665

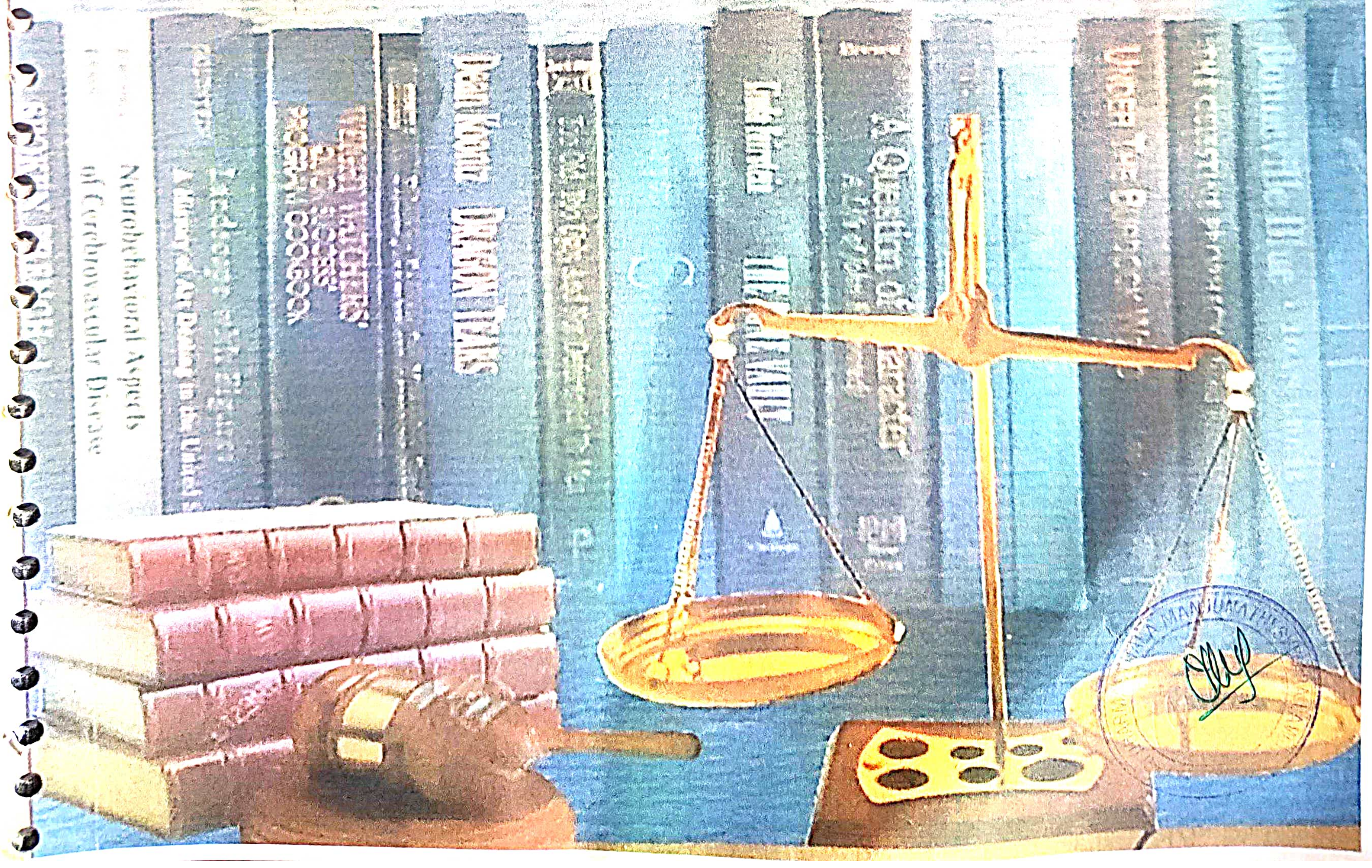
Shri Dharmasthala Manjunatheshwara Law College
Centre for Post Graduate Studies & Research in Law
MANGALURU - 575 003.
(NAAC Re-accredited B++ CGPA 2.9)

Sponsored by :
Shri Dharmasthala Manjunatheshwara Educational Society (R.), Ujire, D.K.

Legal opus

(Peer Reviewed Journal)

Issue No. 13 June 2020



666

LEGAL OPUS

Issue 13 | June 2020

96
667

IDENTITY THEFT A CYBERCRIME

Swathi B. *

Introduction

Human life is made easy day by day with the touch of technology in every field. In this aspect, internet plays a major role. It has it's influence in almost every bit of human life. In this era people completely rely on internet for everything, be it communication, education, business, shopping,moneytransactions,travel bookings etc. One can undoubtedly say out of all the technological advancement internet has taken charge over human life.

