INTERNATIONAL JOURNAL FOR LEGAL RESEARCH AND ANALYSIS

Open Access, Refereed JournalMulti Disciplinary
Peer Reviewed Edition :

www.ijlra.com

 ISSN: 2582-6433

DISCLAIMER

ISSN: 2582-6433

EDITORIAL TEAM

EDITORS

Megha Middha

Megha Middha, Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar

Megha Middha, is working as an Assistant Professor of Law in Mody University of Science and Technology, Lakshmangarh, Sikar (Rajasthan). She has an experience in the teaching of almost 3 years. She has completed her graduation in BBA LL.B (H) from Amity University, Rajasthan (Gold Medalist) and did her post-graduation (LL.M in Business Laws) from NLSIU, Bengaluru. Currently, she is enrolled in a Ph.D. course in the Department of Law at Mohanlal Sukhadia University, Udaipur (Rajasthan). She wishes to excel in academics and research and contribute as much as she can to society. Through her interactions with the students, she tries to inculcate a sense of deep thinking power in her students and enlighten and guide them to the fact how they can bring a change to the society

Dr. Samrat Datta

Dr. Samrat Datta Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Samrat Datta is currently associated with Seedling School of Law and Governance, Jaipur National University, Jaipur. Dr. Datta has completed his graduation i.e., B.A.LL.B. from Law College Dehradun, Hemvati Nandan Bahuguna Garhwal University, Srinagar, Uttarakhand. He is an alumnus of KIIT University, Bhubaneswar where he pursued his post-graduation (LL.M.) in Criminal Law and subsequently completed his Ph.D. in Police Law and Information Technology from the Pacific Academy of Higher Education and Research University, Udaipur in 2020. His area of interest and research is Criminal and Police Law. Dr. Datta has a teaching experience of 7 years in various law schools across North India and has held administrative positions like Academic Coordinator, Centre Superintendent for Examinations, Deputy Controller of Examinations, Member of the Proctorial Board

ISSN: 2582-6433

Dr. Namita Jain

Head & Associate Professor

School of Law, JECRC University, Jaipur Ph.D. (Commercial Law) LL.M., UGC -NET Post Graduation Diploma in Taxation law and Practice, Bachelor of Commerce.

Teaching Experience: 12 years, AWARDS AND RECOGNITION of Dr. Namita Jain are - ICF Global Excellence Award 2020 in the category of educationalist by I Can Foundation, India.India Women Empowerment Award in the category of "Emerging Excellence in Academics by Prime Time & Utkrisht Bharat Foundation, New Delhi.(2020). Conferred in FL Book of Top 21 Record Holders in the category of education by Fashion Lifestyle Magazine, New Delhi. (2020).Certificate of Appreciation for organizing and managing the Professional Development Training Program on IPR in Collaboration with Trade Innovations Services, Jaipur on March 14th, 2019

Mrs.S.Kalpana

Assistant professor of Law

Mrs.S.Kalpana, presently Assistant professor of Law, VelTech Rangarajan Dr. Sagunthala R & D Institute of Science and Technology, Avadi.Formerly Assistant professor of Law,Vels University in the year 2019 to 2020, Worked as Guest Faculty, Chennai Dr.Ambedkar Law College, Pudupakkam. Published one book. Published 8Articles in various reputed Law Journals. Conducted 1Moot court competition and participated in nearly 80 National and International seminars and webinars conducted on various subjects of Law. Did ML in Criminal Law and Criminal Justice Administration.10 paper presentations in various National and International seminars. Attended more than 10 FDP programs. Ph.D. in Law pursuing.

