INTERNATIONAL JOURNAL OF CRIMINAL JURISPRUDENCE

VOLUME 1 AND ISSUE 1 OF 2023

INSTITUTE OF LEGAL EDUCATION

International Journal of Criminal Jurisprudence

(Free Publication and Open Access Journal)

Journal's Home Page – https://ijcj.iledu.in/

Journal's Editorial Page - https://ijcj.iledu.in/editorial-board/

Volume 1 and Issue 1 (Access Full Issue on - https://ijcj.iledu.in/category/p-volume-1-and-issue-1-of-2023/)

Publisher

Prasanna S,

Chairman of Institute of Legal Education (Established by I.L.E. Educational Trust)

No. 08, Arul Nagar, Seera Thoppu,

Maudhanda Kurichi, Srirangam,

Tiruchirappalli – 620102

Phone : +91 94896 71437 - info@iledu.in / Chairman@iledu.in

INTERNATIONAL JOURNAL OF CRIMINAL JURISPRUDENCE

(P) Volume I and Issue I of 2023

ISBN - 978-81-960702-2-9

Published by

Institute of Legal Education

https://iledu.in

A COMPARATIVE ANALYSIS OF INDIAN AND INTERNATIONAL JURISPRUDENCE ON IDENTITY THEFT

Author - ABHAY RAJ SINGH, STUDENT at AMITY LAW SCHOOL, AMITY UNIVERSITY, LUCKNOW.

Best Citation - ABHAY RAJ SINGH, A COMPARATIVE ANALYSIS OF INDIAN AND INTERNATIONAL JURISPRUDENCE ON IDENTITY THEFT, INTERNATIONAL JOURNAL OF CRIMINAL JURISPRUDENCE, 1 (1) of 2023, Pg. 21-27, ISBN (P) - 978-81-960702-2-9.

ABSTRACT

Identity theft is a growing menace in the digital era and has emerged as a global problem. Unauthorized access to an individual's personal information, such as financial details, their social security number, or government identification, is a violation of their privacy and can cause severe harm to the victim. This paper explores the concept of identity theft, its legal framework in India and other countries, and the challenges in combating this crime. The paper examines the legislative measures in place to prevent and punish identity theft, the judicial approach to the crime, and the role of law enforcement agencies in addressing identity theft. Finally, the paper recommends measures to strengthen the existing legal framework and enhance the effectiveness of the criminal justice system in combating identity theft.

KEYWORDS

Identity theft, identification, Information Technology (Amendment) Act, 2008, Hacking, Phishing, Pharming, Skimming, Vishing, Victim, Information Technology Act, 2000, Cybercrime, Cybercriminals, Punishment, Convention, Anonymization, Investigation , Encryption Technology.

INTRODUCTION

Identity theft refers to the act of stealing an individual's personal information, which can then be used for fraudulent purposes. Unauthorized access to an individual's personal information, such as financial details, their social security number, or government identification, is a violation of their privacy and can cause severe harm to the victim. The consequences of identity theft can range from financial loss to reputational damage, and in extreme cases, it can lead to criminal activities such as money laundering, terrorism financing, and human trafficking.

The rise of the internet and the digital revolution have made it easier for identity thieves to access personal information. The anonymity provided by the internet has made it more difficult to detect and prosecute identity thieves. The problem of identity theft is not limited to a particular region or country, but it has emerged as a global issue that requires a coordinated response.

The objective of this paper is to examine the legal framework for combating identity theft in India and other countries and to analyze the effectiveness of the criminal justice system in addressing this crime.

INTERNATIONAL JOURNAL OF CRIMINAL JURISPRUDENCE

(P) Volume I and Issue I of 2023

ISBN - 978-81-960702-2-9

Published by

Institute of Legal Education

https://iledu.in

WHAT CONSTITUTES IDENTIFICATION ACCORDING TO LEGAL GUIDELINES?

In favored parlance, the identification of a individual is a crew of unique and secure traits associated to the character that distinguishes him/her from others. Every individual, even two similar-looking people, has a special identification. In a jail context, identification encompasses the focus factor of a personality as per authorities statistics collectively with begin registration, voter id, using license, etc. It contains the subsequent: call, citizenship, deal with, bodily distinguishing attribute (a scar or mole), image, and blood group statistics. This can help authorities keep track of people who live in or travel through the territory. identity as a result of Identity theft crimes range from stealing Social Security numbers to stealing vital information such as savings card accounts. It consists of any such facts that can be used by the crook to take over the victim's identification to commit myriad crimes. Section sixty-six C of the Information Technology (Amendment) Act, 2008, consists of digital signatures and passwords as the means of identity.