Every coin has two sides likewise internet as a technology too proves to be a boon as well as a bane in the present day society. The influence of internet in every sector has paved it's way to innumerable criminal activities in cyberspace.

Meaning

CYBER"is a prefix that means "computer" or "computer network," as in cyberspace, the electronic medium in which online communication takes place[1]. **CYBERSPACE** is a place that is not real, where electronic messages exist while they are being sent from one computer to another. **CYBERSPACE CRIME** is any crime that takes place online or primarily online.Cyber crime is an activity done using computers and internet. We can say that it is an unlawful act wherein the computer is either a tool or target or both.

Cybercrime can range from security breaches to identity theft[2].

Categories of Cybercrime : There are three major categories of cyber crimes:

1. Crimes Against People
2. Crimes Against Property
3. Crimes Against Government

Cyber Theft

"The fantastic advances in the field of electronic communication constitute a greater danger to the privacy of the individual."[3] Cyber theft is one such crime which manipulates personal information.

* Visiting Faculty, SDM Law College, Mangaluru.

[1] https://www.webopedia.com

[2] https://us.norton.com

[3] Quoted by Earl Warren in the privacy guru.com

Cyber theft is a part of cybercrime which means theft carried out by means of computers or the Internet.The most common types of cyber theft include identity theft, password theft, theft of information, internet time thefts etc. This paper mainly throws light on one type of cyber theft that is identify theft.

Identity Theft

Identity theft pertains to illegally obtaining of someone's personal information which defines one's identity for economic benefit. It is the commonest form of cyber theft. Identity theft can take place whether the fraud victim is alive or deceased.

Various techniques of Identity Theft

There are various techniques through which data theft could be committed and personal information could be procured from electronic devices. These are as follows:

Hacking- The persons known as hackers unscrupulously break into the information contained in any other computer system. It is a method wherein viruses or worms like malware divert information from another computer system by decrypting it to the hacker who after obtaining the information either use it themselves or give it to others to commit fraud using such information.

Phishing- It uses fake email-ids or messages containing viruses affected websites. These infected websites urge people to enter their personal information such as login information, account's information.

E-Mail/SMS Spoofing- The spoofed e-mail is one which shows its origin to be different from where it actually originated.

Carding- The cyber criminals makes unauthorized use of the ATM debit and credit cards to withdraw money from the bank accounts of the individual.

Vishing- The cyber-criminal calls the victim by posing to be a bank representative or call center employee, thereby fooling them to disclose crucial information about their personal identity.

Theft of intellectual property- Intellectual property (IP) theft is defined as theft of material that is copyrighted, the theft of trade secrets, and trademark violations etc. One of the most commonly and dangerously known consequence of IP theft is counterfeit goods and piracy[4]

By targeting children online-Children can easily share their passwords without realizing its consequences[5].

Laws governing Identity Thefts in India

The crime of identity theft consists of two steps:

- Wrongful collection of personal identity of an individual

[4] www.mondaq.com. (Article on Cyber- Theft A Serious Concern in India by S.S.Rana&co.last updated 28 Feb 2019)

[5] www.blogipleaders.in

- Wrongful use of such information with an intention of causing legal harm to that person information.

1. Indian Penal Code, 1860

Although by its name, identity theft is a kind of theft of specific kind involving user data, it is not governed by Section 378 (theft) of the IPC. This is because it caters to only movable property or such property which is capable of being severed from the earth and is tangible in nature (Section 22 of IPC).

However an identity theft involves both theft and fraud, therefore the provisions with regard to forgery as provided under the Indian Penal Code, 1860 (IPC) is often invoked along with the Information Technology Act, 2000.

Some of the Sections of IPC such as forgery (Section 464), making false documents (Section 465), forgery for purpose of cheating (Section 468), reputation (Section 469), using as genuine a forged document (Section 471) and possession of a document known to be forged and intending to use it as genuine (Section 474) can be coupled with those in the IT Act.

According to Ministry of Electronic and Information Technology, Government of India, Cyber Laws yields legal recognition to electronic documents and a structure to support e-filing and e-commerce transactions and also provides a legal structure to reduce, check cyber crimes.

Importance of Cyber Law:

- It covers all transaction over internet.
- It keeps eyes on all activities over internet.
- It touches every action and every reaction in cyberspace.[6]

2. The Information Technology Act, 2000 (IT Act)

IT Law also called Cyber Law is the law regarding Information-technology including computers and internet. It is the main act which deals with the legislation in India governing cybercrimes.It is related to legal informatics and supervises the digital circulation of information, software, information security and e-commerce.

