A REVIEW OF UNIQUE IDENTIFICATION AND IDENTITY THEFT- THE INDIAN STANDPOINT

Farha Khan[1,2], Rituja Sharma[1]

[1]*School of law, Banasthali Vidyapeeth, Rajasthan, India- 304022,*

[2] *Graphic Era Hill University Bhimtal Campus, Nainital, Uttarakhand, India- 263132,*

Abstract: India is transforming the global digital scene in the twenty-first century with programmes like the Aadhaar-enabled payment system, the Agrimarket app, Beti Bachao Beti Padhao, Crop Insurance Mobile App, and others. Though digitization creates an ecosystem that contains a variety of data that can be filled in a variety of ways by an individual, there is concern about the data's fortification. The topic of data fortification in terms of material, routine, and curative ways must be tackled as soon as such ecosystems are developed, and without fail. The rising concept of digitization in India is examined in relation to unique identification, identity theft, and data security regulation in this research paper. With an emphasis on India, the purpose of this essay is to demonstrate the importance of data protection rules across the board, as well as the implications of failing to integrate privacy and data protection principles in the mandate. According to a thorough literature review, identity theft and other cybercrimes are growing at an alarming rate and must be handled to prevent inhabitants of the Republic of India from becoming victims. The study looks into the inequality of identity theft, as well as the harm it does to persons whose identities are stolen and the social order. Doctrinal and theoretical techniques are employed to find appropriate answers to the study difficulties.

1. INTRODUCTION

In recent years, the requirement to build digital identification has prompted several governments to create identity information ecosystems. The availability of an individual's biometrics data is one of the most critical requirements for establishing such an ecosystem. Governments will surely benefit from this technical advancement in changing their inefficient paper-based system to a more sophisticated system. However, there is cause for concern when it comes to the security of such information. As soon as such ecosystems are formed and maintained, the issue of data protection in terms of substance, procedure, and remedy must be addressed. Governments that save such data without safeguarding the privacy of the general public can use it to determine surveillance, repression, and social control, which can then lead to identity theft by cyber criminals. Biometrics is the term for a person's unique identifier, which allows them to be distinguished from others in terms of identification. The most often used biometric is fingerprint recognition, which is followed by iris recognition, DNA recognition, facial recognition, voice recognition, and signature recognition. Biometric data storage by governments around the world is not a new concept; it has been used by the US, Europe, and many other countries under various programmes since 1900. The Indian government joined the race in 2009, storing biometric data on individuals and bringing the Aadhaar project under the umbrella of the "UIDAI" plan (Unique Identification Authority of India). A 12-digit Unique Identification number is assigned to each enrollee. An Aadhaar card stores an individual's biometrics and demographic data, including fingerprints, iris, and date of birth, as well as sex, the citizen's address, and an image.

2. IDENTITY THEFT AND THE DEVELOPMENT OF THE CONCEPT OF UNIQUE IDENTIFICATION

Since the beginning of time, humans have used physical features such as voice, face, and stride to distinguish themselves. Alphonse Bertillon, the chief of the Paris police department's criminal identification unit, conceived and subsequently implemented the idea of employing a range of bodily assessments to identify criminals in the mid-nineteenth century. Just as his theory was gaining acceptance in the late 1800s, it was debunked by a more convincing and accurate examination into the uniqueness of human fingerprints. The idea of collecting criminals' fingerprints and preserving them in a database was eventually adopted by several significant law enforcement agencies. The fingerprints acquired at the crime scene can then be compared to fingerprints in the records to discover who the perpetrators are. Despite the fact that biometrics arose from law enforcement's widespread use of the technology to track down criminals. It's becoming more common to utilize it to authorize person recognition in a variety of civilian applications. Fingerprints have been used for identification and verification since 500 BC and are still the most frequently accepted and used method today. Following the introduction of biometric identification by Sir Francis Galton, who was of English heritage and favored slavery, dominion powers kept suspect identification offices in India and Egypt. The Bengal police also admitted to calibrating the biometric identification system. Keeping a database of such unique person identifications is one thing; protecting such databases so that they cannot be misused by others is quite another. Cyber thieves can utilize a freely available database containing individual personal information for their own purposes. Identity theft is one of them.

Identity theft happens when a person gets another person's personal and financial information with the goal of getting benefits for themselves by conducting any type of transaction or purchase using that person's name or identity. In ancient times, identity theft took the form of somebody pretending to be someone else and being purposely untruthful. As industrialization and technological improvements proceeded, most identity thefts began with the introduction of credit cards and the usage of more and more verification methods in government. This section provides a brief review of current identity theft trends and how they relate to data security.

