WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Digital Deception: An In-Depth Investigation of Identity Theft in the Indian Cyberspace

Diya Charaya

Student B.A. LL. B (H.), 5th Year, Amity Law School, Amity University, Noida (Uttar Pradesh)
DOI: https://doi.org/10.55248/gengpi.5.0424.0961

ABSTRACT

The article delves into the growing problem of cyber identity theft in India, acutely challenging the nation that is the world's fastest-growing digital economy with a consistent increase in the number of internet users. It examines the legal framework given by the Information Technology Act 2000 and Indian Penal Code that facilitates punishing cyber identity theft crimes. It analyses some prominent cases that provide insights into the multifaceted consequences of cyber identity theft, such as financial losses, mental trauma, public scorn and so on. It also deciphers the vulnerabilities such types of crimes pose for agencies and law enforcement and the problems in curbing them, such as legal hindrances, jurisdiction issue and publicity. It sheds light on the global practices of dealing with such crimes and recommends the improvement in Indian laws and cyber security measures by comparing it with other countries. In conclusion, it reflects upon the dynamic nature of cyber identity theft and the need for India leading and cooperating among other countries in curbing this menace.

Keywords: Cyber Identity Theft, Information Technology Act 2000, Indian Penal Code, Digital Privacy, Bharatiya Nyaya Sanhita

1.1 INTRODUCTION

In the dawning digital age, the development and implementation of a plethora of helpful and transformative new technologies promises to enrich the human condition, and help forge a brighter future for all. Regrettably, the Internet Age has also spawned a diabolical new genre of crime – namely, 'cyber identity theft'. What does cyber identity theft entail? The definition for cyber identity theft encompasses a vast array of criminal conduct – activities that involve the unauthorized access and acquisition of a person's private and confidential data, and are motivated by the potential for criminal profit to be made by using or disclosing such information to an unauthorized third party involving identity theft in the United States involves 'fraudulently appropriating another person's identity, in whole or in part, including a name, social security number, or other identifying information'. Congress defined federal identity theft to include the unlawful use of someone's identifying data, such as a credit card number or bank account

1.1.1 Definition and Scope of Cyber Identity Theft

Cyber identity theft is not merely a theft of information; it is a theft of one's virtual existence. In legal terms, it encompasses a range of activities where personal data is obtained without permission, often through cyber means such as hacking, phishing, email spoofing, malware attacks, or exploiting data breaches. This information is then utilized to impersonate or commit fraud, impacting victims financially, emotionally, and reputationally. The scope of cyber identity theft is vast, extending beyond individual victims to corporations and governments, leading to significant financial losses, compromising of sensitive information, and erosion of trust in digital systems.

The Information Technology Act, 2000 (IT Act), amended in 2008, serves as the cornerstone of cyber law in India, addressing a range of cybercrimes, including identity theft. Specifically, Section 66C of the IT Act deals with identity theft, prescribing punishment for anyone who, fraudulently or dishonestly, makes use of the electronic signature, password, or any other unique identification feature of any other person.

1.1.2 Significance of Studying Cyber Identity Theft in the Indian Context

Given the Indian context, with the country having almost 760 million internet users, and an expanding digital economy which could provide tempting targets for cyber thieves, it becomes crucial to study cyber identity theft in the Indian framework. Post-2016 demonetization, with the push to curb black money and promote digital payments given by the Indian government, the volume of digital financial activity in India has exploded, providing more opportunities for cyber identity theft.

The importance of studying this phenomenon in India also lies in the fact that its population, being socio-economically diverse, still has a large section that's partially or completely in the process of getting digitally literate. Lack of awareness about safe digital practices would keep the same section

vulnerable to cyber frauds. Rising cases of cyber-attacks mean that India needs a legal and regulatory framework designed to meet the fluidity of technology Similarly, it is important to study the nature and intricacies of cyber identity theft at a time when the legal and regulatory framework designed to address it in India is still in the process of catching up with the speedy advancements in technology. Understanding the nature, modes and impact of cyber identity theft could not only enable the legislators to design better laws, improve cybersecurity measures and even create awareness programmes but could also help to reduce the risk of such crimes.

The Reserve Bank of India (RBI) and the Indian Computer Emergency Response Team (CERT-In) issued injunctions and advisories on the preventive and punitive measures through cyber-technology to curtail frauds. These highlighted the importance of public awareness on cyber-security. In a flurry of recent judgments (e.g., Shreya Singhal v. Union of India) that affirmed the constitutional rights to privacy and free speech against the necessities of surveillance and policing that technology enabled, the Supreme Court of India was also clear that these were in tension. Taken together, these began making India's legal and ethical dilemmas on targeting cyber-identity theft more apparent.