Although, its aim was to mainly recognize e-commerce in India and it did not define cybercrimes as such. Before its amendment in 2008, Section 43 of the Act could be used to impose civil liability by way of compensation not exceeding one Crore for unauthorized access to a computer system or network (Subsection a) and for providing assistance to facilitate such illegal act (Subsectiong).

Section 66 of the Act only pertained to cybercrime of hacking wherein some destruction, deletion, alteration or reduction in the value of computer resource attracted penal sanctions. If a person obtained identity information from the computer stealthily without causing any changes in it whatsoever, this provision could not be used.

[6] https://www.geeksforgeeks.org.

3. The Information Technology Act, 2008

The term identity theft itself was used for the first time in the amended version of the IT Act in 2008

Section 66 criminalizes any fraudulent and dishonest conduct with respect to Section 43 of the same Act.

Section 66 (A) which is now held to be unconstitutional, covered the crimes of Phishing. **Section 66 B** pertains to dishonestly receiving any stolen computer resources.

Section 66 C specifically provides for punishment for identity theft and is the only place where it is defined.

Several other provisions inserted in the amendment include punishment for violation of privacy and for cyber terrorism. Women and children have also been provided protection under Section 67 A and 67 B of the Act. Further, stronger laws have been formulated with respect to the protection of "sensitive personal data" in the hands of intermediaries and service providers (body corporate) thereby ensuring data protection and privacy. The ambit of sensitive personal data is defined by the IT Rules, 2011 as well as The Data Protection Bill, 2018 to mean password, financial information, physical, physiological and mental health condition, sexual orientation, medical records and history, and biometric information. Hence, depending upon the method using which identity theft has been committed, the aforementioned laws can be applied.

Combating Cyber Crime

To combat cyber crimes, the CBI has in place the following special units & structures:

(i) Cyber Crimes Research and Development Unit (CCRDU);

(ii) Cyber Crime Investigation Cell (CCIC);

(iii) Cyber Forensics Laboratory; and

(iv) Network Monitoring Centre.

According to The Information Technology Act of India, when a cyber crime has been carried out, it has a worldwide purview and jurisdiction. Furthermore, a complaint or a grievance can be recorded at any cyber-crime cell in any of the cities. A person may need to give a name, street address and a phone number alongside an application letter headed to the respective person heading the cyber-crime cell when recording a complaint with the cyber-crime cell. A person must give specific documentation with a specific end goal to enroll a complaint with cyber-crime cell. List of records change with the kind of cyber-crime activity and differs from crime to crime basis.[7]

[7] http://www.ipleaders.in

Cyber Crime Identity Theft Cases

Pune Citibank MphasiS Call Centre Fraud

In this case, ex-employees of MphasiS Ltd cheated US customers of Citibank with around Rs. 1.5 crores. Unauthorized access to the personal information in the Electronic Account Space of the customers was used to commit this fraud.

Under the Information Technology Act, 2000 use of electronic documents is considered a crime when there is the use of 'written documents', 'breach of trust', 'cheating', 'conspiracy', etc. So this is considered as an offense under Section 66 and 43 of the Information Technology Act, 2000 and the people are liable for imprisonment and fine and they must pay damages to the victims.

Sony Sambandh Case

In this case, Sony India Private Ltd filed a complaint against Non-Resident Indians. The website Sony Sambandh helped them to send Sony products to their friends and family in India after paying online.

It all started when Barbara Campa gifted a Sony Colour Television and a cordless headphone to ArifAzim in Noida. She completed the payment through a credit card, After the completion of all the procedures, the company delivered the items to ArifAzim. Later, the credit card company informed the company about the transaction. They told that the real owner of the credit card had declined about the purchase and claimed the transaction unauthorized.

The company filed a complaint at the Central Bureau of Investigation under Section 418, 419 and 420 of the IPC. After investigation, ArifAzim was arrested and he told that during his job at a call center he gained access to a credit card number and he misused it.

This was India's first cybercrime conviction in 2013 and CBI recovered the headphones and television. The CBI proved the case with evidence and the accused admitted his guilt. The Court accused Arif under Section 418, 419 and 420 of the IPC and it showed leniency towards the boy as he was just a young boy of 24 years and a first-time convict by releasing him on probation for one year.

State of Tamil Nadu vs. SuhasKatti

This case is important in cyberlaw cases as the judgement of this case arrived under 7 months. In this case, a man who was a known family friend of a divorced woman was posting obscene, defamatory and demeaning messages about the woman. He was sending emails to the woman to gather information through a fake account in the name of the victim. As a result, many unreasonable phone calls were received by the woman in the belief that she was soliciting.