Avinash Kumar

Avinash Kumar has completed his Ph.D. in International Investment Law from the Dept. of Law & Governance, Central University of South Bihar. His research work is on "International Investment Agreement and State's right to regulate Foreign Investment." He qualified UGC-NET and has been selected for the prestigious ICSSR Doctoral Fellowship.He is an alumnus of the Faculty of Law, University of Delhi. Formerly he has been elected as Students Union President of Law Centre-1, University of Delhi.Moreover, he completed his LL.M. from the University of Delhi (2014-16), dissertation on "Cross-border Merger & Acquisition"; LL.B. from the University of Delhi (2011-14), and B.A. (Hons.) from Maharaja Agrasen College, University of Delhi. He has also obtained P.G. Diploma in IPR from the Indian Society of International Law, New Delhi.He has qualified UGC – NET examination and has been awarded ICSSR – Doctoral Fellowship. He has published six-plus articles and presented 9 plus papers in national and international seminars/conferences. He participated in several workshops on research methodology and teaching and learning.

ISSN: 2582-6433

ABOUT US

INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANLAYSIS ISSN

2582-6433 is an Online Journal is Monthly, Peer Review, Academic Journal, Published online, that seeks to provide an interactive platform for the publication of Short Articles, Long Articles, Book Review, Case Comments, Research Papers, Essay in the field of Law & Multidisciplinary issue. Our aim is to upgrade the level of interaction and discourse about contemporary issues of law. We are eager to become a highly cited academic publication, through quality contributions from students, academics, professionals from the industry, the bar and the bench. INTERNATIONAL JOURNAL FOR LEGAL RESEARCH & ANALYSIS ISSN 2582-6433 welcomes contributions from all legal branches, as long as the work is original, unpublished and is in consonance with the submission guidelines.

www.ijlra.com
Volume 2 Issue 7 | Jan 2024
ISSN: 2582-6433

IDENTITY THEFT AND CYBER CRIMES IN CONTEMPORARY SOCIETY

AUTHORED BY - BERTILA. A, JANESHWAR RAJ Y, ROSY KUMAR[1]

ABSTRACT

The premise of this article is that identity theft is not a recent phenomenon, but rather that the advent of the cyber and information age has given identity thieves new opportunities and presented law enforcement with new procedural and criminal law challenges. Identity theft continues to be one of the fastest growing crimes in the twenty-first century. According to recent trends and developments, no country is completely immune to this highly complex crime. The advancement and expansion of telecommunications technology, which connects computers in networks and allows information to be transmitted between computer systems, has accelerated the processing of personal information. Networks afford more users the opportunity to have access to a wider range of personal information, and enables this information to be shared across varied information technology platforms. The global economy is dependent on the transfer of information, including personal information via global information networks. The collection of personal information is as old as civilisation itself. However, the advancement of information technology has had an impact on the collection and use of personal information. However, sometimes personal information is collected surreptitiously by means of technological inventions that the data subject is not aware of, for example the use of cookies, radio frequency identification tags (RFID tags) on consumer items. The advent and the apparent anonymity of the internet has also progressively facilitated the commission of cybercrimes such as identity theft.

KEYWORDS: *Identity Theft, transfer of information, criminal law challenges, global information networks*

[1] Authors are Assistant Professors of Saveetha School of Law, Chennai

ISSN: 2582-6433

INTRODUCTION

Identity theft is a crime in which a criminal obtains vulnerable information from a victim through deception and uses that information to act in the victim's name. These criminals frequently have their own financial gain to motivate them. Private information like passwords, bank account information, and security numbers are frequently obtained by identity thieves and used to commit fraud in the victim's name. This private information can be used for a number of nefarious activities, such as borrowing money, shopping online, and gaining access to the victim's financial and medical records. Phishing is a practise that is frequently used to obtain vulnerable information from victims and is closely related to identity theft. Criminals can use the information on public social media profiles to imitate their targets. Individuals who have been affected may suffer short-term financial losses as a result of unauthorised transactions made in their names. Victims may face legal charges, changes in their credit status, and damage to their reputations if they are found to be culpable for the criminals actions and assessed by law enforcement agencies. If you're going to utilise your private information online, be sure you're using a secure connection, such as a home or office networks or cellular data. If at all possible, avoid using public Wi-Fi without a password. If you have no other choice, use a VPN, which will encrypt all communications and thus protect you from eavesdropping burglars.