1.2 UNDERSTANDING CYBER IDENTITY THEFT

One of the most pernicious forms of cybercrime is identity theft: it pervades the fabric of your life with tentacles running deep into your psyche and with consequences you might struggle to reverse. This part of my book explores the phenomenon of cyber identity theft, starting from the theoretical aspects, then moving to the modes of its operation and finally explaining the multiple ramifications of becoming an identity theft victim.

1.2.1 Conceptualizing Identity Theft: Definition, Types, and How It Occurs

For our purposes, we define identity theft over cyberspace as the unauthorized acquisition, possession or disclosure of personal information over the digital environment, with the intention of committing fraud or deceit. This definition belies a wide range of specific activities, including financial fraud, criminal impersonation, and identity cloning, each of which has its own modus operandi and consequences.

- Financial fraud: These generally pertain to the unauthorized manipulation of another's personal and financial information to perpetrate fraudulent transactions or the theft of funds. For this there is the potential punishment under the Information Technology Act, 2000 (amended in 2008), for cheating by personation using a computer resource or communication device under Section 66D.
- Criminal Impersonation: this is when a perpetrator adopts another person's identity to commit an offence, evade detection or obtain an unlawful benefit. This can include creating fake email and social media accounts to posing as another person in legal and criminal proceedings.
- Cloning of identities: Copying an identity for opening accounts and getting credit cards, identity theft, crime and impersonation.

1.2.2 Methods of Cyber Identity Theft

The routes by which cyber identity theft can be perpetrated are numerous, and criminals are constantly evolving tactics to exploit new weaknesses.

- Phishing attacks: The most common of the various types of scams, phishing consists of emails or messages concealed as originating from a legitimate institution, attempting to elicit sensitive information from the recipient. Section 66C of the IT Act specifically applies to identity theft, thus potentially providing a legal route for retaliation.
- Malware and Spyware: Malicious software programmes that infiltrate and damage computers. Often these are written to 'stealthily' obtain or transmit personal and financial information directly from a victim's computer. Identity theft using malware comes under Sections 43 and 66 of the IT Act, which prohibit accessing a computer system without authorization.
- Data Breaches: Large-scale data breaches where personal information has been taken from databases by unauthorized individuals results in widespread identity theft – the Personal Data Protection Bill, 2019 yet to be enforced, presumes that the Legislature is alive to the problem and is ready to impose severe restrictions on non-consensual data collection and severe sanctions on malicious data breaches.

1.2.3 Impact on Victims

The consequences of a cyber identity theft can be even greater, extended into financial issues as well as other areas of the victim's life.

- Financial loss: The most immediate, quantifiable outcome. That can range from transactions on a credit card to bankruptcy. In the worst cases, victims may be held liable for debts the thief has incurred.
- Mental repercussions: suffering may significantly increase and include stress, anxiety, feelings of violation when the victim finds out about the identity theft. Mental distress may have persistent impact like depression and feeling of insecurity for the victim.
- Reputational harm: The impersonator's wrongful use of a person's identity might cause harm to the victim's reputation, especially if the identity theft plays a role in new criminal activity attributed to the victim. The consequences could affect job prospects, friends, colleagues, and others.