2.1 Identity Theft Timeline

The frequency of identity theft offences has increased as modernization has happened in any field, whether digital or not, as the history of identity theft shows. It is now largely acknowledged as the fastest-growing illegal enterprise on the planet. People who wished to stay anonymous or who needed a fresh start would steal your entire identity, including your name, social security number, entire family background, career information, and even your life storey. It's probable that this occurred after a murder, when more moral criminals hunted for dead people with similar enough identities to assume. "Ghosting" is the term for the process, and it has been the subject of numerous books and films. A clever thief can access the victim's bank accounts, apply for new credit cards, and even file fraudulent tax returns. One of the most well-known ghosting episodes from the 1930s involved actor Wallace Ford.

Phone-based identity theft had become a severe problem by the 1960s. The caller would claim that they were phoning to give the person lottery winnings or other gifts, but that they needed some personal and financial information in order to do so. The offender would then use the information to entirely assume the victim's identity or to commit financial fraud. At this stage, few identity thieves desired to

depart and start a new life. These were the strategies stated when the term "identity theft" was invented in 1964, according to the Oxford Dictionary. By the 1980s, criminals had to evolve. Scams involving phones were well-known, and victims were well-informed. Identity thieves began looking for critical personal information in garbage cans outside homes and businesses, such as bank statements, credit card offers, invoices, pay stubs, and other revealing documents. In the late 1980s, television and print media sufficiently publicized this method for individuals and businesses to begin purchasing small paper shredders.

In the 1990s, the emergence of residential and commercial internet connections opened up a whole new world. Unfortunately, identity thieves were up to date as well, and they only cared about one thing: money. Within ten years, up to 62 percent of identity theft cases were performed through the internet, according to the FTC. By 2011, the majority of data theft was due to hacking, which included the use of viruses, malware, and other methods of gaining unauthorized access to computers. This terrible new sort of theft prompted a flood of "IDENTITY THEFT PROTECTION" companies to spring up. Authorities responded with isolations as the virus spread over the world in 2020, and digital trade prospered as internet connectivity lagged. Digital ratification has reduced a five-year time period to just two months across the board (McKinsey). India's expenditure arrangements in the areas of commerce, health management, and E-payments show this reversal. This has given criminals a fantastic opportunity to perpetrate crimes like identity theft, data privacy violations, and other types of cybercrime without ever having to leave their homes. As a result, strong laws to handle this threat should be enacted. Theoretical techniques are employed to identify appropriate solutions to the study's problems.

2.2 Prevalence of Identity Theft

Identity theft is regarded to be the crime of the century, the most recent and most heinous of a series of heinous white collar crimes. Almost everyone is at risk, as data fraud instances continue to make international news on a daily basis. In developing countries and economies, such as India, the instances are fast increasing. Personal information is sold to criminals who utilize it to their advantage. They take on phony identities to get loans, get jobs, buy cars, rent houses, accumulate debts, and even commit severe crimes. To avoid the nightmare misuse, helpless victims are obliged to legally change their names and personal information. The majority of the damage occurs in the first few hours, while untangling from the tangle takes years. The public is increasingly concerned about death shame, financial ruin, reputation blemishes, and life disaster. What is more essential than your name, after all?

There is no going back after your 12 digit card number, 15 digit account number, and basic details have been put into cyberspace. We're all sitting ducks in the hands of clever thieves looking for "quick– cash." Identity theft is the leading cause of fraud in India, accounting for 77% of all fraud incidents. [10 February 2016 – India] The 'Fraud Report 2016' was released by Experian India.'[1] According to the 2017 Experian fraud report, Indian consumers are the most vulnerable to online fraud in Asia Pacific: 2017 Experian Fraud Insights[2].With more than 5,000 cases reported to police in 2018, India's southern state of

[1] available at https://www.experian.in/identity-theft-is-the-largest-contributor-to-fraud-in-india]
[2] (available at https://www.experian.in/indian-consumers-have-the-highest-exposure-to-online-fraud-within-asia-pacific-experian-fraud-insights-2017).