The real-world citizen is becoming a network world citizen (Netizen), and his identity is being challenged as a result. In terms of identity, cyberspace allows us to be whoever we want to be. It enables us to communicate with almost anyone on the planet. Everyone chooses a mask of some sort, a social role, and enters with a new identity.

From this vantage point, virtual identity is comparable to an accepted theory of Dialogicality of Identity, a concept indicating that genre characteristics construct identity. It means that people form their identities by positioning themselves in relation to others. As a result, virtual identity construction can be viewed as something that occurs through discourse.

Although there are virtual identities that correspond to real people in almost every way, most people use cyberspace's illusory anonymity to enjoy the freedom to be whoever they want to be. These people make a variety of masks that are painted with false colours.

ISSN: 2582-6433

The freedom to be anyone implies that a specific individual selects a pseudonym and identifies himself or herself with this pseudonym in cyberspace. The ability to create an identity or virtually change our own identities is limitless. From a legal standpoint, it may cause some issues, because the freedom to be whoever we want means violating the general principle of legal operation.

The emergence of a phenomenon about identity known as virtual identity sparked much debate among identity scholars, and everyone agreed that identity has been challenged. In the age of information technology. Because of the internet's transformation and development of human lifestyle, personality, and identity, emerging issues have made the entry of the law into the information technology environment unavoidable.

WHAT IS IDENTITY THEFT?

"Identity Theft" refers to crimes in which a person obtains and uses another person's data without their consent. The fraudulent or deceptive use of a person's name, date of birth, and other personal information is one example. This can technically be done for monetary gain in order to obtain any type of product or service. Criminals could use this information to obtain fake ID cards, bank accounts, birth certificates, and other important documents.

Defining and understanding identity theft in the cyber and information sphere

Historically, identity thieves committed their crimes by stealing wallets, stealing pre-approved credit applications from mailboxes, or raiding trash dumps for discarded receipts and files[2]. More sophisticated methods, such as securing low-level employment with a financial institution or other entity that gives the perpetrator access to consumer credit reports or other identifying data for personal exploitation or use by organised identity theft rings, have recently gained popularity[3]. Phishing is also a form of identity theft[4].

Phishing is the practise of using emails to dupe victims into disclosing personal and financial information, which is then used to commit identity theft and fraud[5]. Phishing is a particularly dangerous form of identity theft because it costs both the individual consumer and internet use in general. Identity theft and identity fraud refer to the theft of personal information for fraudulent

[2] D Medine 'Prepared statement of the Federal Trade Commission on "identity theft" (1998)
[3] *Ibid*
[4] J Lynch 'Identity theft in cyberspace: crime control methods and their effectiveness in combatting phishing attacks' (2005) 20 Berkley Tech LJ 259.
[5] *Ibid*

ISSN: 2582-6433

purposes, such as account numbers, social security numbers (SSNs), and other personal identifiers such as a mother's maiden name.

Newman and McNally introduced a framework that describes the three basic stages of identity theft and divides the crime into different phases:

- Time 1 (Tl): Date of the first offence (acquiring personal information). The acquisition of personal information at T1 is the first step in a chain of events that leads to identity theft.
- Time 2 (T2): (identity theft) - Personal information obtained at T1 may or may not be directly collected by the offender who uses it at T2 to do the act of identity theft.
- Time 3 (T3): (outcomes of identity theft) - This is the period of discovery and potential criminal justice involvement in the act of identity theft, as well as the realisation of the victim's losses[6].

These different phases, however, do not provide a workable definition of identity theft, but they may help to guide identity theft research and establish a better definition.

Identity theft is the illegal use of another person's identifying facts (name, date of birth, social security number, address, telephone number, or other similar information) to commit an economic fraud, such as opening a bank account, obtaining credit, applying for bank or department store cards, or leasing cars or apartments in the name of another[7].

MODES OF IDENTITY THEFTS

Data theft and the theft of personal data from electronic devices can be performed in several ways.

PHISHING

To deceive the victim into providing crucial information about their identity, the cyber-criminal poses as a bank representative or a contact centre employee. This is called Phishing.

