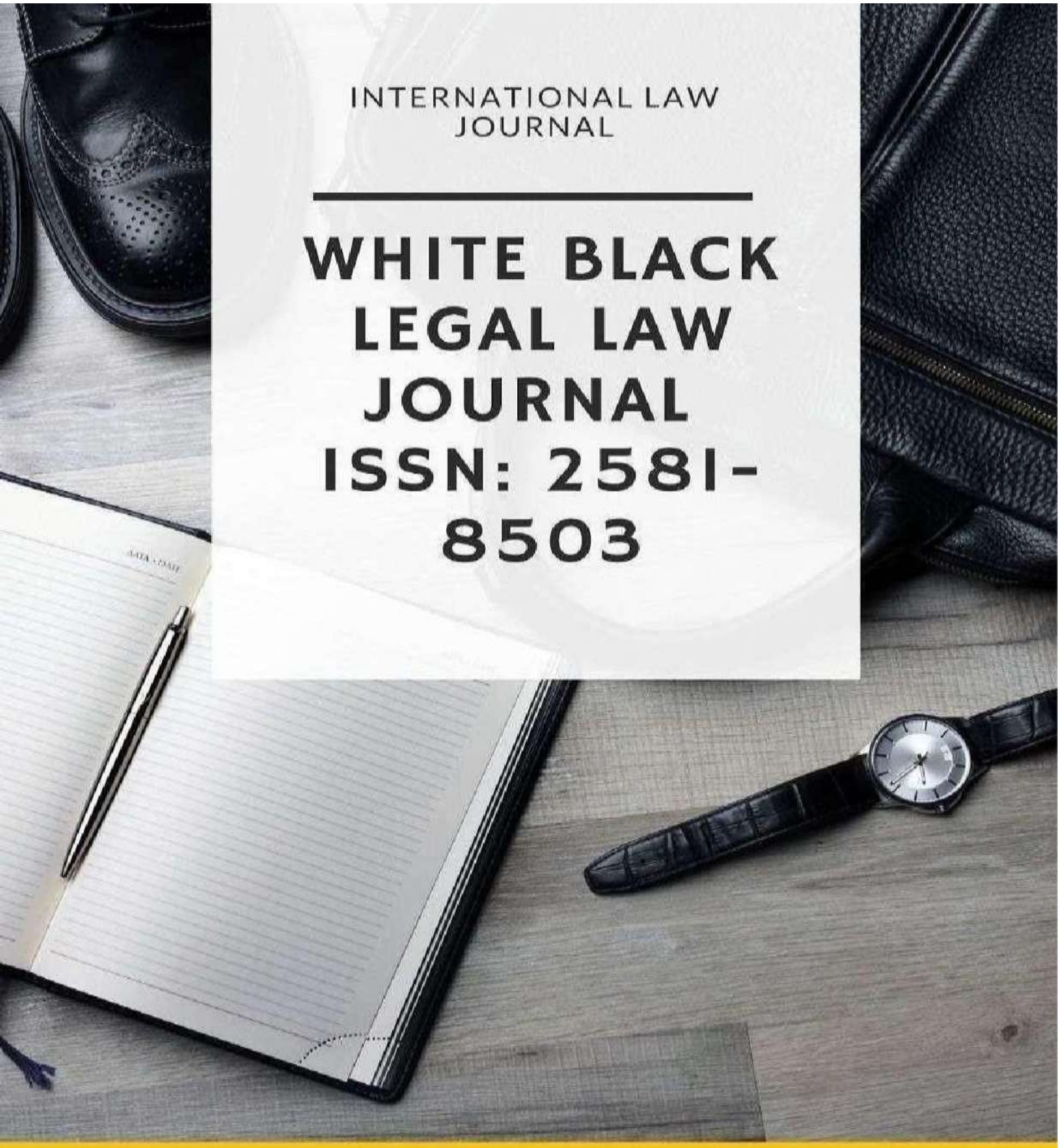

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

WWW.WHITEBLACKLEGAL.CO.IN

DISCLAIMER

EDITORIAL TEAM

Raju Narayana Swamy (IAS) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala . He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University . He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

Senior Editor

Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

ABOUT US

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | March 2025 ISSN: 2581-8503

LEGISLATIONS IN INDIA AND THE UNITED STATES OF AMERICA FOR THE OFFENCE OF IDENTITY THEFT

AUTHORED BY - NEERU KAPIL
(Research Scholar) Department of Laws Panjab University, Chandigarh.