CONCEPT OF IDENTITY THEFT

Identity theft involves the unauthorised use of another person's identity to commit fraud or other criminal activities.The stolen personal facts can encompass the victim's call, cope with, social protection quantity, driving force's license range, passport quantity, monetary information, credit card numbers, financial institution account info, and passwords.

The methods used by identity thieves to obtain personal information can vary. They can obtain the information through phishing, hacking, dumpster diving, skimming, or social engineering. Phishing is a method in which the victim is tricked into providing their personal information through fake emails or websites. Hacking involves gaining unauthorized access to a computer or network to obtain personal information. Dumpster diving involves searching through garbage to obtain discarded documents that contain personal information. Skimming is the process of stealing credit card information by using a small electronic device that reads the magnetic stripe on a credit card. Social engineering involves tricking the victim into revealing their personal information through manipulation or persuasion.

The crime of identity theft consists of two steps which may or may not be committed by the same person, namely:

1) Wrongful collection or acquisition of an individual's personal identity information

2). The wrongful use of such information with the intention of causing legal harm to that person.

The first step in fraudulently obtaining personal identification information can be done in several ways. It can be done by the thief who fraudulently uses such data himself or buys the stolen identity from dealers in such an illegal trade. Here too, coming in contact with such traders becomes easier through the internet. As the researcher is focusing on computer-aided ID theft, techniques of procuring personal data from electronic devices are as follows:

1). Hacking : It is a method through which malware like computer viruses or worms are used to divert information to the hackers who decrypt it and then either use it themselves or sell it to others to commit fraud using such information. Such attacks can be done in the garb of infected links, free software download, signing in through Facebook account or where there is no proper firewall protection or strong password to protect networks or computers as such.

INTERNATIONAL JOURNAL OF CRIMINAL JURISPRUDENCE
(P) Volume I and Issue I of 2023
ISBN - 978-81-960702-2-9
Published by
Institute of Legal Education
https://iledu.in

2) Phishing: The fraudster may send an e-mail with a link to a fake webswebsite,t may resemble an authentic link to, say, a bank site, where personal information and account information will be requested. The reasons for seeking such information may be to keep the customer's information up-to-date for better bank services or to claim that failure to provide such information would result in account suspension.

3). Pharming: It is similar to phishing, but in this case, clicking on the authentic link of the bank website would redirect the website's traffic to a fake site even if the user had entered a valid internet address. Pharming is done by installing malicious code either on the personal computer or on a server. Hence, it can target various users at the same time. It happens without the consent or knowledge of the victim and is often called "Phishing without a Lure." [15]

4). Nigeria 419 Scam: This method is target-specific, where the fraudster sends an e-mail as a rich family member of a dead African millionaire wanting to use the victim's bank account to transfer some money on the pretext that it is difficult to access it due to the political turmoil in his country, in return for a huge sum of money as payment for the transfer. Another of its kind is informing the victim of a huge lottery amount won by him amongst thousands of accounts and asking for the account details to transfer such a lottery amount. Such details, once given by the gullible user, are used to steal their funds.

5). Skimming: This employs various devices stealthily attached to the ATM machines or any other machines where the credit or debit card is put to use. These stealth devices fit on the original machines and have a magnetic card reader with a pinhole camera to shoot the victim's movements on the machine while he or she enters the PIN. Some sophisticated skimming devices generate an automatic message that is received by the thief each time a person swipes his card.

6). Vishing: In this, the fraudster calls the victim by pretending to be a bank representative or a call center employee, thereby tricking the victim into disclosing crucial information about their identity.

Online advertising fraud and business transaction fraud involving online payments through unsecured gateways are two other types of fraud methods.

After the initial step of illegal personal identity information collection is completed, various crimes aimed at achieving economic enrichment, like withdrawing money from the existing account or applying for new bank loans, credit cards, or benefiting from certain government schemes in the name of the stolen identity, are committed.

This creation of a new means of identification using the victim's existing identity is called breeder identification. Such a thief might not have been able to avail himself of these facilities if he had applied in his real name. Sometimes, graver crimes other than impersonation, forgery, cheating, immigration fraud, etc., can be committed.

The stolen identity information can be used to procure illegal weapons or bomb parts by the terrorists to dodge the authorities, which can subject the victim to stricter laws. In such a case, proving the victim's innocence becomes very difficult unless the fact of stolen identity information comes to the notice of the victim before it is used in furtherance of terrorist activities and he reports it to the police. This again is not possible if such personal information is stealthily accessed through a computer, in which case no trace or sign of theft can be gauged before the information is actually used for illegal purposes.