1.3 STATISTICS OF CYBER CRIME IN INDIA

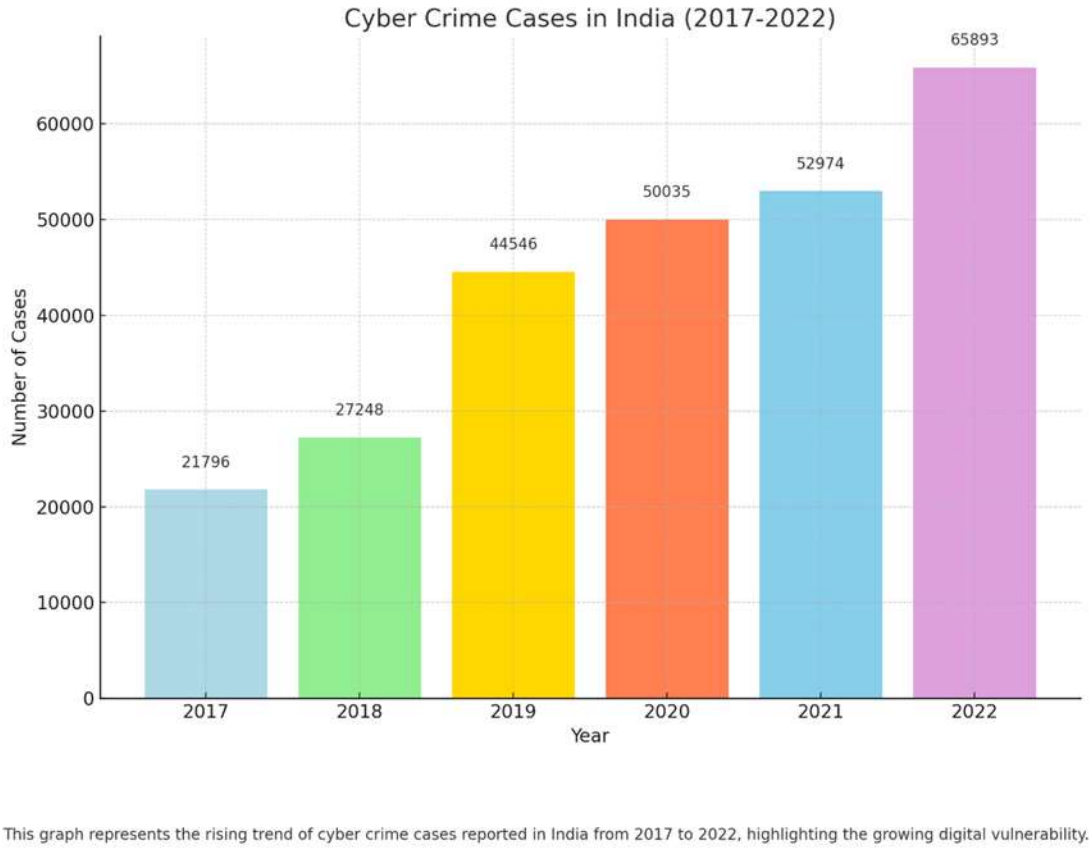

Fig1. Cyber Crime Cases in India (2017-2022) (NCRB)

The bar graph depicts the number of reported cyber-crime cases in India from 2017 to 2022, as per the data provided by National Crime Records Bureau (NCRB).A summary and insights of the data are as follows:

- 2017: Baseline at 21,796 cases. The initial case count of 21,796 is already much higher than it would have been five or 10 years prior, a reflection of an increasing number of cyber-crimes of various kinds – including fraud, hacking, identity theft and more as communications technologies are increasingly integrated into our daily lives.
- 2018: There is an increase to 27,248 instances.
- The jump in the figure indicates that cyber-crime is most probably on the rise. Perhaps this is because many services are now available online and people are using the internet extensively these days, making more of them susceptible to online scams and attacks.
- 2019: This figure dramatically increased to 44,546, nearly doubling in only two years. This could reflect an increase in the amount of online activity that people engage with and, perhaps more optimistically, a better understanding of reporting avenues, in which victims are encouraged and empowered to disclose.
- 2020: The numbers climb to 50,035 incidents. The year 2020 saw the emergence of COVID-19, which resulted in lockdowns and a proliferation of digital domains following as working, studying and leisure activities became increasingly conducted online.
- 2021: The count increases slightly to 52,974 cases. The increase is less dramatic than the previous year, but the trend continues, which might indicate that the factors that fueled the rise of cybercrimes remained.
- 2022: The data peaks at 65,893, the highest number for the present period. On win popularity affect most people to continue the tendency, and this trend could be associated to further adoption of digital devices, improved awareness and reporting of cybercrimes and or these criminals could also be improving their techniques.

The figures reveal an increasingly critical and expanding problem that India (as elsewhere) has to address as it becomes more digital, emphasizing the need for holistic strategies for cyber resilience.

1.4 LEGAL FRAMEWORK IN INDIA ADDRESSING CYBER IDENTITY THEFT

India's law on cyber identity theft is a tripartite body of law which constitutes of general and specific laws and the legal framework used to contain and penalize the crime is an interdependent one which lends assistance from laws specifically curated towards cybercrimes and even provisions from the Indian Penal Code (IPC), 1860 regarding identity theft. The framework includes provisions for cybercrime, it continues to span laws from the IPC, 1860 and it has recently been modified with new enactments in an attempt to modernize and tighten digital security as well as updating cyber laws to be in line with modern times and cybercrimes.

1.4.1 The Information Technology Act, 2000

The Information Technology Act, 2000, amended in 2008, provides the most comprehensive cyber law in India, directly addressing issues relevant to digital commerce and cybercrimes, such as identity theft.

Section 66C — Entitlement to punishment for identity theft: Whoever fraudulently or dishonestly represents himself to be another person, or fraudulently or dishonestly obtains, possesses, discloses or uses the electronic signature, password or any other unique identification feature of another person, shall be punishable with imprisonment for a term which may extend to three years, or with fine which may extend to ten thousand rupees, or with both. This is the relevant law for cyber identity theft, giving legal means for a victim to invoke.

Section 66D pertains to cheating by personation using a computer resource or communication device, which encompasses a wider set of identity theft activities committed on computer networks.

