VOLUME 2 | ISSUE 3

INTERNATIONAL JOURNAL OF ADVANCED LEGAL RESEARCH

LAW RELATING TO DIGITAL IDENTITY THEFT IN INDIA AND ITS INVASION OF PRIVACY

- Adv. Narmada Singh[1]

"If we don't act now to safeguard our privacy, we could all be victims of identity theft"

– Bill Nelson.

ABSTRACT

Notion of Privacy derives from the assumption that all information about a person is in a fundamental way his own, for him to communicate or retain for himself as he sees fit. In modern society, especially, retention of information about oneself is extremely important. However there are few evil minds who steal this information for personal financial gains. This digital theft of sensitive personal information of an individual is known as digital identity theft. In India, law relating to identity theft exists under section 66C of The Information Technology Act, 2000. Identity theft can also be punished under Indian Penal Code, 1860 as it is an extended wing of Forgery and Cheating. This article aims to analyse law relating to digital identity theft and how it invades into Right to Privacy of an Individual. After Justice K.S. Puttaswamy Judgment, Information Privacy also comes within the ambit of Information Privacy. Further, the article also throws light on Personal Data Protection Act (PDPA), 2020, and how identity theft invades privacy. PDPA is the result of Justice K.S. Puttaswamy judgement. However this Act is still in paper and there is no real implementation of the same. This article also provides the steps that an identity theft victim must take.

INTRODUCTION

Identity theft occurs when one person having criminal intentions impersonates to be another person in order to defraud the other person of his money or valuable security by obtaining his personal or financial information without his permission. In layman'sterms,identity theft is a theft when someone steals the personal information of an individual without their permission.

1 Feb. 2022 NET qualified for Assistant Professor and a Law Practitioner at District & Sessions Court Pune & Bombay High Court

The Black Law's Dictionary states identity theft as the unlawful taking and use of another person's identifying data for fraudulent purposes.[2]Personal identification information, like their name, identifying number,Aadhar card, driving licenses, PAN card number, salary slip, phone number, health insurance, or credit card number, and other personal information can be misused by the impersonator to gain an unlawful financial advantage for himself and cause unlawful financial loss to the victim whose information is misused.

Personal identity theft not only strips an individual of their finances but also invades their private space. The privacy of an individual is safeguarded by the constitution of India, thus it becomes the duty of the state to secure this constitutional mandate by providing security to personal data of an individual shared in internet space. Personal identity theft leaves an individual with scare not only abouttheir finances but also about their credit and reputation.

HOW DIGITAL IDENTITY THEFT TAKES PLACE?

Today, in the age of the digital environment, everyone wants to have a presence in the digital ecosystem and that becomes an individual's digital identity. Therefore in today's digital world digital theft of identity as a crime has become more relevant. Thus it is necessary to safeguard the interest of those who are vulnerable to such theft especially children and elder citizens. Identitytheft takes place when an individual's personal information such as biometrics, CVV, credit card numbers, etc. is stolen.

There are many different ways by which identity theft can be committed. It can be committed online as well as in offline mode. The growing use of technologyand the realm of data that we upload online has exposed the personal data of an individual and in consequence, theonline mode of identity theft has become more frequent. Some identity thieves sneakinto trash bins in emails and messages looking for bank accounts and credit card statements. Accessing company databases to obtain lists of client information is a more high-tech technique of stealing of personal information. Identity thieves can destroy a person's credit rating and the status of other personal information once they obtain the information they need.

Digitalmode of identity theft has been progressively used to obtain other people's personal information for identity fraud. To find such information, they may hack into a computer or computer networks, search the hard drives of stolen or discarded computers,access computer-

[2] Henry Campbell Black, Black's Law Dictionary, pg. 443, (9 ed. Thomson Reuters: Minneapolis-St. Paul 2001)

based public records, use information-gathering malware to infect computers,browse social networking sites, or use deceptive emails or text messages by spamming an individual's inboxes with malware link and then when such link is clicked upon by the person to whom it was sent,the person ends up becoming a victim of identity theft. The biggest challenge over and above law is that locating the accused becomes difficult and almost not possible when such theft takes place. Thus, the prosecution of these accused becomes difficult.