[6] GR Newman & MM McNally 'Identity theft literature review' (2005), available at https./www.ncjrs.gov/pdffilesl/ns)/grants/210459.pdf accessed on 28 February 2023.
[7] WM Grossman 'The other you: the misery of identity theft' (1998) Broward Daily Bus R, 4 September 1998, B.

ISSN: 2582-6433

PHARMING

Pharming is a scamming practise in which a cybercriminal installs malicious code on a user's computer or server, redirecting them to a fraudulent website without their knowledge or consent. Pharming is the practise of disguising fraudulent, data-stealing websites as legitimate and trusted ones. Pharming is a type of online fraud in which criminals use malicious code and bogus websites to install malicious malware on a computer system.

ATM SKIMMING

The concept of "cash anywhere, anytime" fuelled the development of ATMs that made it simple for authorised account holders to withdraw cash. Automated Teller Machines (ATMs) have become the major and important mechanism through which banks provide services to their consumers, sooner or later. It has become a more familiar and connected form of monetary fraud as a result of all of this. Identity theft is the starting point since it leads to other types of crime, and the complete chain of events can result in financial loss[8].

Victims of credit card skimming discover fraudulent withdrawals and charges on their accounts. It is worth noting that all of this occurs while the victim is in possession of the credit card.

It is a type of credit card theft in which crooks frequently use a small device to steal credit card information such as the card number, expiry date, full name of the cardholder, and so on. The information is stolen using a small device known as a "skimmer." When a person swipes his credit card on the skimmer, the skimmer captures all of the data stored on the card's magnetic strip. Thieves use this information to conduct fraudulent transactions and withdraw funds.

Once the information is obtained, the thief can use a cloned credit card to conduct n transactions. Victims of credit card skimming are frequently unaware that their cards have been stolen. Thieves can also install a hidden camera to steal the ATM card's PIN.

HACKING

Hackers obtain unauthorised access to any computer system's data.

"Anyone with the intention or intent to cause any loss, damage, destruction, deletion, or alteration

[8] Debargha Chatterjee, 'Laws that govern ID theft in India' (Ipleaders, 22 August 2021) Laws that govern ID theft in India - iPleaders accessed on 28 February 2023

ISSN: 2582-6433

of any information that resides in a public or any person's computer", According to Section 66[9]. "Diminishing its utility, values, or adversely influencing it in any way" is what hacking is defined as. Hacking violates the fundamental right to privacy guaranteed by the Indian Constitution. It is a method by which viruses, such as malware, divert data from another computer system by decrypting it and transferring it to a hacker who then uses or gives the information to others to commit fraud.

INDIA'S LEGAL EXPLORATION OF IDENTITY THEFT

"Identity" refers to proof of one's existence, whereas "theft" refers to the illegal possession of something without the permission or ownership of the rightful owner. As a result, personal information theft occurs when one person claims ownership of another's existence without their consent or property. Simply put, identity theft occurs when one person accidentally imitates or replicates another. The Black Law Dictionary defines personal information theft as the unauthorised collection and use of another's identity. Personal information theft is a broad term that encompasses a wide range of crimes, from forgery to misrepresentation, though some are classified as traditional crimes, such as ATM skimming and phishing.

This alludes to the heist's wider scope. The Indian Penal Code (IPC) 1860 and the Information Technology Act of 2000 both characterise the theft of personal information as a crime. Theft of personal information is now a crime according to the updated Information Technology Law.

According to the IPC of 1860, electronic recordings are "data, recordings, or generated data, images, sounds, transmissions or receptions in any electronic format," which is similar to the IT Act of 2000's definition of "data, recordings, or generated data, images, sounds, transmissions or receptions in any electronic format". In terms of the laws governing offences involving the theft of personal information, Section 378[10] of the IPC from 1860 specifies that cyberspace is not included in the definition of "theft," which makes the theft of personal information unlawful. The Indian Penal Code of 1860 contains provisions to punish counterfeiting, but does not specifically address "personal information theft" in sections 463, 464, 465, 469, and 474[11]. Following the revision of the IPC in 1860, we divulged private information. These clauses also apply to theft.