Giving effect to this, section 43A makes a corporate body liable for any wrongful loss or wrongful gain to any person caused by the negligence of such entity in implementing and maintaining reasonable security practices and procedures, and for failure to prevent unauthorized access, change or first-hand data transmission, provided the loss or gain is caused by reasons for which such entity is responsible under law. In other words, entities dealing in any sensitive personal data, such as Aadhaar numbers, will be required to ensure its security from any breach that may create an opportunity for identity theft.

1.4.2 The Indian Penal Code, 1860

Despite being passed long before the rise of the internet, the IPC includes provisions which are well-suited to tackling the criminal offences faced by identity fraud victims.

Section 416 and Section 419 pertain to cheating by personation and the punishment for such an act, respectively. These sections are used when the act of identity theft involves any form of personation, to dupe or harm others.

Section 420 covers cheating. Cheating is defined as an act that deceives by helping or discouraging another person from exercising due diligence, and thus causing them to give property or valuable security in an unlawful manner. It can be used in cases of identity theft that involve financial fraud.

Sections 464, 465, 468, 469, 471 and 474 cover the complete range from making a false instrument (for the purpose of effecting fraud) to possessing forged instruments, furnishing a basis

1.4.3 The Bharatiya Nyaya Sanhita, 2023

This new legislation is a radical reform of the criminal justice system, and thus contains the same sort of offences related to cybercrime and, by extension, cyber identity theft.

Sections 170 and 172: The details of these sections are not given in the brief; presumably they deal with aspects such as hacking crimes and identity theft, as a way of bringing India's criminal law to accommodate the contours of developing crime in the digital age.

Sections 316 and 317 (1) and (2): These probably simply elaborates on offences relating to cybercrimes and the punishments for such offences, underscoring the legal system's adaptation to current threats in the realm of cybersecurity.

1.4.4 Recent Amendments and Legislative Changes

Considering the growing menace of cybercrimes, there has been a number of changes in many legislations to make India's digital security more reliable and strengthen cyber laws.

The raft of amendments to the Information Technology Act, and the Bharatiya Nyaya Sanhita, 2023: principles of law of evidence in a digital age, are indicative of India's desire to lay the legal groundwork to rebuff malicious cybercriminals gaining momentum by and large thanks to advances in technology.

The legal codes relating to cyber identity theft in India are quite comprehensive. They cover several activities ranging from phishing and hacking to impersonation and forging. However, cybercrime, being an ever-evolving phenomenon, requires constant updates and amendments to the existing laws. This is precisely why we incorporate codes such as the Bharatiya Nyaya Sanhita, 2023, and the mention of various other on-going amendments to the

existing and relevant laws, which highlight India's attempt to adopt its legal regime for the protection of rights to effectively tackle the ever-changing kaleidoscope of cybercrime. It is important to note that although many online activities can easily cross-national boundaries, the emphasis on national identity will have an implication for those outside India who wish to interact online with those from the country. The legal scaffolding that is being built for protecting individuals from cyber identity thefts may also act as a deterrent from committing the crime and protect digital identity in a world that is rapidly becoming more interconnected.

1.5 CASE STUDIES

Although the Indian case of cyber identity theft is sprawling and diverse, it is possible to understand it better by looking at some of the prominent cases – those that have not only made news but have also set a precedent, reflecting both the strengths and weaknesses of the existing legal framework. We will examine a few prominent cases of cyber identity theft, analyses the judicial proceedings, results, lessons and the new legal jurisprudence emerging from these cases, and finally try to identify gaps in the legal process in dealing with cyber identity theft crimes.

1.5.1 Notable Cases of Cyber Identity Theft in India

One of the first landmark cases that brought the question of cyber identity theft into light was the S. Umashankar v. ICICI Bank case. In this case, an imposter posed to be S Umashankar, a District Collector in Tamil Nadu, and acquired a credit card in Mr. Umashankar's name and carried on transactions with it. The battle in court that ensued brought to light many problems, especially as they pertain to the onus of proving the innocence of the victims and the extent of liability of the banks in preventing such frauds. The banks were found liable for failure in verifying the credentials of the applicant for a credit card. This was a landmark judgment towards defining the responsibilities of banks in handling issues of financial fraud.

The other key case is Avnish Bajaj v. State (NCT of Delhi), which was technically a case about obscene content on a website but was equally important in asserting the role of intermediaries' liability in ensuring prevention of cybercrimes, including ID theft. It laid down the legal framework that indicated that digital platforms had to have foolproof system for preventing misuse, the precedent that would emerge later in cases about digital identities being misused.

The course of legal proceedings in these cases have been equally torturous due to the precision required of the victim to untangle the complicated web of cybercriminal, in tracing and apprehending perpetrators invisible in the ether. In S Umashankar v. ICICI Bank, the proceedings highlighted, in no uncertain terms, the importance of KYC (Know Your Customer) norms and banks' fiduciary duty towards their customers, to ensure that their customers really are who they say they are. The exoneration of the complainant set a judicial precedence deterring future forms of criminality at the hands of financial institutions, blaming the victim for identity theft.