HOW IDENTITY THEFT INVADES THE PRIVACY OF AN INDIVIDUAL?

Digital identity theft is stealing of personal information, it evades information privacy of an individual as it is a person's choice on how much and to what extent a person chooses or consents to reveal. After Privacy Judgment it is clear that 'privacy right being a choice of an individual to let someone come near him or not into either the physical space or the mental space'. It is not limited to 'Spatial Privacy' as M. P. Sharma v. Satishchandra and Kharaksingh v. state of UP. In 2017, a petition was filed by Justice K.S. Puttaswamy and Others, the supreme court constituted a 9 judges' bench under Chief Justice J.S. Kehar to examine whether the right to privacy was a fundamental right or not the court stated that 'the right to privacy is protected as an incentric part of the right to life and personal liberty under Article 21 and as a part of freedom guaranteed by part III of the constitution. The privacy judgement did not incorporate a definition of privacy in its final order. However, the individual judgement of the members of the bench which formed 578 pages of the judgement incorporates and reflects on the definition of privacy and these are now the indicators that guide us today as to the definition of privacy and help to establish a link between privacy protection and data protection[3].

Justice Chandrachud, while passing the judgement, highlighted the importance of digital privacy by pointing outthat 'in this age information technology govern virtually every aspect of our lives and it is a task before the court is to impart constitution meaning to individual liberty in an interconnected world. The court has to be sensitive to the needs of and the opportunities and dangers posed to liberty in a digital world.' This discussion of the interconnected world gave rise to the discussion of the term 'Information Privacy' in the judgement[4].

[3] Personal Data Protection Act of India, by author Naavi, pg 19-20
[4] ibid

Justice Chandrachud and members of the bench gave a concept of privacy as follows: Privacy postulates the reservation of a private space for the individual described, as the right to be alone. The age of information has resulted in complex issues for informational privacy. These issuesarise from the nature of information itself. Information has three facets[5] :

1. Information is nonrivalrous in the sense that there can be simultaneous users of the good- use of a piece of information by one person does not make it less available to another.
2. Invasion of data privacy is difficult to detect because it can be invisible. Information can be accessed, stored, and disseminated without notice. Its ability to travel at the speed of light enhances the invisibility of access to data, information collection can be the swiftest theft of all.
3. Thirdly, Information is recombinant in the sense that data output can be used as an input to generate more data output.

This argument has brought Privacy Protection into the domain of 'Data Protection. Therefore, one branch of privacy is 'Information Privacy'. Hence identity theft invades a person's Right to Privacy. The implication of Privacy Judgment is that privacy can be an obligation even on private corporate entities. Once the Personal Data Protection Act, 2020 is effective, the law for establishing such obligations by private persons flows through this act.

Digital identity theft not only invades the privacy of an individual but also causes great damage to an individual which might take months to resolve. In 2022, every big and small organization needs to take steps to secure the privacy of an individual. When privacy is not given the same importance both by the business and consumer alike then the need for security of an individual's personal information arisesbecause sometimes it may lead to identity theft. For instance, a recently reported identity theft was in March 2022, when several Indians complained on social media that unaccounted loans have appeared in their credit history even when they never borrowed any money from Indiabulls-owned Dhani Loans and Services. Fraudsters had reportedly used the permanent account number (PAN) details of people to avail instant loans from the Dhani app. While some complained that they were facing show-cause notices by collection agents for loans they never took, others said their credit scores too had been impacted as credit reports have listed loans they had never availed as defaults. This

[5] ibid

is a major privacy breach, and this has led to identity theft. Hence privacy of an individual is compromised[6].