1.1Introduction

Giving a specific explanation of the term "identity" is challenging, because this term is a bit ambiguous. Many questions come up when we try to figure out what this term means. For example, does identity refer to one's personal self, the self that can be identified by government-issued identity cards, the self that can be established by one's name, the way one is recognised by one's family or friends, or something else entirely? What exactly does a criminal take when he steals someone's identity? Is it accurate to say that someone has lost his/her identity? The conundrum that legislative bodies have when addressing the problem of identity theft is reflected in each of these queries. Furthermore, it is clear that different legislative bodies in different countries will tackle these issues in different ways, leading to a wide range of techniques followed by these countries to combat identity-related crimes.

There are several ways for a person to preserve their identity in the modern world. A person's name, birthdate, address, parents' names, and other details make up their physical identity. This kind of identity serves as the foundation for creating a person's financial identity, which includes his credit card details and bank account numbers. Another type of identity is social media identity and like any other valuable asset, identification information or data has a significant value in the digital economy and is therefore susceptible to theft. The proliferation of online commercial transactions and the development of information technology have led to a number of crimes and illegal activities involving identity information. Identity theft is one such offence, and identity for the purposes of identity theft relates to financial information, such as a person's bank account or credit card details, as well as numbers like their Aadhaar number or Social Security number (SSN).

To put it another way, identity theft includes any information that can be utilised by a criminal to assume the victim's identity and carry out numerous other crimes. It is crucial to remember that any act that qualifies as identity theft can cause the victim great financial and psychological damage, and that recovering from the effects of the crime takes substantial amount of time and money. Additionally, identity theft affects not just individuals but also businesses and financial institutions, causing them to suffer not only financial losses but also harm to their reputations during the course of the crime.

But in the United States, a federal law has narrowed the definition of "identity" to include specific kinds of personal data and identification documents; as a result, the statute's application is limited to offences involving such data and documents. The statute lists a number of examples of personal documents and information, including: name, date of birth, social security number, government-issued driver's license or identification number, passport number, alien registration number, unique biometric information like voice print, fingerprint, retina or iris image, or other physical representation, telecommunication identifying information, or access device.[1] It is important to remember that identity is a complex concept that has been thoroughly studied over the years by several philosophers, psychologists, sociologists, and legal experts. Because identity is now seen as a valuable resource that needs to be safeguarded, it is necessary to pay more attention to it in light of the development of the internet and faceless interactions.

Since not all identity theft occurrences entail a fraudulent conduct at the moment of personal information theft, there has been interest in the area to distinguish between identity theft and identity fraud in light of the stages and victims of identity theft. Because the acts covered by the terms "identity theft" and "identity fraud" are connected to each other, they are commonly used interchangeably. It is recognised, nevertheless, that these phrases have distinct legal meanings.[2] Javelin Strategy and Research (2021) defines identity theft as "unauthorized access of personal information" and identity fraud as identity theft incidents in which there is an element of financial gain. The inability to differentiate between these two phases of identity theft and ignorance about different types of identity theft may cause people to underestimate the possible long-term consequences of their personal data being compromised.

In general, the majority of nations lack legislations expressly targeting identity theft. However, a small number of countries have "identity-specific statutes," or laws that specifically address

identity crimes and also other laws that may be used to convict identity thieves, which are referred to as "identity-related statutes." It is interesting to note that the United States was the first country to pass legislation against identity theft and has extensive case law on the subject. The evolution of statutory arrangements, their functioning, and their failure to yield the intended outcomes are all explained by the legislative history of the United States. Identity theft cases are rising annually in the US since it has been noted that the country's identity crime laws do not put identity crimes within the sphere of a single statute.