Karnataka had the greatest number of registered offences linked to online identity theft. In that year, the country had around 6,700 occurrences of online identity theft. Section 66C of the Indian Penal Code covered this type of offence [see Internet/cybercrime and security-number of online Identity Theft reported across India in 2018 by key state police departments]'[3]. According to the 2019 Norton Life Lock Cyber Safety Insights Report, 63 percent of Indians are unsure what they will do if their identities are stolen, despite the fact that 70 percent are concerned. In India, four out of ten people have had their identities stolen. "Cyber thieves stole Rs 1.2 trillion from Indians in 2019: Survey," Mehta Ritu, 2020"[4]. In 2020, a score of 223 out of 300 indicates that Indians are concerned about national, financial, internet, and personal security, as measured by the survey. Identity theft has raised to the top of Indians' security concerns, with 83 percent saying it is a serious problem. [Identity theft tops Indian consumer security concerns: Unisys Security Index,' Sangani Pankaj, June 24, 2020]'[5].

2.3 Cybercrime statistics and legislation - India

3.1 Cybercrime Statistics

This section of the article will attempt to briefly examine cyber crime data from 2014 to 2018, as provided by the National Crime Records Bureau (NCRB), an Indian government agency dedicated to serving as a repository of information on crime and criminals. The three types of cybercrime recorded on the NCRB website are as follows. That is, situations involving cybercrime as defined by the IPC, IT, and SLL Acts. Total offences recorded under the IT Act were 7201, total offences reported under the IPC (Cyber related) were 2272, and offences reported under SLL (Cyber related) were 149, bringing the total number of reported cyber offences to 9622 in 2014. In 2015, there was a significant increase in the graph of cybercrime. The entire number of offences reported under the IT Act was 8045, the total number of offences reported under the IPC (Cyber related) was 3422, the number of offences recorded under SLL (Cyber related) was 125, and the total number of reported cyber offences under all headings was 11592. The number of cybercrime offences increased in 2016. Total cyber offences recorded under the IT Act were 8613, IPC (Cyber related) offences were 3518, and SLL (Cyber related) offences were 186, for a total of 12317 reported cyber offences under all headings. The year with the largest number of cybercrime reports was 2017. Total offences reported under the IT Act were 13635, total offences recorded under the IPC (Cyber related) were 7976, and the offences reported under SLL (Cyber related) were 185, bringing the total number of reported cyber offences to 21796. However, the total number of cybercrime incidents decreased somewhat in 2018. Total offences reported under the IT Act were 18495, total offences recorded under the IPC (Cyber related)

[3] available at https://www.statista.com/statistics/1097526/india-number-of-online-identity-theft-offences-registered-by-leading-state/

[4] available at: https://economictimes.indiatimes.com/wealth/personal-finance-news/cyber-criminals-stole-rs-1-2-trillion-from-indians-in-2019-survey/articleshow/75093578.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst].

[5] available at: https://economictimes.indiatimes.com/tech/internet/identity-theft-tops-indian-consumer-security-concerns-unisys-security-index/articleshow/76552105.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

were 8647, and the offences reported under SLL (Cyber related) were 106, bringing the total number of reported cyber offences to 27248. (See Figure 1 and Figure 2)

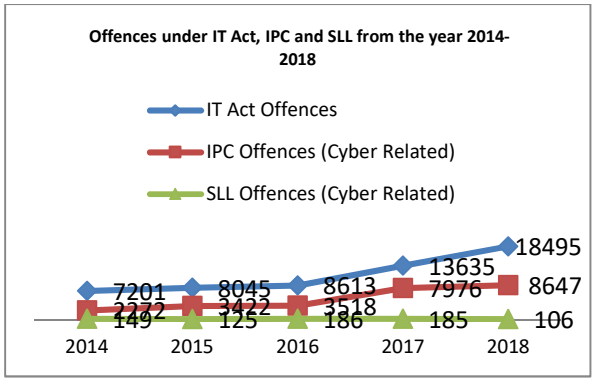

Figure 1

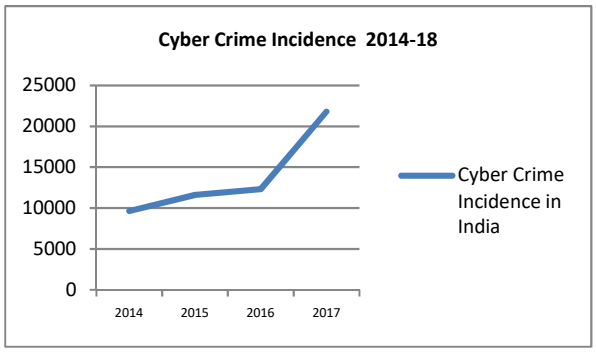

Figure 2

Durkheim's argument was that a person's feeling of culture and subculture can be one of the causes of deviant conduct when they find it difficult to accept the norms of mainstream society. Every day, the number of crimes in India increases (NCRB). According to cyber crime statistics from 2014 to 2018, the percentage fluctuation in the number of crimes is increasing with each passing year. From 2014 to 2015, there was a 20.5 percent increase, 6.3 percent increase from 2015 to 2016, 76.9% increase from 2016 to 2017, which was the largest, and 25.01 percent increase from 2017 to 2018. (See Figure 3)