According to the 2021 Norton Cyber Safety Insights Report[7], the cyber safety major surveyed more than 10,000 adults in 10 countries for the results, among which 1000 adults from India submitted their respective responses. The report indicates that, of 1000 respondents in the country, 36% of Indian adults detected unauthorized access to an account or device in the past 12 months. Every 2 out of 5 Indians experienced identity theft. 14% of the victims were impacted during the past year alone, which indicates that almost 27 million Indian adults experienced identity theft in the past 12 months, as per the reports. The reports also indicate that almost 60% of the entire population of adults and from the older generation have a fear of their identity being stolen. This data is alarming.

LAW RELATING TO IDENTITY THEFT EXISTING IN INDIA (IT ACT & IPC)

In India, digital identity theft is punishable under two legislations namely Information Technology Act, 2000 (IT Act 2000)and Indian Penal code, 1860. These two provisions are often used to serve the punishment for this type of crime.Indian Penal Code, 1860 initially did not include digital identity theft as an offence until it was amended in the light of the Information Technology Act,2000 and the word 'electronic record' was added to it. The word electronic record had a similar meaning as mentioned under sec. 2(1)(t) defines an electronic record as data, record or data generated, image, sound which is sent or received through electronic form. Digital Identity theft has features of both theft and fraud, the basic provisions of fraud, forgery and cheating by impersonation, etc. as provided in the IPC are often invoked along with those of the IT Act[8].

The definition of theft under section 378 of Indian Penal Code, 1860 only includes theft of movable property;theft is the taking of another person's property without that person's permission or consent with the intent to deprive the rightful ownership of the property. The word is also used as an informal shorthand term for some crimes against property, such as burglary, embezzlement, larceny, looting, robbery, shoplifting and fraud. Thus, it does not apply to digital identity theft due to differences in the nature of the theft.

[6]Explained: What is identity theft and how you can protect your personal data online - Times of India (indiatimes.com)
[7] 2021_NortonLifeLock_Cyber_Safety_Insights_Report_Global_Results.pdf (symassets.com)
[8] https://jcil.lsyndicate.com/wp-content/uploads/2016/08/Aishwariya-Joshi.pdf

However, certain provisions of Indian Penal Code, 1860 can be invoked in case of digital identity theft and those are, forgery and fraud. Earlier before the amendment was made to Indian Penal Code, 1860these definitions only applied to false documents. But after the Information Technology Act 2000 came into force the Indian Penal code was amended IT 2000 to include electronic records and hence its ambit was widened to include computer datarelated crime as well.

Thus, after the amendment in the Indian Penal Code, 1860 the following Sections 463, 464, 465, 469, 471, 474 will include Digital Identity theft. Sections 468 and 471, for example, can be triggered when a person creates a fake website in the nature of an electronic record in order to trick victims into giving sensitive information with the goal to defraud them. In addition, Section 419 can be used in circumstances where the accused has impersonated the victim by using the victim's personal identifying information to perpetrate fraud or deceit. If "everything capable of being turned into a valuable security" within the meaning of the act is construed to include an individual's unique identification information, Section 420 can be utilised[9].

Even though Indian Penal Code, 1860 to a large extent apply todigital identity theft crime but it did not specifically upon digital identity theft as it was read as an extended branch of forgery and cheating. There was a need for an identity theft crime specific section which would define Identity theft and lay down a punishment for the same. In India, Information Technology Act 2000 is the only act which dealt with cybercrime[10]. However,this single legislation had no mention regarding Identity Theft, it was only after the 2008 amendment of the India Information Technology Act, that section 66C[11] was added, it is the only section which specifically defines Identity theft. According to this sectionwhoever, fraudulently or dishonestly makes use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of eitherdescription for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh[12].