1.2Laws Enacted In The United States Of America For

The Offence Of Identity Theft

The United States' laws pertaining to identity theft are separated into two sections, as explained below:

1.2.1 Statutes enacted Particularly for Identity Crimes

1.2.1.1 *Identity Theft and Assumption Deterrence Act, 1998 (ITADA)*

The following points need to be mentioned in relation to this Act:

A. History of the First Identity Crime Statute in the United States

Section 1028 of Title 18 of the United States Code, which is the first identity crime statute, was passed in 1982. Since then, it has undergone numerous amendments. It was originally named "Fraud and related activity in connection with identification documents, authentication features, and information." Only the production, possession, and transfer of government-issued identity documents was covered within the limited scope of this statute. Nonetheless, false documentation is no longer a need for committing any form of identity theft in the present era. In reality, the most suitable instrument for committing identity theft by criminals is primarily identification information. However, the security of identifying information was not guaranteed under the old criminal statute.

As a result, when the issue of financial identity theft began to surface in the United States in the mid-1990s, the legal authorities mostly ignored the complaints of numerous victims. Individuals complaining about the offence of identity theft were not accepted as victims by the legal community. The lack of specific laws that forbid identity theft in general and financial identity theft in particular was the reason behind it. The criminals who committed the offence were also aware of this legal ambiguity. To raise awareness about the predicament faced by

identity theft victims, Bob Hartle, a victim himself, took this matter before the US Senate. He was the drafter of the Arizona State Law that officially made identity theft a crime in Arizona.[3] Thus, in 1996, Arizona became the first US state to make identity theft a crime, followed by California[4] and numerous other states.

Following the successful state-level implementation of criminal legislation, Hartle approached U.S. Senator Jon Kyl from Arizona, who, with the assistance of Congressman John Shadegg, introduced Senate Bill known as the Identity Theft and Assumption Deterrence Act (ITADA), in 1997 to criminalise identity theft at the federal level and declaring it as a federal offence. The Bill was enacted by Congress in October 1998 and went into effect in January 1999. This Act added a new sub-section (7) to s. 1028(a) of Title 18, United States Code to expressly criminalise the offence of identity theft. The wording of s. 1028(a)(7) is as follows:

[Whoever] "knowingly transfers or uses, without lawful authority, a means of identification[5] of another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law;"[6] [commits identity theft].

B. Essential Requirements for the Offence of Identity Theft according to the Federal Statute

As per the federal identity crime statute, it is necessary to prove that an individual committed the offence of identity theft "knowingly" in order to convict him for the same. It is crucial to remember that identity crimes cannot be mistakenly or accidentally committed. If the criminal committed the following activities with knowledge[7] or with a guilty mind, they would be considered illegal under the statute:

- production of an identification document, authentication feature or a false identification document without legal authority (s. 1028(a)(1)),
- transfer of an identification document, authentication feature or a false identification document knowing that such document or feature was stolen or produced illegally (s. 1028(a)(2)),
- possession of five or more such documents or features with the intent of using or transferring them unlawfully (s. 1028(a)(3)),
- possession of an identification document, authentication feature or a false identification

document with the intent of using such document or feature to defraud the United States (s. 1028(a)(4)),

- production, transfer, or possession of a document-making implement[8] or authentication feature with the intent of using such implement or feature in the production of a false identification document or for producing another document-making implement or authentication feature which can be so used (s. 1028(a)(5)),
- possession of an identification document or authentication feature that seems to be a document or feature of the United States or of a sponsoring organisation appointed for an event of national significance, which is, in fact, stolen or produced without legal authority, with the knowledge that such document or feature was stolen or produced without such authority (s. 1028(a)(6)),
- transmission or use of a means of identification of another person without lawful authority with the intent of committing, aiding, or abetting any unlawful activity which amounts to a breach of federal law or a felony under any state or local law (s. 1028(a)(7)),
- Trafficking in fake or actual authentication features for using them in fake identification documents, document-making implements, or means of identification (s. 1028(a)(8)).