In February 2004, the woman filed a complaint and the police found the man and arrested him in the next few days. The accused wanted to marry the lady rather she married another person which later ended up in a divorce. This made the accused trying to contact her again. She again rejected him which forced the accused to start harassment through the internet.

The accused was charged under Section 67 of the Informational Technology Act, 2000 and Sections 469 and 509 of the IPC. The argument of the defense stated that some of the documentary evidence present here are not qualified as evidence under Section 65B of the Indian Evidence Act and all the emails could be spread by her ex-husband and her ex-husband is trying to frame the accused. Rather, the Court hung on the main witness, the cybercafe owners, and all the evidence.

As a result, the Court found the man guilty and charged him with imprisonment and fine both. This is the first case ever convicted under Section 67 of the Information Technology Act, 2000.

Cyber Attack on Cosmos Bank

In August 2018, there was a cyberattack on the Pune branch of Cosmos Bank which drained around Rs. 94 crores. The attackers hacked into the main server and transferred the money to a bank in Hong Kong and they also tracked the details of various Visa and Rupay debit cards.

The hackers found and used a link between the centralized system and the payment gateway was compromised, that means both bank and account holders were unaware of the money being transferred.

This attack was huge and one of its kind as the first malware which attacked ended all the communication between the payment gateway and the bank. This attack caused a lot of damage as there were 14,000 transactions across 28 countries using 450 cards and 2,800 transactions using 400 cards in India.

Prevention of cybercrimes

Computer users can adopt various techniques to prevent cybercrime.

- Computer users must use a firewall to protect their computer from hackers. Most security software comes with a firewall. Turn on the firewall that comes with their router as well.
- Computer users are recommended to purchase and install anti-virus software such as McAfee or Norton Anti-Virus. AVG offers free anti-virus protection if they do not want to purchase software.
- It is advised by cyber experts that users must shop only at secure websites. Look for a Truste or VeriSign seal when checking out. They should never give their credit card information to a website that looks suspicious or to strangers.
- Users must develop strong passwords on their accounts that are difficult to guess. Include both letters and numerals in their passwords. They must continuously update passwords and login details. By changing login details, at least once or twice a month, there are less chances of being a target of cybercrime.

- It is suggested to monitor children and how they use the Internet. Install parental control software to limit where they can surf.
- Make sure that social networking profiles such as Facebook, Twitter, YouTube, MSN are set to private. Check their security settings and be careful what information users post online. Once it is on the Internet, it is extremely difficult to remove.
- Secure mobile devices. More often than not, people leave their mobile devices unattended. By activating the built-in security features, they can avoid any access to personal details. Never store passwords, pin numbers and even own address on any mobile device.
- Protect Data to avoid criminals to hack. Use encryption for most sensitive files such as tax returns or financial records, make regular back-ups of all important data, and store it in a different location.
- Users must be alert while using public Wi-Fi Hotspots. While these access points are convenient, they are far from secure. Avoid conducting financial or corporate transactions on these networks.
- Protect e-identity. Users must be careful when giving out personal information such as name, address, phone number or financial information on the Internet. Make sure that websites are secure.
- Avoid being scammed: It is suggested that users must assess and think before they click on a link or file of unknown origin. Do not open any emails in inbox. Check the source of the message. If there is a doubt, verify the source. Never reply to emails that ask them to verify information or confirm their user ID or password.

There are some warning signs or indicators that people must know and should always keep in mind to prevent themselves from Identity theft:

- Unexpected verification call from the bank
- A warning or notice from the bank
- Unexplained entries in your credit report
- Small debits in the bank statement
- Unfamiliar purchases in the card statement
- Receiving any receipt or bill for a service you don't have

These indicators might help you from identity fraud.[8]

[8] www.blogipleaders.in

Conclusion

Cyber crimes are increasing day by day and with the increase in the number of frauds and cyber related crime, the government is coming up with refined regulations to protect the interest of the people and safeguard against any mishappenning on the internet. Further, stronger laws have been formulated with respect to protection of "sensitive personal data" in the hands of the intermediaries and service providers (body corporate) thereby ensuring data protection and privacy[9].

Prevent the security breach by keeping the data out of reach. So it is not only the police the public too has equal responsibility to take care in matters of online transactions by following basic rules of keeping them safe during the process.

* * * * *

[9] www.mondaq.c

675

Shri Dharmasthala Manjunatheshwara Law College

Centre for Post Graduate Studies & Research in Law

MANGALURU - 575 003.

Rs. 250/-