Section 66D penalises cheating by impersonation by means of any communication device or computer resource with imprisonment of either description for a term which may extend to

[9] https://indraprasthalawreview.in/wp-content/uploads/2020/10/ggsipu_uslls_ILR_2020_V1-I1-13-aditi_palit-abhishek_kushwaha.pdf
[10] ibid
[11] https://www.itlaw.in/section-66c-punishment-for-identity-theft/
[12] ibid

three years and shall also be liable to a fine which may extend to one lakh rupees.Though this section does not mention the word phishing but is still inclusive of Phishing and its extended forms as, in phishing, there is impersonation for the purpose of cheating or duping people to extract data.

DRAWBACKS OF IDENTITY THEFT LAW IN INDIA

Section 66C provides imprisonment up to three years, or/and with a fine up to Rs. 1,00,000.The fine provided in the section is not sufficient. Digital identity theft is a broad term that encompasses a variety of crimes of varying severity. A spoofing criminal can steal property worth thousands of rupees from a single person or millions of rupees from a vast community. In either case, a symbolic fine of not more than rupeesone Lakh would be issued. In addition to other sections of the Indian Penal Code, which may be combined with Section 66 C of the IT Act, do not specify a fine limit (upper or lower) or the manner in which it should be calculated, leaving it to the discretion of the court.

Regardless of the fact that the IT Act applies to everyone who is involved in identity theft involving any computer resource in India, jurisdiction concerns remain and cannot be reconciled. When a non-Indian citizen is charged, the nation of his citizenship is considered, and it is examined whether their country is yet to conclude an extradition deal with India. It is impossible to apprehend such a suspect if such extradition legislation does not exist.

The Act is insufficient in light of the compensation awarded to the victim. The compensation given is capped at 1 crore under Section 43 of the IT Act, and it is increased to 5 crore if the loss of data is committed by a body corporate. A victim may lose more money than this, but that isn't taken into account. Furthermore, under Section 47 of the Act, whenever claims below 5 crore, the adjudicating officer must consider solely the victim's tangible/quantifiable loss when awarding compensation. As stated previously in the article, the victim suffers a great deal of emotional stress and hardship as a result of the crime, depending on the subsequent offence to which the victim is subjected it takes a massive amount of time and resources to reclaim a damaged reputation or rectify a credit record, which should be factored into compensation calculations.

Identity theft is currently a cognizable, bailable, and compoundable offence under the IT Act. Section 77A states that an offence committed under section 66C is a compoundable

offence. Laws are intended to serve the dual goals of crime prevention and deterrence. It is impossible to escape identity theft by anticipating it. In the instance of this crime, a deterring effect can be generated by simply investing a certain amount of aforethought before executing it. This can be accomplished by applying harsher penalties and/or fines. Furthermore, a three-year prison sentence is insufficient and will not act as a deterrent. Making the provision bailable may give the accused an opportunity to obstruct the investigation.

HOW PERSONAL DATA PROTECTION ACT CAN PREVENT IDENTITY THEFT?

Parliament has passed a bill in 2020 known as Personal Data Protection Act, 2020 (PDPA)that may contribute to the quest of achievingthe security of the personal data of individuals**.** This bill was passed in the light of Right to Privacy Judgement. It is the first comprehensive Act in addressing 'Protection of Privacy' of Indian citizens. Once this Act is implemented it will be a game-changer in the aspect of protection of personal data in terms of information privacy. Since PDPA is a separate legislation, it is more strong in terms of implementation and also in terms of creating a deterrence effect. European Union's General Data Protection Regulation(GDPR) has been imbibed into the Indian PDPA along with several improvements. PDPA is therefore an improvement over GDPR as it should be since it is being enacted two years later with the knowledge of how the GDPR rollout affects the industry. Therefore, it is high time we implement PDPA since it is has been over two year from the date of passage of PDPA bill in Parliament. PDPA implementation will keep cybercrime under check.

Steps to be taken by victims of identity theft in India:

These are the following steps that a victim of identity theft should immediately take upon gaining knowledge of such crime[13] -:

1. File a report of identity theft:

   The report of such theft can be lodged with the following individuals:

   (i) One can go to their local police station and report this identity theft.