C. Fine and Punishment provided under the Federal Statute

- The minimum penalty mentioned under the statute, without any further sentencing enhancements, is a fine, or imprisonment up to a year, or both.[9] This penalty may be applied if none of the components of a longer sentence, as stated in the paragraphs mentioned below, are present. However, there is hardly any criminal action under 18 U.S.C. s. 1028(a) which can be exempted from a harsher penalty.
- The statute's minimum punishment for certain other criminal offences is five years in prison, or a fine, or both, without any enhancements. These crimes are related to any other production, transfer, or use of a means of identification, an identification document, authentication feature or a false identification document; or an offence provided under s. 1028(a)(3) and (7).[10]
- If the offence involves the production or transfer of an identification document, authentication feature, or a false identification document that seems to be a document or feature issued or authorised by the United States Government; or the production or transfer of any such document that seems to be a birth certificate, driver's license, or personal identification card;[11] or the production or transfer of more than five identification

documents, authentication features, or false identification documents; or an offence mentioned under s. 1028(a)(5); or an offence under s. 1028(a)(7) which involves the transfer, possession, or use of one or more means of identification, if because of such offence, the offender obtains anything of worth $1,000 or more during the time-period of one year,[12] the statute may impose an imprisonment of maximum 15 years, or a fine, or both.

- If the offence is committed in connection with a drug trafficking offence under s. 929(a)(2); or with regard to an offence of violence under s. 924(c)(3); or if the perpetrator has a prior conviction for an offence involving identification documents,[13] then he may be sentenced to up to 20 years in prison, or a fine, or both.
- If the offence is committed to encourage the acts of domestic or international terrorism under ss. 2331(5) or 2331(1) respectively,[14] then the offender will face up to 30 years in jail, or a fine, or both.
- In all the circumstances covered by s. 1028(a)(1)-(8), any personal property used or intended to be used in commission of the crime must be forfeited to the United States Government.

D. Outcome of the Identity Theft and Assumption Deterrence Act

Two pertinent goals are accomplished by the Identity Theft and Assumption Deterrence Act. First and foremost, it establishes harsh penalties for those who commit identity theft[15] and implements specific schemes for law enforcement and crime investigation. Second, it instructs the Federal Trade Commission to start new procedures for advising customers, receiving victims' complaints, and working with other investigative organisations to take effective law enforcement actions.[16] With regard to the first goal, the Act instructs the US Sentencing Commission to revise the Federal Sentencing Guidelines in order to include the crime of identity theft in the sections pertaining to fraud.[17] To ensure that the punishments for offences under s.1028 are appropriate, the Act grants the Sentencing Commission broad discretion for carrying out this task. In relation to the second goal, the Act explicitly states that the Federal Trade Commission is the primary federal body to ensure that the Act is implemented effectively. Consequently, Congress directed the FTC to train the public about the different ways by which the offence of identity theft can be committed, to create a suitable system for promptly filing identity theft complaints, and to respond to those complaints in cooperation with other law enforcement organisations.

E. Critical Appraisal of the Identity Theft and Assumption Deterrence Act

As a result of the implementation of ITADA, law enforcement agencies began to acknowledge the complaints of victims of identity theft.[18] Prior to this Act's implementation, no federal law forbade the theft of another person's identity in cases where the perpetrator did not utilise false identifying documents. But, even if the forged documents are not used in the commission of offence, the ITADA recognised the technological advancement by strengthening protection to identifying information. It broadened the scope of offences pertaining to identity to include the use or transfer of any of the "means of identification" specified in the Act, as long as such use or transmission was carried out with the intent to commit, or to aid or abet, an additional crime.[19]

Furthermore, the United States Congress introduced this Act in order to serve as a deterrent to identity thieves' future actions. This Act made identity theft a separate criminal offence in order to make it more difficult for criminals who commit the crime. Although the contention of deterrence in favour of criminalization, is still up for debate. Designating identity theft as a white-collar crime, indicates that there is a bleak chance of apprehending criminals and that the amount of potential punishment is minimal, which is basically a slap on the wrist.[20] As a result, rather than serving as a strong deterrent for potential offenders, ITADA appears to be more beneficial to the victims of identity theft.