By contrast, Avnish Bajaj v. State (NCT of Delhi) illustrated the inability to hold intermediaries responsible for the actions of third parties on their sites, and prompted the adjustment of the IT Act's clauses on intermediary liability. It sparked debates over the balance between regulation and freedom of expression on the internet.

Now these cases, taken together, present at least five important lessons and fundamental legal implications, including the utmost necessity for:

- Better authentication processes: Banks and other service providers should tighten up the process by which they authenticate users, to prevent impersonation and fraud.
- More articulate responsibility of intermediaries: The cases underscore the importance of clear legislation on the responsibility of intermediaries in preventing the misuse of their interfaces for cybercrimes, especially identity theft.
- Good legal frameworks that adjust: Cybercrime evolves quickly, and its legal framework has to evolve with it (requiring frequent adjustments for 'new' developments that are not really new at all).

1.5.2 Gaps Identified in the Legal Response

Although cybercrimes are gradually being recognized by the Indian state in their attempts to address them through am in the legal response to cyber identity theft. These are:

- Unawareness/under-reporting: As many cases of cyber identity theft are left unreported, often because victims are unaware that they have actually been victims of a crime or fear the social stigma associated with sexuality, more public awareness campaigns are needed, along with the assurance of confidentiality and sensitivity in their handling.
- The cross-jurisdictional nature of cybercrimes for which technical personnel are required to trace the digital footprints can be the biggest drawback in the investigation and prosecution of cases dealing with cyber identity theft.
- Courts must be specialized: Collectively, the complexity of online crimes merits the establishment of specialized courts where judges, prosecutors and other judicial officers are trained in cyber law and digital forensics, to enhance the chances of getting cases right.

1.6 CHALLENGES IN COMBATING CYBER IDENTITY THEFT IN INDIA

But solving the novel problem of cyber identity theft in India is like putting altogether three puzzles, which are cased in the triad of challenges – legal, technical as well as social. No surprise that each new piece of the triad we add to the solutions to this crime, whether civil or criminal, tech-driven initiatives, or social consciousness and education initiatives – makes it harder to solve the difficult triad of challenges that are posed by this 21st-century crime.

1.6.1 Legal and Regulatory Challenges

However, the Indian legal infrastructure, mostly through the previously mentioned Information Technology Act, 2000 (ITA) along with a variety of sections in the Indian Penal Code (IPC), attempts to cover cybercrimes. Since change in technology and the novel methods and technologies deployed by cyber criminals are a fast-paced field, it becomes difficult for the law to be constantly in tune with them. It, therefore, suffers from several lacunae. For example, an instance of this could be seen when the ITA (2000) contains provisions that prohibit identity theft under sections 66C and 66D, but these can unlikely be able to accurately capture the nuanced techniques of modern cyber identity theft. Through this lacuna, cyber criminals can exploit the situation, leaving the victim, in most cases, with a weak response under law.

1.6.1.1 Jurisdictional Issues and Cross-Border Crimes

As a 'trans-border' crime, victims and perpetrators could be in different jurisdictions, which means that there are more jurisdictional issues involved in these crimes, such as the investigation and prosecution of such offences. The lack of international legal instruments and cooperation agreement also hinder the enforcement process of pursuing international cybercriminals.

1.6.2 Technical Challenges

1.6.2.1 Advanced Hacking Techniques

Also, cybercriminals foreseeably keep evolving and devising more effective strategies along with advanced hacking (phishing, malware, software vulnerabilities), thus making it ever more difficult to detect and thwart identity theft. Indeed, some of these positively techniques will require a high level of technical skills and tools that law enforcement might not possess. This technical gap, in addition to making it easier to commit these crimes, also creates an investigative hurdle..

1.6.2.2 Lack of Robust Cybersecurity Measures

Despite such raising awareness, there is a large number of people and institutions in India who have not installed robust cyber-security apparatus, ranging from financial costs to lack of knowledge as to why it is required, resulting in deficient cyber-security apparatus making it easy for the cyber-criminals to exploit these vulnerabilities to carry out identity theft with relative ease.

1.6.3 Social and Educational Challenges

1.6.3.1 Awareness Levels Among the Public

A major hindrance in stopping cyber identity theft is the large proportion of people who are not sufficiently aware of safe online habits and the risks associated with digital activities. Most Indians, especially new internet users are unaware of such dangers or fail to see the significance of safeguarding personal details in the digital realm. This leaves them vulnerable to the clutches of identity thieves.