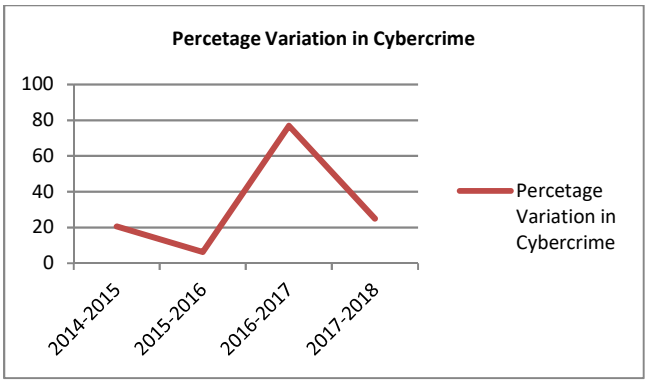

Figure 3

3.2 Cyber legislation in India

The rise in frauds and cyber crimes is driving the Indian government to take steps to defend citizens' rights, particularly against cyber crimes and fraudulent activities. Stronger legislation is being drafted to protect citizens' data and privacy. Wrongfully obtaining a person's personal information is done with the goal of inflicting legal injury to the person whose information was obtained. Identity theft occurs when a person commits both fraud and theft, hence the laws of the Indian Penal Code, 1860 (IPC), as well as the Information Technology Act, 2000, are frequently cited. Forgery – sec 464, Making false documents – sec.465, Forgery for the Purpose of Cheating – sec.468, Reputation – sec. 469, Using as Genuine a Forged Documents – sec.471, and Possession of a document known to be Forged and intending to use it as Genuine – sec. 474 are some of the sections of the Indian Penal Code that can be combined with those in the Information Technology Act. The Information Technology Act of 2000 (IT Act) regulates cybercrime in India. The following are the sections that deal with cybercrime and theft:

O Sec.43- Penalty and compensation for computer/operating system damage, etc.

O Computer-related offences (Section 66).

• Sec.66B- Penalty for receiving stolen computer resources or any other communication equipment dishonestly.

• Section 66C: Penalties for identity theft

• Sec.66D- Punishing a person for impersonating computer resources in order to cheat.

Sections 147A and 419A of the IPC (Indian Penal Code) have been recommended by the government for inclusion. Cheating by utilizing any unique identity feature of another person is punishable by imprisonment for a term of up to three years, a fine, or both under Section 147A. Cheating by impersonating utilizing a network or computer resource is punishable under Section 419A by imprisonment for a term up to 5 years, a fine, or both.

With the rise in cybercrime and fraud, the government is developing more precise rules and regulations to defend the public's interests and protect them from any cybercrime. More stringent rules have been enacted to ensure the protection of "sensitive personal data" in the hands of intermediaries and service providers (corporations), assuring data security and privacy.

2.4 Conclusion

Many examples of impersonation were highlighted in NCRB's 23rd edition of "Finger Prints in India" for the year 2019. The cases involve offenders impersonating others using their fingerprints for various purposes. The book offers information on key cases that the Central Finger Print Bureau (CFPB) and State Finger Print Bureau (SFPBx) have solved using Finger Print Science. Digitization has both beneficial and negative aspects. The widespread use of the Internet and reliance on technology undoubtedly boosts productivity and lowers costs, but the rising rate of cybercrime casts a pall over the positive aspects of the situation. With the aid of technology, the criminal is able to target individuals in any region of the world. The larger the number of online transactions, the greater the risk of losing personal information and becoming a victim of identity theft, which has been elevated to the rank of a mainstream crime due to the millions of people who have been victims of identity theft around the world. The NCRB statistics from recent years clearly shows that cyber crime is expanding at an alarming rate every year. There has been an instance where the government started efforts to grant IDs to Indian citizens, but that personal data was discovered on a public platform where it might be misused by anyone. The Digital India initiative has had a huge impact on the Republic of India in terms of ensuring an unrivalled future for every person; however the lack of comprehensive data security and privacy regulations is a source of concern. The Indian government has taken steps to protect citizens' rights by amending numerous laws relating to data protection, data privacy, and data theft, but these efforts are insufficient to fulfill current data protection and privacy needs. The Indian government must yet solve the hurdles of striking a balance between digitization and data protection by enacting more severe and well-considered legislation.