1.2.1.2 The Identity Theft Penalty Enhancement Act, 2004 (Aggravated Identity Theft)

A. Primary Reason for the Execution of Identity Theft Penalty Enhancement Act

By passing the "Identity Theft Penalty Enhancement Act (ITPEA)" in 2004, the US Congress added a provision to the federal law to address the problem of "aggravated identity theft."[21] This Act further modified federal law,[22] by adding the term "possesses," in addition to "transfers" and "uses." It specifically links identity theft to other crimes and stipulates that when identity theft is perpetrated in connection with those other crimes, harsher punishments have to be inflicted. Congress cited the growing number of identity theft cases since the original identity theft law was enacted, as the main reason for passing the ITPEA. Additionally, a lack of effective deterrence against identity theft served as a catalyst for the passage of new legislation.

The aggravated identity theft statute lays down that "whoever, during and in relation to any felony violation enumerated in subsection (c),[23] knowingly transfers, possesses, or uses,

without lawful authority, a means of identification of another person shall, in addition to the punishment provided for such felony, be sentenced to a term of imprisonment of 2 years."[24] To put it another way, aggravated identity theft can only be committed if the identity crime occurs "during and in relation to" one or the other designated offences, such as embezzlement, immigration offences, and various forms of fraud. Aggravated identity theft legislation was passed in order to penalise offenders with an appropriate sentence. This Act instructs the courts or judges that anyone who is found guilty of aggravated identity theft, shall not be put on probation.[25] Judges are also directed not to allow a sentence imposed for aggravated identity theft to run concurrently with any other sentence provided under some other statute.[26]

B. Critical Evaluation of the Identity Theft Penalty Enhancement Act

However, there were some protesters who were against mandatory minimum penalties. It was argued that, "mandatory minimum sentences not only defeat the rational sentencing system that Congress adopted but make no sense in our separation of powers scheme of governance. Moreover, the notion that mandating a two- or five-year sentence to someone who is willing to risk a 15-year sentence already is not likely to add any deterrence."[27] The implementation of the Identity Theft Penalty Enhancement Act was also debatable because of the strong criticism levelled at its ideology.

1.2.1.3 Identity Theft Enforcement and Restitution Act, 2008

Some members of the U.S. Congress persisted in their efforts to enact a legislation pertaining to identity theft even after the Identity Theft and Assumption Deterrence Act of 1998 and the Identity Theft Penalty Enhancement Act of 2004 were passed. The Identity Theft Enforcement and Restitution Act was introduced in the Senate in October 2007 in order to provide better security to the residents of the United States. The primary goal behind the introduction of this Act was to give identity theft victims greater options to receive compensation for the consequences of the crime and restitution for any additional expenses that they may have suffered as a result of the crime. The Act also demanded that those who are found guilty of identity crimes should receive harsher punishments in accordance with the offence. This Act mandates that the victims of cybercrimes shall receive appropriate damages for the time and money they have lost as a result of these crimes,[28] and has made it very easy for law enforcement agencies to punish identity thieves who utilise virtual means to commit the crimes.

1.2.2 Statutes related to Identity Crimes

In the United States, there are a number of laws that do not specifically address identity crimes, but they do provide additional ways to stop similar crimes. These legislations cover the gap created by two main identity theft statutes[29] in specific circumstances. The statutes pertaining to wire fraud, mail fraud, or email fraud can be used to prosecute an identity thief if the identity theft was committed over telephone, mail, or e-mail. The statutes mentioned below are used frequently with regard to identity crimes:

1.2.2.1 Access Device Fraud (Fraud by Using ATMs, Credit cards, Debit cards, etc.)

Misappropriating someone else's credit or debit card information and using it to obtain valuable items in that person's name is a prevalent method of committing identity crimes. According to the federal statute,[30] credit cards, debit cards, and other similar devices are referred to as "access devices,"[31] and the crime involving these cards is known as "fraud in connection with access devices." Access device fraud, as well as attempt and conspiracy to commit access device fraud, are underlying felonies under the aggravated identity theft statute. Prosecutors can use the access device legislation in conjunction with the aggravated identity theft statute to prosecute identity thieves.

