Educational Administration: Theory and Practice
2023, 29(4), 4536–4540
ISSN: 2148-2403
https://kuey.net/

Research Article

Identity Theft: Cross-Border Legal Paradoxes and India's Cyber-Economic Crisis in the Algorithmic Age

Saima Jan[1*], Dr. Anna Bashir[2]

[1*]Research Scholar, School of Law, University of Kashmir - 190006, Hazratbal, India, Email: syedsaima144@gmail.com
[2]Assistant Professor, School of Law, University of Kashmir - 190006, Hazratbal, India, Email: annabashir@gmail.com

Citation: Saima Jan, et.al (2023), Identity Theft: Cross-Border Legal Paradoxes and India's Cyber-Economic Crisis in the Algorithmic Age, *Educational Administration: Theory and Practice*, 29(4) 4536–4540
Doi: https://doi.org/10.53555/kuey.v29i4.9497

ARTICLE INFO

ABSTRACT

In the 21st century, the rapid increases in computers storage capacity and the ease of conducting tasks with a simple click have transformed the world into a virtual global village. This interconnected digital landscape has connected businesses worldwide and popularized net banking. However, the exponential growth in storage capabilities, the widespread use of the internet for business and financial transactions, and the rise of social networking have also created opportunities for white-collar crimes and illicit activities. Among these, identity theft has emerged as a growing concern across jurisdictions. Identity theft not only impacts victims' financial security and mental well-being but also poses a significant threat to economic stability. Once primarily observed in Western nations, this crime has now become prevalent in developing countries like India. This research paper explores the rising phenomenon of identity theft in India and its severe economic implications for victims. It examines the prevalence and impact of identity theft, analyzes the legal framework addressing the issue in India, and delves into the various techniques and types of identity theft. Furthermore, the study offers a comparative analysis of the legal provisions for identity theft in India and the United States.

Introduction

Information technology has profoundly transformed human life, reshaped social structures and fostering a globally connected community. The internet, as a groundbreaking innovation, has enhanced human interactions and created opportunities for global connectivity. However, alongside these benefits, it has also given rise to numerous offenses collectively known as cybercrimes.[1] One of the primary drivers of cybercrime is the easy access to the internet, which has facilitated privacy violations and opened new pathways for criminal activities. Among these cybercrimes, identity theft has emerged as a significant and growing concern worldwide.[2]

Identity theft, often referred to as a crime of the new millennium, is one of the fastest-growing crimes globally, affecting individuals across regions, genders, and ethnicities. Its transnational nature makes it challenging for law enforcement to track offenders and deliver justice.[3]Over the past two decades, identity theft has become a major challenge for legislators, law enforcement agencies, and victims alike, causing substantial economic losses to individuals, businesses, and governments. Beyond financial damage, it also compromises privacy and moral values, leaving long-lasting effects on victims. The term "identity theft" was first coined in 1964. Since then, countries like the United Kingdom and the United States have provided statutory definitions of identity theft, describing it as the unauthorized acquisition and use of personally identifiable information. This crime typically involves fraudulently obtaining personal details—such as names, addresses, credit card or bank account numbers, social security numbers, passwords, or medical insurance details—and using them for financial gain or to harm the victim.[4]

[1] Berni Dwan, "Identity theft, Computer Fraud & Security", p. 14-17, (2004)
[2] FawziaCassim, "Protecting personal information in the era of identity theft: Just how safe is our personal information from identity thieves?" 18 PELJ 69 (2015).
[3] Daniel J. Solove, "Identity Theft, Privacy, and the Architecture of Vulnerability" 17 HLJ 54 (2003) .
[4] Ruchika Jha, "Identity Theft: Is it a modern crime? The identity theft prevention in post internet era", LTJ (2020),

While identity theft existed before the internet era through traditional physical crimes, the reliance on digital technology has made it much easier for offenders to commit such crimes today. Historically, methods like stealing mail from mailboxes, bribing or deceiving individuals with access to personal data, or purchasing stolen identity cards were common. Techniques like "dumpster diving," where personal information was retrieved from discarded bank statements, checks, or bills, were also widely used. Scammers would even impersonate customer service representatives or survey researchers to gain direct access to sensitive information. Although these methods were risky, time-consuming, and often led to the identification of offenders, advancements in technology have simplified the process while making detection significantly harder.