INTERNATIONAL JOURNAL OF CRIMINAL JURISPRUDENCE

(P) Volume I and Issue I of 2023

ISBN - 978-81-960702-2-9

Published by

Institute of Legal Education

https://iledu.in

LEGAL FRAMEWORK FOR IDENTITY THEFT

The legal framework for identity theft varies from country to country. In India, identity theft is recognized as an offense under the Information Technology Act, 2000. Section 66C of the Act provides for punishment for identity theft, which can range from imprisonment for three years to imprisonment for ten years, along with a fine. The act defines identification theft as the "fraudulent or dishonest use of the digital signature, password, or some different unique identification attribute of each different man or woman."

Within the u. S. A., identification theft is recognized as a federal offense under the identification theft and assumption deterrence act, of 1998. The Act provides for punishment for identity theft, which can range from imprisonment for two years to imprisonment for 30 years, along with a fine.The act defines identity theft because the "understanding switch or use, without lawful authority, of a way of the identity of some other individual with the intent to commit, or to useful resource or abet, any illegal pastime that constitutes a contravention of federal regulation, or that constitutes a criminal underneath any relevant country or nearby law."

In the European Union, identity theft is recognized as a crime under the European Convention on Cybercrime, 2001. The Convention provides for punishment for identity theft, which can range from imprisonment for six months to imprisonment for three years, along with a fine. The Convention defines identity theft as the "unlawful acquisition, use, or disposal of personal data."

JUDICIAL APPROACH TO IDENTITY THEFT:

The judicial approach to identity theft varies from country to country. In India, the courts have taken a strict view towards identity theft and have recognized it as a serious offense. In Ravi Singh vs. State of Haryana (2010), the Punjab and Haryana High Court held that "identity theft is a serious offense that is on the increase." "Such crimes pose a serious threat to the economic and social structure of the country." The court also observed that "identity theft is an offense that strikes at the very root of an individual's personality, reputation, and dignity."

In the United States, courts have also taken a strict stance against identity theft, recognizing the harm done to the victim. In United States vs. Larson (2007), the court observed that "identity theft is a serious crime that strikes at the heart of a person's identity and can cause significant harm, both financially and emotionally."

In the European Union, the courts have also recognized the seriousness of identity theft and acknowledged the need to protect personal data. In Paeffgen vs. Germany (2010), the European Court of Human Rights held that "the protection of personal data, including identity, is a fundamental right protected by the European Convention on Human Rights."

INTERNATIONAL JOURNAL OF CRIMINAL JURISPRUDENCE
(P) Volume I and Issue I of 2023
ISBN - 978-81-960702-2-9
Published by
Institute of Legal Education
https://iledu.in

CHALLENGES IN COMBATING IDENTITY THEFT

The challenge in combating identity theft is due to the anonymity provided by the internet, which makes it difficult to track down the identity thieves. The use of encryption and anonymization tools can further complicate the investigation. The lack of awareness among the general public about the threat of identity theft also makes them vulnerable to the crime. Inadequate training and resources for law enforcement agencies to investigate and prosecute identity theft cases are also a significant challenge.

Identity theft is a growing concern worldwide, with criminals using stolen personal information to open credit accounts, take out loans, and commit other types of fraud. The fight against identity theft is a complex and ongoing challenge, requiring the cooperation of individuals, businesses, and governments at both national and international levels. Here are some of the challenges involved:

INCREASING SOPHISTICATION OF CRIMINALS:

Cybercriminals are constantly developing new tactics to steal personal information, such as phishing scams, malware attacks, and social engineering. This requires continuous updates to security measures to stay ahead of the threat.

GLOBAL NATURE OF THE PROBLEM:

Identity theft is a transnational crime, and perpetrators can be based anywhere in the world. This makes it difficult to track down and prosecute offenders and requires international cooperation and coordination.

FRAGMENTED LEGAL FRAMEWORK:

Laws around identity theft and data protection vary widely between countries, making it difficult to prosecute criminals and establish consistent standards for prevention and detection.

LACK OF AWARENESS:

Many people are not aware of the risks of identity theft or how to protect themselves, which can make them vulnerable to scams and fraud.

PRIVACY CONCERNS:

Balancing the need for security measures with individuals' right to privacy is a delicate issue. Some security measures, such as collecting biometric data, can be controversial and raise concerns about surveillance and civil liberties.