1.2.2.2 Computer Fraud

Certain characteristics of the federal statute dealing with computer fraud[32] are closely related to the crime of identity theft. This statute protects information saved in "protected computers,"[33] (a term that specifically means computers safeguarded by this federal statute). Anyone who intentionally obtains access to a computer without authorisation or exceeds his permitted access, has violated the federal law, according to the provisions of this Act. Computer fraud is an underlying offence to support the accusation of aggravated identity theft.[34]

1.2.2.3 E-mail Fraud

As a component of the CAN-SPAM Act of 2003,[35] the statute that addresses crimes pertaining to email identity theft was passed in 2003. According to the Senate Report attached to the Bill, customers who buy items via spam or junk email face a number of risks such as identity theft or theft of credit card. Thus, preventing identity theft was one of the primary goals of the Bill. Email fraud and the attempt and conspiracy to commit email fraud are considered main crimes under the aggravated identity theft statute.[36]

1.2.2.4 Mail Fraud

Mail fraud, which is described as "making false representations through the mail to obtain an economic advantage,"[37] is a sort of fraud that can be perpetrated through the usage of the US Postal Service. The main goal of the mail fraud statute[38] is to make it illegal to use the US mail as part of a fraudulent scheme. One of the criminal offences covered by the aggravated identity theft statute is mail fraud.[39]

1.2.2.5 Wire Fraud

Another kind of fraud that can be carried out using electronic communications is wire fraud, which includes, making false representations over the phone in order to obtain money. In interstate or international commerce, the wire fraud statute[40] forbids the transmission of any signs, signals, sounds, pictures, or writings through the medium of wire, radio, or television communication in order to acquire money or property by fake promises, or to carry out any scheme or artifice to defraud. Under the aggravated identity theft statute, wire fraud and attempt and conspiracy to commit wire fraud are primary offences.[41]

1.3 Laws in India for the Offence of Identity Theft

Identity theft is a very broad term that encompasses a number of offences, including fraud, forgery, deception, and cheating and it can also be committed jointly with other cybercrimes. At the start of the age of information technology, India passed a specific law known as the *Information Technology Act*, 2000 (IT Act)[42] to control online activities in the digital environment. Therefore, the IT Act sought to make identity theft a crime at a time when the information technology was still in its infancy in India, but it did not go into great detail about what identity theft meant or how it was defined. It was in 2008, the *Information Technology (Amendment) Act*, 2008,[43] introduced Section 66C, which made identity theft a distinct criminal offence under Indian law. In light of this, it is not possible to take sufficient guidance from the IT Act itself regarding what would and what would not be considered identity theft. In this situation, extra guidance can be obtained from the *Bharatiya Nyaya Sanhita*, 2023,[44] the principal Act that defines offences in India. Although there are no definite provisions in the *Bharatiya Nyaya Sanhita* to address identity theft, but it has some other provisions that might help to clarify the general outline of the characteristics of the crime of identity theft within the framework of Indian criminal justice system.