In the digital age, technology enables individuals to create multiple virtual identities through email accounts and passwords, which often bypass physical verification. This grants anonymity and privacy during online transactions, making it easier for cybercriminals to exploit such systems. While the world has recognized cybercrime, particularly identity theft, as a serious issue, its prevention and prosecution remain complex. The anonymity afforded by technology has turned identity theft into a pervasive problem, resulting in losses of economic value, privacy, and ethical standards across the globe.[5]

Online techniques of Identity Theft

Techniques of procuring personal data from electronic devices are as follows:

1. Hacking: This method involves using malware, such as computer viruses or worms, to redirect information to hackers. Once obtained, the hackers decrypt the information and either use it themselves or sell it to others for fraudulent purposes. These attacks often occur through infected links, free software downloads, or by exploiting vulnerabilities like weak passwords, lack of firewalls, or signing in through social media accounts like Facebook.

2. Phishing: In phishing scams, fraudsters send emails containing links to fake websites that mimic legitimate ones, such as a bank's website. These emails often request personal and account information, claiming it is necessary to update customer details or warning that failure to comply will result in account suspension.

3. Pharming: Similar to phishing, pharming redirects users to fake websites even when they enter a legitimate URL. This is achieved by installing malicious code on a server or personal computer. Unlike phishing, pharming can occur without the user's awareness or any interaction, making it capable of targeting multiple users at once. This is often referred to as "phishing without a lure."

4. Skimming: Skimming involves using hidden devices attached to ATMs or machines that process credit or debit cards. These devices often include a magnetic card reader and a pinhole camera to capture the victim's PIN as they use the machine. Some advanced skimming devices can instantly transmit the stolen information to the thief.

5. Vishing: This scam involves fraudsters impersonating bank representatives or call center employees over the phone. They trick victims into revealing sensitive personal and financial information under the pretense of resolving issues or verifying account details.

Additional online scams include fraudulent click advertisements and business scams involving payments made over unsecured channels, further exploiting users' trust and technological vulnerabilities.[6]

Types of Identity Theft

The rise of digitalization has simplified various aspects of life, making it easier to conduct business and access government services, such as paying bills and filing income tax returns. However, it has also exposed personal and financial information to the risks of cybercrime. Identity theft, in particular, has emerged as a significant threat, and it can be categorized into the following nine types:

1. Criminal Identity Theft: This is the most common form of identity theft, where offenders unlawfully use stolen identities to commit crimes or sell them on the black market.

2. Financial Identity Theft: In this form, offenders use the victim's financial identity to engage in fraudulent activities involving bank accounts, insurance, or other financial transactions.

3. Identity Cloning and Concealment: Criminals use stolen information to hide their true identities, often to obstruct investigations. They may request and misuse identification tools or exploit the victim's bank account for money laundering. Additionally, stolen identities can be used to bypass identification requirements and counterterrorism security checks.

4. Synthetic Identity Theft: This type involves creating a new, fake identity by combining stolen information with fabricated details. Often, data from multiple individuals is used to construct the synthetic identity. For instance, fraudsters can use a fake identity to obtain a credit card, which is then used for online

[5] Shun Yung Kevin Wanga and Wilson Huang, "the evolutional view of the types of identity thefts and online frauds in the era of the internet", ISSN 2045-6743 IJC (2011).

[6] Aishwarya Joshi, "Identity Theft- A Critical and Comparative Analysis of Various Laws in India", 2 JCIL 6 (2016).

or offline purchases. Victims of this type of identity theft may experience a drop in their credit scores as a result.

5. Medical Identity Theft: In this case, offenders fraudulently use the victim's medical insurance or health benefits, often selling this information to hackers. Fraudulent claims may also be submitted under the stolen identity. Victims of medical identity theft, like other identity theft victims, can face denial of services or other significant challenges.

Digitalization, while offering convenience, has also made safeguarding personal data an essential priority to prevent such forms of identity theft.[7]

Prevalence of Identity Theft

Identity theft is one of the fastest-growing crimes, not only in the United States and other developed nations but increasingly in developing countries as well. In India, despite legislative measures to address the issue, identity theft remains rampant. Statistics reveal that the crime is on the rise, causing significant economic losses to individuals, private companies, and governments worldwide. According to the National Crime Records Bureau, India registered 44,546 cases of cybercrimes in 2020, compared to 28,248 in 2019, with 60.4% of these cases motivated by fraud. The 2021 Norton Cyber Security Safety Insights Report highlights that out of 55 million victims of identity theft across 10 countries, India alone accounted for 27.7 million.[8] Over 27 million Indian adults experienced identity theft in the past year, with two out of every five individuals being victims. Around 45% of Indian adults have encountered online identity theft, and 63% reported feeling more vulnerable to cybercrime since the onset of the pandemic. Astonishingly, 1.3 billion hours have been spent addressing these issues.[9]

The Union Territory of Jammu and Kashmir has not been immune to this growing menace. Victims of identity theft can be found in the Union Territory of Jammu and Kashmir as well. In one high-profile case, a cybercriminal impersonated senior IAS officer Shahid Iqbal Choudhary by using his picture and phone number on WhatsApp to defraud colleagues and acquaintances. Another incident involved the Cyber Police of Kashmir Zone apprehending two Nigerian fraudsters in Delhi for scamming a Baramulla resident of ₹36.35 lakhs through an online scam.