1.6.3.2 Social Engineering Scams

Social engineering is frequently used by cybercriminals to trick victims into knowingly supplying personal information. Rather than exploiting technological vulnerabilities, these scams target human psychology. As a result, social engineering scams are particularly effective and difficult to protect against because they simply rely on 'human nature'. Successful social engineering scams illustrate the importance of sustained educational initiatives to educate the public about the tactics used by criminals.

1.7 COMPARATIVE ANALYSIS WITH INTERNATIONAL LEGAL FRAMEWORKS

This fear of Cyber Identity theft is not limited to India and we can see other nations developing comprehensive laws legislating their lives in this field. India can also learn from foreign legal frameworks by analyzing and comparing international legal frameworks like General Data Protection Regulation (GDPR) of European Union for the data protection of the citizens and the Identity Theft and Assumption Deterrence Act of United States for the definition and ways of handling identity theft. Hence, it becomes important to identify their landmark provisions, explore their innovativeness and highlight where

they can be improved and suitably settled in the form of Indian legal frameworks to combat cyber identity theft. The venture of understanding the strengths and innovativeness of international frameworks will shed light on the global best practices which can further assist India in enhancing and modifying her legal frameworks for the dismay of Cyber Identity theft.

1.7.1 GDPR and its Approach to Identity Theft

The European Union's General Data Protection Regulation (GDPR) was adopted in May 2018, and represents the highest bar for personal data protection and privacy in the world to date. A core part of the roadmap strategy against ID theft comes from its fully fledged data protection principles, including:

- Data Minimization and Purpose Limitation: Data will have stayed within organisations that need access to it for a specific purpose, reducing the body of personal information potentially for the taking.
- Consent: The GDPR strongly empowers the mechanism of consent so that the processing of personal data shall (under certain conditions) only be allowed if you have given your clear, affirmative consent;
- Right to erasure: Also referred to as the 'right to be forgotten', this right enables an individual to seek the erasure of his or her data. The latter means that their private data will not remain exposed to possible data theft for a long period.
- Breach Notification: One of the pillars of GDPR is the breach notification requirement, mandating that companies must report the loss to the appropriate regulator and affected users within 72 hours of an incident taking place: halting the tide of identity theft in its tracks.

1.7.2 The US Identity Theft and Assumption Deterrence Act, 1998

The Identity Theft and Assumption Deterrence Act, which was passed by the US in 1998, is among the first laws aimed specifically at combatting identity theft. The Act recognizes identity theft as a federal crime and outlines the roles of individual governmental bodies in the prevention and prosecution of identity crimes. Specific features include:

- Identity theft: The Act contains a single, clear, and broad definition of identity theft: 'An individual engages in identity theft with respect to another individual when the individual (that is, the defendant) intentionally obtains or uses, without lawful authority, another individual's identifier, or more than one such identifier, which may belong to the same or different individuals.
- Creation of the Federal Trade Commission (FTC) as a Central Reporting Agency: Federal Trade Commission is a central agency for reporting and assisting victims in identity theft, and for coordinating a response to the crime.
- Restitution for Victims: Victims of identity theft may now seek restitution because of the loss and humiliation it causes.

1.7.3 Lessons for India from Global Best Practices

The analysis of the GDPR and the US Identity Theft and Assumption Deterrence Act show that learning from these laws and implementing some of their best practices can be useful for India to improve its legal framework to safeguard against cyber identity theft:

- Upgrading data protection and privacy laws: If the GDPR, with its broad-based data-protection framework, can be imitated to offer better protection of personal data in India, the problem of identity theft can be mitigated.
- Mandatory Breach Notification: Many countries, such as Brazil, the EU and India, have mandated breach notification requirements, after the GDPR's example. This can help to make the response to data breaches quicker and more effective, limiting some of the harm from identity theft.
- Central Reporting Agency: Create a central agency for reporting identity theft similar to the FTC in the US. Having one report for resolving such cases will help the victims approach the cases.
- Broad Definition, Clear Coverage: A broad definition with clear coverage in law (such as the US Act) might also help to systematically capture identity theft's various modalities, and bring the laws into compliance with the realities it should address.
- Empowerment and Protection of Victims Measures giving victims of identity theft greater rights to the restitution and protection of their interests, such as rights to erasure in the style of the GDPR, could give fuller support and redress to victims.

1.8 SUGGESTIONS FOR STRENGTHENING THE LEGAL FRAMEWORK

The growing threat of identity theft over the internet in India requires a robust legal and regulatory regime capable not only of fighting shadows but also of preventing the crime. The clocks of the Information Technology Act, 2000 (IT Act), and the Indian Penal Code, 1860 (IPC) provide the basic foundation. Given the evolutionary nature of crime in the cyber world, it needs laws and regulations to keep pace and be further amended.