[9] Information Technology Act, 2000, S. 66
[10] Indian Penal Code, 1860, S. 378
[11] Indian Penal Code, 1860, S. 463, 464, 465, 469, and 474

ISSN: 2582-6433

Under IPC sections 419 and 420[12], the theft of personal information qualifies as fraud and is punished the same way as spoofing fraud.

The Indian Criminal Code of 1860 included the theft of personal information as a crime and included it as an extension of forgery and fraud. The Information Technology Act 2000 now includes the phrase "personal information theft" as a result of an amendment made in 2008. It took some time for Section 66C[13] of the 2000 IT Act to recognise the need for criminal legislation to protect fraudsters and the misuse of personal identification. The execution of these laws presents the judiciary with yet another important challenge. India lacks the manpower to combat the evolving cybercrime. Personal data theft incidents also rise as a result of people's ignorance of these serious cybercrimes.

NCSP has no plans to implement additional authentication policies because the IT 2000 Act currently only permits one type of authentication policy, IS0027001 ISMS certification, which does not satisfy the legal requirements for such authentication. Without providing the main description, NCSP, 2013, also encourages open standards and public key infrastructure compliance. The policy intends to establish a team of staff worth roughly 50,000 rupees over the course of the next five years, which is insufficient. Overall, the 2013 National Cyber Security Policy was a flimsy, unrealistic blueprint. While it appears that these laws are effective in preventing identity theft, the growing number of reported cybercrimes raises some questions about the laws that are currently in place.

A pornographic MMS clip was created on campus and distributed outside the university in the Jawaharlal Nehru University MMS Scandal[14]. The Mumbai police reported a case of "cyber terrorism" after a threat email was sent to the BSE and NSE. The police tracked down the email address and IP address, and later learned that the sender had included two mobile phone numbers in the personal details column to thwart their efforts to find the suspect.

Investigation led to the discovery that both numbers belonged to a Patna-based company that made photo frames.

[12] Indian Penal Code, 1860, S. 419 and 420
[13] Information Technology Act, 2000, S. 66C
[14] Lionel Faleiro, 'IT Act 2000 - Penalties, Offences with Case Studies' (Network Intelligence, 24 June 2014)

ISSN: 2582-6433

Suhas Katti's case concerned the posting of offensive, offensive, and disturbing messages about a divorced woman in a Yahoo message group. Using a phoney email account created in the victim's name, the accused sent emails seeking information to the victim. Sections 469 and 509 of the Indian Penal Code, 1860, as well as Section 67 of the IT Act, 2000, were found to have been violated by the defendant.

In Sandeep Varghese v. State of Kerala[15], it is claimed that the IPC's Sections 419 and 420 as well as numerous sections of the IT Act, 2000, were violated. The first defendant and others sent emails using fictitious email addresses for numerous clients, suppliers, banks, and other organisations in an effort to malign the names and reputations of the company and its directors. All of the smear campaigns carried out by the mentioned individuals through the use of identity theft have seriously harmed the company's name and reputation.

CONCLUSION

Personal information theft is a serious breach of privacy that has an emotional and social toll on the victims. Theft of personal data, on the other hand, has an abstract impact. Additionally, it threatens institutions and commercial enterprises. The theft of personal information and protection from personal or organisational data are areas where Indian law lags behind international standards in terms of law, policy, and regulation, and there is room for improvement. A strong system with an efficient hierarchy of responsibilities is necessary for the proper application of current law and equal monitoring of the situation[16]. Additionally, it's critical to avoid abuse of power and include enough sympathetic individuals. Finally, governments must create awareness about personal information, their rights and options. Additionally, people look up instances of private information usage on credit reports and inquire as to the justifications for such usage as well as the security measures required to lessen the impact and prevent identity theft.

[15] No.2003 & 2638 of 2010
[16] Debargha Chatterjee, 'Laws that govern ID theft in India' (Ipleaders, 22 August 2021) Laws that govern ID theft in India - iPleaders accessed on 28 February 2023