References

[1]. Dixon Pam. 2017 "A Failure to ‘Do No Harm’- India’s Aadhar biometric Id Program and its inability to protect privacy in relation to measures in Europe and the U.S.” Springer, Health Technol. DOI 10.1007/s12553-017-0202-6

[2]. Chauhan Swati, Sharma Chetanshi, Geetanjali, Verma Akshita, Gupta Jaya. 2014 “Survey Paper on UID System Management.” International Journal of IT, Engineering and Applied Sciences Research(IJIEASR), Volume 3, NO. 2, February.

[3]. Martin Andrew, Martinovic. 2016, "Security and Privacy Impacts of a Unique Personal Identifier” University of Oxford, Cyber Studies Programme, working paper series- no.4 www.politics.ox.ac.uk/centre/cyber-studies-programme.html.

[4]. Roberds William, L.Schreft Stacey 2009, “Data Breaches and Identity Theft”, Elsevier, Journal of Monetary Economics 56, 2009, 918-929.

[5]. Zelazny Frances, 2012, "The Evolution of India's UID Program- Lessons Learned and Implications for other Developing Countries", Center for Global Development, www.cgdev.org.

[6]. Bhalla Ajay. 2020, "The latest evolution of biometrics", Biometric Technology Today, Volume 2020, Issue 8, Pages 5-8, https://doi.org/10.1016/S0969-4765(20)30109-0

[7]. Barnes G. Jefferey. "Chapter 1, History" see page 15, Available at https://www.ncjrs.gov/pdffiles1/nij/225321.pdf

[8]. Kak U. Amba, Malik Swati. 2010 "Privacy and the National Identification Authority of Indian Bill: Leaving Much to the Imagination", NUJS Law Review, Volume 3, Issue 4.

[9]. See 'what is Addhaar' at https://uidai.gov.in/what-is-aadhaar.html

A. K. Jain, A. Ross and S. Prabhakar, "An introduction to biometric recognition," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 14, no. 1, pp. 4-20, Jan. 2004, doi: 10.1109/TCSVT.2003.818349

[10]. Bhable G. Suvarnsing, Kayte Sangramsing, Maher Raju, Kayte Jaypalsing, Kayte Charansing, 2015 "DNA Biometric", IOSR Journal of VLSI and Signal Processing(IOSR-JVSP), Volume 5, Issue 5, Ver. I (Sept-OCT.2015), PP 82-84.

[11]. Breckenridge Keith. 2014, "Biometric State-The Global Politics of Identification and Surveillance in South Africa, 1850 to the Present", Cambridge University Press. Available at https://libcom.org/files/keith-breckenridge-biometric-state-the-global-politics-of-identification-and-surveillance-in-south-africa-1850-to-the-present.pdf

[12]. Sengoopta, Chandak. (2003). Imprint of the Raj: How Fingerprinting Was Born in Colonial India. The English Historical Review.

[13]. Moses, Agana. (2015). "Cyber Crime Detection and Control using the Cyber User Identification Model", IRACST-International Journal of Computer Science and Information Technology & Security, Vol. 5, No 5.

[14]. Rupper, Aliene Carrie. 2005, "Identity theft prevention in CyberCIEGE", http://hdl.handle.net/10945/1811.

[15]. Farina A Katie 2015 "Cyber Crime: Identity Theft", Elsevier Ltd. Available at https://coek.info/pdf-cyber-crime-identity-theft-.html

[16]. World Privacy Forum, 12625 SW 62ND Ave., Portland, OR 97219, USA

[17]. Aiyar. S. 2017. Aadhar: A biometric history of India's 12- Digit Revolution. India: Westland.

[18]. Harper. J. 2006. Identity Crisis: How Identification is overused and misunderstood. Washington DC: CATO Institute.

[19]. K. Hoffman S. 2010. Identity Theft: A reference handbook. Santa Barbara: ABC-Clio.