1.8.1 Amendments to the IT Act and IPC

Amend the IT Act to include detailed sections relating to different types of cyber identity theft, specifying what such crimes entail (such as phishing, spoofing and unauthorized access to personal data) so as to provide a clear legal basis for action against such acts.

1.8.2 Clearer Definitions and Penalties

Make the law more of a deterrent by changing the penalties to reflect the severity of identity theft crimes against individuals, adding more fines, and increasing length of prison sentences.

1.8.3 Strengthening Cybersecurity Measures

A state may enunciate a national cybersecurity strategy, providing a guiding document on the goals and roles of government entities, the private sector and its citizens to combat cyber threats.

Develop and implement a federal cyber (identity) incident response and management capability that involves a broad range of stakeholders and institutions and that facilitates and coordinates responses to cybercrimes.

1.8.4 Private-Public Partnerships in Enhancing Security

Create incentives for private-public partnerships to share threat intelligence, develop shared security technologies, and cooperate on public-facing awareness campaigns.

Directed support and resources to Small and Medium Enterprises to bolster their cybersecurity postures, which are vulnerable to such attacks as they could have a disproportionate impact on our broader economy.

1.8.5 Public Awareness and Education Campaigns

Launch nationwide, multilingual, public awareness campaigns to educate citizens on the dangers of cyber identity theft and how to take precautions when online. Utilize all available media channels.

Teach digital literacy and cybersecurity, as well as the consequences of identity theft, in education from primary school through to college, so that those entering the workforce know what they are responsible for to avoid personal information being compromised.

Prepare targeted workshops for vulnerable classes, e.g. elderly and new internet users: These are more vulnerable to identity theft and require such training.

Public education concerning identity theft schemes involving Non-Delivered Goods – office furniture purchased on credit card: victim is paid for things never delivered; second variety is party receives cheque for more than agreed sum for purchase, is then asked to wire money back from party.

1.9 FUTURE OUTLOOK

The digital sphere is ever-changing, and technological and criminal changes driving shifts towards new and evolving forms of cyber identity theft. At this rapidly evolving moment in history, India is uniquely placed to shape the cyber identity theft response at a national and global level, due to its rapidly growing digital economy and expanding users.

1.9.1 Emerging Trends in Cyber Identity Theft

Given this perspective, it is not a far stretch to predict continuous sophistication and growth in the number of cyber identity theft as technology becomes an integral part of our daily living. Given the number and variation in the types of technologies that are emerging, cyber criminals will soon have access to new technologies such as artificial intelligence (AI) and machine learning (ML) to automate phishing attacks, create more believable fake online identities, or evade conventional security mechanisms. The adoption of Internet of Things (IoT) devices also widens the attack surface, potentially adding new avenues through the use of such technologies for identity theft. Another trend is exploiting social media platforms for identity theft purposes. Personal data or information shared via various social media platforms have been harvested for use in identity fraud and other illegitimate activities.

1.9.2 Anticipated Legal and Technological Developments

These trends have also spurred a series of countermeasures to the cyber identity theft phenomenon, from the legislative to the technological.

- Legal Amendments: It is likely that there will be more changes to the IT Act and IPC in India to keep up with the changing nature of cybercrimes and to have specific laws against the misuse of AI and other IoT devices, to have more stringent data protection laws and robust laws to

strengthen cooperation among nations to investigate and prosecute cybercrimes under international law. The passing of the Personal Data Protection Bill would be another positive step that is currently in the offing.

• Tech Advances: Technological advances related to encryption, blockchain and biometric checks will make identity theft much more difficult, and limit where stolen data can be used. In a similar vein, although AI and ML make it easier for criminals to represent themselves as others, they can also be used to automatically monitor transactions and detect suspicious behaviour, and prohibit it in real time. New decentralized identity systems (where individuals control their identity themselves, rather than relying on centralized institutions) could also help reduce the threat of identity theft.

1.9.3 India's Role in Global Efforts to Combat Cyber Identity Theft

India's huge digital economy and its position as a substantial IT hub places it in a crucial role to offer a significant contribution to the wider international response to cyber identity theft by: forging international partnerships and participate in other international cybercrime prevention initiatives, learn from international best practice, and share international knowledge on the subject; enabling foreign law enforcement entities to conduct their cybercriminal investigations and enable extradition of suspects with Indian cybercriminals; sharing threat intelligence and cybersecurity innovation involving joint research and development of cybersecurity technologies. That India has engaged with international processes such as the way it has engaged in the Budapest Convention on Cybercrime initiative – an initiative that goes beyond the Convention's reach through participation in working groups and as an observer to the committee of the experts – more than suggests that India is ready to engage in international discourse on cybercrime.