COST:

Identity theft can be expensive to prevent and mitigate, with costs borne by individuals, businesses, and governments. This can make it challenging to allocate resources effectively and prioritize prevention efforts.

Addressing these challenges requires a multifaceted approach that involves public awareness campaigns, education and training for individuals and organizations, technology upgrades, and international cooperation on data protection and law enforcement.

PROBLEMS CONFRONTED IN IMPLEMENTATION OF THE LAWS

Despite the fact that cybercrime is increasing year after year, the conviction rate in India is dismally low. As against 3682 complaints, 1600 of the accused have been arrested, and merely seven of them have been convicted as per 2013 data. This might be due to improper implementation of the existing rules or an insufficiency in the infrastructure required for implementing the laws.

Firstly, there is a dearth of police personnel specialized in dealing with cybercrime cases. As technology advances, cyber criminals employ new forms of encryption technology that are difficult to decipher due to the authorities' limited resources. This delays the entire process, sometimes leading to the release of the accused due to a lack of proof.

INTERNATIONAL JOURNAL OF CRIMINAL JURISPRUDENCE

(P) Volume I and Issue I of 2023

ISBN - 978-81-960702-2-9

Published by

Institute of Legal Education

https://iledu.in

In the U.S., some judicial pronouncements have given the police the power to ask the cybercriminal to decrypt the digital evidence in return for some prison concessions, but it has not been deployed often. In addition, India currently has eight cyber labs, which are overburdened due to the large number of cybercrime cases.

Lastly, one of the reasons for the low rate of conviction or reporting may be because of these of non-registration of cybercrime complaints by the police. This issue should also be look these short comings can be overcome by the government increasing the number of vacancies for skilled police officers and allocating more funds to update to the most recent technology, which can aid in the current requirement of confronting a cyber criminal.

RECOMMENDATIONS

To address the challenges in combating identity theft, the following measures can be taken:

AWARENESS CAMPAIGNS: The government and other stakeholders can conduct awareness campaigns to educate the public about the threat of identity theft and the preventive measures they can take.

STRENGTHENING THE LEGAL FRAMEWORK: The legal framework for combating identity theft can be strengthened by increasing the punishment for the offense and including provisions for compensation to the victim.

CAPACITY BUILDING: Law enforcement agencies can be provided with adequate training and resources to investigate and prosecute identity theft cases. Collaboration with international law enforcement agencies can also enhance the effectiveness of the investigation.

TECHNOLOGY: The use of advanced technology such as artificial intelligence, machine learning, and blockchain can assist in the detection and prevention of identity theft.

CONCLUSION

Identity theft is a growing menace in the digital era and has emerged as a global problem. Unauthorized access to an individual's personal information is a violation of their privacy and can cause severe harm to the victim. The legal framework for combating identity theft varies from country to country. The judicial approach to the crime has been strict, and the courts have recognized the seriousness of the offense. The challenges in combating identity theft can be addressed by increasing awareness, strengthening the legal framework, building capacity, and using advanced technology. A coordinated response at the national and international level is required to combat this crime effectively.

REFERENCE

1.Title:Identity Theft and Identity Fraud, Website title: Department of Justice, URL:https://www.justice.gov/criminal-fraud/identity-theft/identity-theft-and-identity-fraud, Date published: November 16, 2020, Date accessed: February 24, 2023

2.Title:Privacy and the Information Technology Act — Do we have the Safeguards for Electronic Privacy? — The Centre for Internet and Society, Website title: The Centre for Internet and Society, URL:https://cis-india.org/internet-governance/blog/privacy/safeguards-for-electronic-privacy, Date published: April 7, 2011 Date accessed: February 24, 2023, Author: Prashant Iyengar

3.Website title:The Information Technology ACT, 2008, URL:https://police.py.gov.in/Information%20Technology%20Act%202000%20-%202008%20(amendment).pdf, Published year: Missing, Date accessed: February 24, 2023

4. Title: Universal's Concise Commentary on the Information Technology Act, 2000 (21 of 2000) with Exhaustive Case Law Publisher: LexisNexis Published year:2016
5. Title: CETS 185 - Convention on Cybercrime Website title: https: //rm.coe.Int URL:https://rm.coe.int/1680081561 Published year: Missing Date accessed: February 24, 2023
6.Title:Identity Theft and Assumption Deterrence Act, Website title: Federal Trade Commission, URL:https://www.ftc.gov/legal-library/browse/rules/identity-theft-assumption-deterrence-act-text, Date accessed: February 24, 2023 Author: Stephanie T Nguyen