[20]. Khera. R. 2019. Dissent on Aadhar (Big data meets Big brother). India: Orient Black Swan

[21]. Mc Nally M. 2012. Identity Theft in Today's world. Santa Barbara: Praeger.

[22]. Ramnath. NS, Assisi. C. 2018. The Aadhaar Effect: Why the World's Largest Identity Project Matters India: Oxford University press

[23]. Atlantic Publishing Company 2008, “The Online Identity Theft Prevention Kit: Stop Scammers, Hackers, and Identity Thieves from Ruining Your Life”, Atlantic Publishing Group Inc. (February 28, 2008).

[24]. Bhardwaj Kritika 2017, “Explainer: Aadhaar is vulnerable to identity theft because of its design and the way it is used”, https://scroll.in/article/833230/explainer-aadhaar-is-vulnerable-to-identity-theft-because-of-its-design-and-the-way-it-is-used

[25]. BQ Desk 2018, “Aadhaar’s Security Questioned Again: Are Indians At Risk Of Identity Theft?”,https://www.bloombergquint.com/law-and-policy/2018/01/04/aadhaars-security-questioned-again-are-indians-at-risk-of-identity-theft#gs.x0yrlz4.

[26]. Chauhan Swati, Sharma Chetanshi, Geetanjali, Verma Akshita, Gupta Jaya 2014, "Survey Paper on UID System Management", International Journal of IT, Engineering and Applied Sciences Research (IJIEASR), Volume 3, No.2 , ISSN: 2319-1113, www.irjcjournals.org

[27]. Das S.K. 2015, " Making the Poor Free?: India's Unique Identification Number", Oxford University Press.

[28]. Goyal Gaurav , Kumar Ravinder 2010, “The Right to Privacy in India: Concept and Evolution”, Partridge India 11 January 2016.

[29]. Hinde Stephen, Bupa , 2008 "Identity theft: the fight”, Computer Fraud & Security, http://www.spinaltwist.eclipse.co.uk/Files/Dissertation/ID/Hinde.%20S.%20-%20Identity%20theft%20-%20the%20fight.pdf

[30]. Jim Stickley 2008, “The Truth about Identity Theft”, Que Publishing; 1 edition September 1, 2008.

[31]. Joshi Aishwarya 2016, “Identity Theft- A Critical and Comparative Analysis of Various Laws in India”, Journal on Contemporary Issues of Law (JCIL), Vol.2 Issue 6. jcil.lsyndicate.com/volume-2-issue-6-july-2016/.

[32]. Martin Andrew, Martinovic. 2016, "Security and Privacy Impacts of a Unique Personal Identifier” University of Oxford, Cyber Studies Programme, working paper series- no.4 www.politics.ox.ac.uk/centre/cyber-studies-programme.html.

[33]. Megan McNally 2012, “Identity Theft in Today's World”, Praeger, Santa Barbara.

[34]. M. Vieaitis Lynne, Copes Heith, A.Powell Zachary, Pike Ashley 2014 “A little information goes a long way: Expertise and Identity theft”, Elsevier, Aggression and Violent Behaviour 20, 2015, 10-18, http://dx.doi.org/10.1016/j.avb.2014.12.008.

[35]. Pemble Matthew 2008, “Don't panic: taxonomy for identity theft”, Elsevier, Computer Fraud & Security, Volume 2008, Issue 7, July 2008, Pages 7-9, https://doi.org/10.1016/S1361-3723(08)70111-8

[36]. Roberds William, L.Schreft Stacey 2009, “Data Breaches and Identity Theft”, Elsevier, Journal of Monetary Economics 56, 2009, 918-929.

[37]. Sandra K. Hoffman, Tracy G. McGinley, 2010, “Identity Theft: A Reference Handbook”, ABC-Clio Santa Barbara.

[38]. Siddharth Raju Raja, Singh Sukhdev, Khatter Kiran 2017, “Aadhar Card: Challenges and Impact on Digital Transformation”, Cornell University Library, Computers and Society (cs.CY), arXiv:1708.05117v1 [cs.CY], https://arxiv.org/abs/1708.05117.

[39]. Zelazny Frances, 2012, "The Evolution of India's UID Program- Lessons Learned and Implications for other Developing Countries", Center for Global Development, www.cgdev.org.
[40]. Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016
[41]. Indian Penal Code, 1860.
[42]. Information Technology Act, 2000.
[43]. Information Technology (Amendment) Act, 2008.
[44]. The National Identification Authority of India bill, 2010.