Besides, because of its deep bench of digital skills and innovation creativity, India's IT industry can lead the creation of next-generation cybersecurity products that can also be of assistance to the world's public and private sectors. India can leverage several policy initiatives and public-private partnerships and state-driven projects under the Digital India programme to enhance the creation of secure digital infrastructures and cybersecurity technologies.

1.10 CONCLUSION

Cyber identity theft in India is a complex issue in the fast-changing scenario of Indian society and the massive spread of the Internet. It plays out on a much larger canvas – highlighting the vulnerabilities of individuals and the emerging social fabric of society in a fast-changing digital world and the burgeoning internet user's base. This study delves into the complexities of modern threats and plays out the vulnerabilities to the new forms of cybercrimes especially identity theft.

The Information Technology Act 2000, coupled with the Indian Penal Code, constitutes the primary legal framework through which cyber identity theft in India is tackled. And yet, as the study reveals, 'it is clear that the existing legal apparatus has not been able to keep pace with the mutating nature of cybercrimes. Studies like this one delve into the most high-profile cases to paint the picture of cybercrime as it is committed – the financial and emotional effects it has on the victims, and what needs to be done to ensure justice and deterrence.

The second important takeaway is that India is witnessing a spike in cybercrime cases year on year, and we urgently need a more robust and flexible legal regime to address the stark reality of the age as lawmakers and governments in India grapple with the question of what the law should look like in the cyber age. Similarly, we can learn from our international counterparts. A comparison of the omnibus General Data Protection Regulation of the European Union, and Identity Theft and Assumption Deterrence Act of the United States could provide two reference points for an approach to cyber identity theft that could be game-changing for India.

Recommendations include proposed legislative modifications affecting aspects of current law, increased security in the cyber environment, and broad-reaching public awareness and education campaigns to help with these challenges. Together, legal and technical vulnerabilities, coupled with social and educational vulnerabilities, have contributed to the immense threat of cyber identity theft.

The study concludes that 'India is poised to take a lead in creating a new approach to cyber identity theft on a global scale'. That's because of two main factors: 'India has a large capacity in IT, and its digital economy is growing rapidly'. But the law and technology therapies, as the report highlights, are only just getting under way and will offer more effective cures.

In short, the study reveals the dynamics between technology development, law and social impacts. It demonstrates that we must be prepared to adjust both on a national and international level to protect digital lives in the future. India's digital journey has just begun. The outcomes and recommendations can provide critical guidance to policymakers, technical experts and the general public for the effective development of cyber identity protection in the country.

REFERENCES

1. Agarwal, R.: Cyber Laws in India: A Complete Overview (1st ed 2006) p 45
2. Avnish Bajaj vs State (N.C.T.) Of Delhi, (2004). (2005) 3 COMPLJ 364 (Del). Delhi High Court.
3. Brenner, S.: 'Cybercrime Legislation in the United States of America: A Survey' Rutgers Journal of Law and Technology (2001: 7) p 45
4. Duggal, P.: Cyber Law (1st ed 2017) p 67
5. Duggal, P.: Cyberlaw: The Indian Perspective (1st ed 2004) p 89

6. Eichensehr, K.: 'The Cyber-Law of Nations' Georgetown Law Journal (2014: 103) p 88
7. Fatima, T.: Cyber Law in India (1st ed 2017) p 23
8. Gandhi, B.M.: Indian Penal Code (2nd ed 2008) p 101
9. Gupta, A.: Commentary on Information Technology Act (1st ed 2015) p 113
10. Lal, B.: Law of Evidence (23rd ed 2020) p 130
11. Mehra, S.: 'Law and Cybercrime in the United States Today' American Journal of Comparative Law (2010: 58) p 67
12. Misra, A.: 'A Comprehensive Legal Framework of Indian Cyber Laws' International Journal of Law and Government (2013: 1) p 29
13. National Crime Records Bureau. (2023). Crime in India. National Crime Records Bureau. Retrieved April 7, 2024, from https://ncrb.gov.in/crime-in-india.html
14. Sharma, R.: 'Legislation Related to Cyber Crimes in United Kingdom' International Comparative Legal Guide to Business Recovery & Insolvency (2020: 1) p 134
15. Shreya Singhal vs Union of India, (2015). AIR 2015 SC 1523. Supreme Court of India.
16. Smt. Suma Umashankar vs ICICI Bank Ltd, (2016). Criminal Petition No.2570 Of 2014. Karnataka High Court.
17. Verma, P.: Digital Regulations: A Comprehensive Study of IT Laws, Data Protection, Software Licensing, Intellectual Property Rights, and E-Commerce (2nd ed 2013) p 150
18. Weber, A. M.: 'The Council of Europe’s Convention on Cybercrime' Berkeley Technology Law Journal (2003: 18) p 112
19. Weil, G. L.: 'The Evolution of the European Convention on Human Rights' American Journal of International Law (1963: 57) p 78