Identity theft cases have also emerged with fintech loan apps. Some individuals discovered that loans had been taken out using their PAN cards without their knowledge, negatively affecting their credit scores. The "Dhani" loan app, for example, was exploited by fraudsters to secure loans, leaving the actual PAN cardholders to deal with the repercussions of unpaid debts.[10]

Impact of Identity Theft

Identity theft occurs when someone gains unauthorized access to your personal information and uses it for illegal or unethical purposes, putting victims at risk physically, emotionally, socially, and financially. It accounts for 58% of all data breaches and has a profound impact in today's digital age, where personal and financial interactions increasingly occur online.[11] Victims face numerous challenges, such as changing passwords, canceling old accounts, opening new ones, addressing financial losses, covering legal fees, and managing disruptions to their lives, including their children's education. According to a 2021 Identity Theft Resource Center survey, 74% of identity theft victims reported stress, 69% experienced fear regarding their financial safety, 60% felt anxiety, and 42% were concerned about the financial security of their families. Some even suffered sleep disorders or were unable to work due to the psychological toll.

The consequences can also extend to legal risks. If crimes are committed using a victim's identity, the victim may face wrongful arrest or legal action until their name is cleared—a process that can take months or even years. Businesses, too, are affected, with employee identity theft accounting for a staggering 90% of business-related data breaches.[12] Recovering from identity theft is often a long and arduous process. Victims not only endure emotional and financial stress but also face challenges dealing with law enforcement and the judicial system. Even when restitution is achieved, it is often a slow and unsatisfactory journey. When personal information is used to take out loans or create accounts in your name, clearing your credit record and

---

[7] Ankita Shrivastava, *"Identity Theft in Cyberspace with Special Reference to India"*, 8 ISSN 2581-5504 (January 2020).

[8] Ministry of Home Affairs, Government of India, National Crime Record Bureau Report, National Crime Record Bureau, available at: http://ncrb.gov.in/ StatPublications/CII/CII2017/pdfs/CII2017-Full.pdf, (last visited Jan 10 2023).

[8]India Today, April 19 2021,available at: https://www.indiatoday.in / (last visited 18 may 2023).

[9]India Today, April 19 2021,available at: https://www.indiatoday.in / (last visited 18 may 2023).

[10] *The Times of India,* Feb. 15, 2022. Available at: https://www.m.timesofindia.com. (Visited at: Sept. 22, 2023).

[11] Shaurya Jain, Muskan Sharma, "Identity Theft in India: A Security Concern" 11 ISSN 2581-5504 (2020).

[12] Dr.P.Arunachalam, "Economic Impact of Identity Theft in India: Lessons from Western Countries", International Journal of Marketing and Trade Policy,Serials Publications, New Delhi.

restoring your reputation can take years, leaving victims to bear the long-term consequences of this devastating crime.

Laws Governing Identity Theft in USA and India

Legislations relating to Identity Theft in USA

In the United States, most states have specific laws targeting identity theft. Some states clearly criminalize identity theft on criminal records, while others have broader provisions that allow for prosecution. The U.S. was among the first nations to establish legislation against identity theft. In 1998, Congress passed the *Identity Theft Assumption and Deterrence Act* (The Identity Theft Act, U.S. Public Law), which laid the foundation for combating this crime. The Act was followed by the introduction of aggravated identity theft as a punishable offense in 2004.[13]

In 2007, the *Identity Theft Enforcement and Restitution Act* was introduced to address existing legal loopholes and was recently approved by the Senate. Unlike many countries, the U.S. has a clear legal definition of identity theft, outlined in the 1998 Identity Theft Act. This law achieved four key objectives:

1. It established identity theft as a distinct crime targeting individuals whose identities were stolen and credit destroyed.
2. It introduced stringent penalties, including up to 15 years of imprisonment and substantial fines.
3. It designated the Federal Trade Commission (FTC) as the central federal agency for reporting identity theft cases, creating the Identity Theft Data Clearinghouse.
4. It closed legal gaps that previously criminalized the creation or possession of false identity documents but not the theft of personal identifying information.