   (ii) One can also go to the cybercrime cells in their respective cities and report about such identity theft and that duty-bound to register a case on your complaint.

[13]Identity theft cyber crime in India (cyberguard.in)

(iii) In case one finds that even after reporting there is some danger then they could seek further assistance from Indian Statutory Authority. They are also known as the Indian Computer Emergency Response Team or I-SERT. They have been made the Nodal Agency for cyber security in India.

Under the Information Technology Act 2000 one can also report about their identity theft to the I-SERT or Indian Computer Emergency Response Team because this is the kind of a cyber security breach and I-SERT is dedicatedly working on such complaints.

2. Further if a victim is doing any internet transactions then they must instantaneously inform or notify all the relevant service providers in this regard. With that they should also monitor their credit score regularly on CIBIL and keep a track of their CIBIL score.

3. Check their mailboxesregularly. Make sure no one has requested an unauthorized address change, title change, PIN or ordered new cards or checks to be sent to another address. If a thief has stolen one'semail to get credit cards, bank and credit card statements, pre-screened credit offers or tax information, or if an identity thief has falsified change-of-address forms, that's a crime. This must be reported to the police.

4. Maintain a written chronology of what happened, what was lost and the steps one took to report the incident to the various agencies, banks and firms impacted. They should be sure to record the date, time, telephone numbers, the person they talked to and any relevant report or reference number and instructions.

CONCLUSIONS

India has a law relating to digital identity theft under Information Technology Act 2000. In India, data protection laws aren't very robust right, but the planned Personal Data Protection Bill, 2020 (PDPA) is a step in the right direction this is a positive step toward enacting stringent data privacy legislation. The Personal Data Protection bill is inspired by European Union's General data protection Act (GDPR), 1996 and applies to both government and private companies. However, unfortunately PDPA is still on paper and there is no real implementation of this act. It is high time that Government of India should bring this Act to

actual practice and save their citizens personal data from further being exploited in the hands of cyber criminals.

However, a lot of work still has to be done on cybercrimes, as the maximum population sharing personal and private data on the internet are not aware that they are exposed to the threat of cybercrimes like identity theft and digital cloning.

Children and the elderly population are the most vulnerable population likely to be a victim of cybercrimes. TheseCyber technology users lack knowledge as to how much private information they should share on Internet space or if they consent to share their private information with any organization on the internet or with e-commerce companies, they are not aware of what steps are taken by these companies to secure their sensitive personal data. Even though we have legislation on identity theft, its implementation is not up to the mark. The designated Police personnel are often not properly trained to deal with cybercrimes. Education and training of investigating officers are most important to understand and implement cybercrime reports.

The legislature should create progressive mechanisms and rules to prosecute identity thieves. However, it is also important to prevent data theft entirely by enacting stricter data protection legislation. The most common places where sensitive identifying information might be obtained are fromservice providers, which are primarily BPOs and IT firms holding a global database of people's personal information and can be accessed by cybercriminals.

These days, with technological advancements, various online financial payment applications are using biometric scan. Government should encourage more and more online payment methods to provide biometric scan facility. Government should also provide a grant for cyber security implementation. Cybercrime is also a crime and the amount of fine to be awarded should be at the discretion of court depending upon each case.

Lastly government needs to spread awareness among the internet users regarding sharing of sensitive personal information online and its consequences. Initiative should be taken by the government to educate the internet users on their rights and the redress mechanisms accessible to them in the event of a violation in case of identity theft, in order to reduce the impact on identity theft and to detect identity theft early.

The law relating to identity thefts in India needs slight amendment, as suggested, with the amendment in existing laws and its effective implementation, instances of identity theft can

be controlled. The time has come when the government must act and Implement PDPA instead of criticising the different versions of data protection laws. Tech giants continue to lobby with the government to delay the inevitable, government must act in favour of its citizens.

"Like other forms of stealing, identity thefts leaves the victim poor and feeling terribly violated." – George W. Bush