and personal information in any situation.

5.2 Orkut fake profiles cases

Orkut description: www.Orkut.com was a social networking website just like Facebook, and it was meant to connect people with the same interests, and allow them to easily interact with each other. Users were required to create profiles and interact with each other, make friends, date, share content, etc. According to www.Wikipedia.com, Orkut.com was owned by Google company, but has been dissolved in 2014 due to different legal issues the company faced, including too many fake profiles, failure to protect users' privacy, copyrights problems etc

Description of the cases: Orkut has been characterised by a very high number of fake profiles, created by many users for different reasons. According to www.cyberlawsindia.net, the most popular case of fake profile was the one created by a 19 years old student who created a fake profile of a girl classmate, describing her in a defamatory way. (www.Cyberlawsindia.net, 2007).

According to www.scribd.com, this fake profile of the girl was created with correct names, home address, and phone numbers, describing her as a girl who is interested in having sexual relations with anyone who wish so. (www.scribd.com, 2018). This created a very big case of harassment since this girl was being called all the time by different people who believed that what was portrayed on Orkut was true, and wanted to have sexual relations with her. After the girl contacted the police, this fake profile was tracked and linked to his class mate Abhishek and he was arrested by the police.

This not the only fake profile case that created controversial debates. Many more fake profiles have been identified and misused for personal interests of the creators. They did so for many reasons such as revenge, defamation, demeaning someone and make him loose his dignity in the society, jealousy, etc. fake profiles on Orkut were also linked to individuals who were advocating for racial hate, sexual content and pornography, Trickery, scamming etc

In many occasions, Orkut was accused of lack of control and allowing fake profiles to be created and to fully operate. According to www.theeconomictimes.com, Google, who owned Orkut, was fined 500,000$ for allowing fake profiles of the formula one racer Rubens Barrichello in Brazil where it operated for many years before its catastrophic downfall. It was not only one fake profile of this man, but more than 300 fake profiles were registered under the names of Rubens Barrichello and fully operational. Many issues like this marked the beginning downfall of Orkut Company and lead to its complete closure in 2014.

6.0 Conclusion

As digital technology continues to spread across India and worldwide, many people are using it for better, and changes their personal lives, business practices, economic development etc. On the other hand, cyberspace is not a perfect system which is hard to monitor and control everyone's activities. Cyber criminals choose to go against the laws governing cyberspace due to monetary profits and immoral gains but they do so on their own risks. Indian government has passed the Information Technology act in 2000, and it has been updated many times, but meant to provide cyber laws, that should be followed by Indians for fair, moral, ethical and legal use of cyberspace. Failure to comply with it results in punishment up to life imprisonment and up to 1,000,000₹ in fines and penalties depending on the nature of the crime.

7.0 Future Work Proposal

Above are just some of the sections of the Indian IT Act of 2000, but there are more sections to be analyzed like section 72 regarding the breach of privacy and confidentiality, Section 77A regarding compounding crimes, Section 85 regarding corporate offences, Crimes committed outside of India and many more.

References

Blog.comodo.com (2018), "*FROM THE COMODO LABS: New Phishing attack Targeted ICICI Bank (Update Includes ICICI Commentary)"*https://blog.comodo.com/it-security/new-phishing-attack-targets-icici-bank/ Accessed on September 16th 2018.

English Oxford living Dictionaries (2018), "*cybercrime definition*", https://en.oxforddictionaries.com/definition/cybercrime *accessed on September 10th 2018.*

Hathaway, Oona et al, (2012). "*The Law of Cyber-Attack*", Faculty Scholarship Series. https://www.researchgate.net/publication/251334352_The_Law_of_Cyber-Attack accessed on September 10th 2018

ICICI BANK (2018) "ICICI bank: about us" https://www.icicibank.com/aboutus/about-us.page accessed on September 16th 2018.

Muthukmaran, B, (2008) "Cybercrime *scenario in India*" Criminal Investigation Department Review.

ndiaforensic.com (2018), "*ICICI bank Phishing*" http://indiaforensic.com/icicihack.htm accessed on September 16th, 2018

Techopedia.com (2018) "cybercrime *definition*" https://www.techopedia.com/definition/2387/cybercrime*Accessed on September 10th 2018*

www.Computerhope.com*, (2018) "cyber law definition"https://www.computerhope.com/jargon/c/cyber-law.htm Accessed on September 10th 2018*

www.Cyberlawsindia.com(2007) "*Cyber laws cases, orkut: the new danger*"http://www.cyberlawsindia.net/cases4.html Accessed on September 16th 2018

www.do.gov.in, (2000). "*The Information Technology Act, 2000*" Ministry of Law, Justice and company affairs (Legislative department), http://www.dot.gov.in/sites/default/files/itbill2000_0.pdf Accessed on September 8th 2018.

www.TheEconomictimes.com(2009) "*Google fined $500 000 for fake Barrichelloorkut profiles*"https://economictimes.indiatimes.com/google-fined-500000-for-fake-barrichello-orkut-profiles/articleshow/5218239.cms Accessed on September 16th 2018

www.Wikkipedia.com, (2018) "*Information Technology act, 2000*" https://en.wikipedia.org/wiki/Information_Technology_Act,_2000 accessed on September10th 2018.