The *Identity Theft Penalty Enhancement Act* of 2004 increased penalties for "aggravated" identity theft. In 2008, Congress further strengthened its stance by passing the *Identity Theft Enforcement and Restitution Act*, a federal law aimed at improving prosecution efforts and ensuring better restitution for victims. [14]

Legislation Related to Identity Theft in India

India's journey to combat cybercrime began with the establishment of the Ministry of Information Technology in 1999, tasked with turning the country into an IT superpower by 2008. Drawing inspiration from the UN's Model Law on Electronic Commerce (1996) and Singapore's Electronic Transactions Act (1998), India enacted its first IT-related legislation, the *Information Technology Act, 2000*, which came into force on October 17, 2000. This Act aimed to regulate technology use, establish investigative processes, and impose penalties for violations.[15]

An important amendment in 2008 introduced provisions for cybercrimes, including identity theft. Section 66C of the IT Amendment Act, 2008, specifically defines identity theft and prescribes punishment for fraudulently or dishonestly using someone else's electronic signature, password, or unique identification feature. Offenders can face imprisonment of up to three years and fines up to ₹1 lakh.

Additionally, the *Indian Penal Code (IPC), 1860* is often used in conjunction with the IT Act to address identity theft. Sections related to fraud, forgery, and impersonation (e.g., Sections 464, 465, 468, 469, 471, and 474) are invoked depending on the case. For instance, Section 468 applies to the creation of fake electronic records for fraud, while Section 419 penalizes impersonation to commit fraud.[16]

The 2008 IT Amendment also introduced Section 66D, penalizing impersonation through computer resources, and aligned it with recommendations to add Section 419A to the IPC for cheating via networks or computer systems. Other additions included penalties for privacy violations, cyber terrorism, and stringent rules for safeguarding sensitive personal data under the IT Rules, 2011.[17]

Sensitive personal data is defined to include passwords, financial information, health details, sexual orientation, medical records, and biometric data. These provisions ensure that identity theft involving such data is addressed under the law. However, data disclosure to government-authorized organizations is allowed in exceptional circumstances under Section 69 of the IT Act.

Challenges in Addressing Identity Theft in India

While the IT Act addresses identity theft, the crime is categorized as bailable and compoundable. This means offenders can secure bail at the police station, and disputes may be resolved amicably between parties. The prescribed penalty under Section 66C—three years of imprisonment—is often criticized as being too lenient to

---

[13] Dagmar Ösp Vésteinsdóttir & Fanney Björk Frostadóttir, “Identity theft: is there a need for a specific legislation?”

[14] Mcintosh, Victoria, “False identity, federal crime: the Identity Theft and Assumption Deterrence Act”, https://www.comparitech.com. (2018).

[15] S. Brenner, “Cybercrime metrics: old wine, new bottles”, VJLT, (2004)

[16] Gordon, Willox, Rebovich, Regan, Gordon, “Identity Fraud: A Critical National and Global Threat", 2 JEM 1 (2004).

S. Brenner, “Cybercrime metrics: old wine, new bottles”, VJLT, (2004)

[17] Amber Gupta, “Data Privacy in India and data theft”, (2013).

deter offenders effectively. Since the punishment is compoundable under Section 77A, offenders can evade stringent consequences, undermining efforts to combat this "millennium crime."[18] In conclusion, while both the U.S. and India have frameworks to address identity theft, India's laws require stricter enforcement and harsher penalties to effectively curb this growing menace.

Conclusion

Despite legislative measures to address identity theft, the crime continues to escalate unchecked. It is becoming increasingly prevalent in India, causing significant economic losses to individuals, private companies, and governments worldwide. No one is immune to this crime, which has evolved into a modern-day menace requiring urgent and stringent attention. There is an urgent need for a uniform legal framework to combat identity theft effectively. Robust legal mechanisms and preventive strategies must be established to curb this growing threat and support India's progress.

While identity theft was once predominantly a problem in Western countries, it has now spread to developing nations like India. Innocent individuals are easily deceived through phone calls or social networking sites, leading to substantial financial losses in mere moments. Victims often endure a traumatic experience, facing financial and emotional harassment at the hands of cybercriminals.

India's existing laws are inadequate to tackle this issue. While the *Information Technology Act* addresses certain cybercrimes, it falls short of effectively combating identity theft. Unlike the United States, which has multiple legislations specifically designed to prohibit and penalize this crime, India relies on a single provision under the *Information Technology Amendment Act (2008)*, which is insufficient to address the growing complexity of identity theft.

To effectively tackle this crime, India needs a dedicated law focused on identity theft. This would ensure stringent measures are in place to protect individuals and penalize offenders. It is equally important to educate people on preventing identity theft in this digital age. By analyzing the crime and the existing legal framework in India, it becomes evident that stronger laws and proactive measures are essential to combat this growing threat and safeguard citizens.

[18] Ruchika Jha, "Identity Theft: Is it a modern crime? The identity theft prevention in post internet era", LTJ (2020).