1.3.1 Sections of the Bharatiya Nyaya Sanhita, 2023 dealing with the Offence of Identity Theft Identity theft combines the characteristics of both fraud and theft, and Section 303 of the *Bharatiya Nyaya Sanhita*, 2023, addresses the crime of theft. The question of whether theft under Section 303 encompasses identity theft is pertinent. According to one view, Section 303 does not apply in cases of identity theft since it only covers movable or tangible property as defined by Section 2(21) of the *Bharatiya Nyaya Sanhita* and excludes activities in cyberspace. On the contrary, another view is that the drafters of the *Sanhita* "intended to include property of every description within the ambit of the term 'movable property', except land and things attached to the earth or permanently fastened to anything which is attached to the earth",[45] so, the definition of 'movable property' under Section 2(21) may include electronic property as well within its purview. Although there is no legal principle that resolves the disagreement between these two viewpoints, it is generally believed that identity theft is not covered by Section 303 of the *Bharatiya Nyaya Sanhita* because the Indian judiciary has not yet used this section or Section 379 of the Indian Penal Code, 1860[46] to punish identity thieves.

The Indian Penal Code, 1860 or the *Bharatiya Nyaya Sanhita*, 2023 do not have an independent section to deal with the offence of identity theft, however, Sections 463 to 477A of the IPC[47] that dealt with offences related to forgery and forged documents were amended in the year 2000, to include the offence of identity theft within their scope. This was done by adding some new words in these sections like electronic record, electronic signature, etc.

In addition to that, identity theft is described as cheating under Sections 318 and 319 of the *Bharatiya Nyaya Sanhita*, where it may be portrayed as cheating by personation.[48] And if the words "anything which is capable of being converted into a valuable security" under Section 318(4) of the *Sanhita* is meant to cover the unique identification feature of a person, then this section can also be invoked for the prosecution of the offence of identity theft.

1.3.1.1 Connection between the Offence of Identity Theft and the Offence of Cheating and Cheating by Personation

Section 318(1) of the *Bharatiya Nyaya Sanhita* describes cheating as an offence that concentrates on the accused's dishonest intention to persuade a person to give any property to another individual. For instance, a person is guilty of both cheating and dishonestly appropriating another person's identity, i.e., identity theft, when he poses as a civil servant with the goal of tricking someone into giving him things on credit for which he has no intention to

pay later. Likewise, identity theft and the crime of cheating by personation, as described by Section 319(1) of the Bharatiya Nyaya Sanhita, are closely connected. For instance, someone is guilty of both financial identity theft and cheating by personation if he poses as a wealthy banker with a similar name and tricks someone into giving him his banking information.

1.3.1.2 Offences in relation to Documents (Sections 335 to 344 of the Bharatiya Nyaya Sanhita and Sections 463 to 477A of the Indian Penal Code)

In order to provide legal recognition to "electronic records" and "digital signatures," the *Information Technology Act* of 2000 introduced a number of amendments in the Indian Penal Code[49] (corresponding present legislation the *Bharatiya Nyaya Sanhita*, 2023). These amendments were intended to prevent illegal transactions that occur over electronic media. In addition to the substantive law amendments, the Bharatiya Sakshya Adhiniyam, 2023[50] has also undergone significant amendments at the appropriate places to support the substantive provisions and give electronic documents and records legal recognition for the purpose of providing them evidentiary value. In the following paragraphs, offences related to documents and how they are related to the offence of identity theft are covered:

A. <u>Forgery and Identity Theft:</u>

Under the Indian criminal law, identity theft and forgery are two distinct but closely related offences. Although both include the unauthorised use of another person's personal data, the nature of these offences and their associated punishments differ significantly. Forgery can take many different forms, such as creating a duplicate certificate or marksheet, forging currency notes, or signing a document with someone else's signature.

On the contrary, the offence of identity theft takes place when there is illegal use of someone else's personal information with the intention of gaining an economic advantage. This could involve opening a bank account in someone else's name, applying for a loan or a job using someone else's identity, or using someone else's credit card information to make unlawful purchases.

Notwithstanding their differences, identity theft and forgery are immediately related. Like in many situations, identity theft entails forging documents or altering pre-existing ones in order to commit fraud. For instance, a person who steals the identity information of someone else might create a false passport or identity card to prove his stolen identity. When identity theft

and forgery are both committed as part of a single criminal act, the perpetrator may face separate charges under the *Information Technology Act*, 2000 and the *Bharatiya Nyaya Sanhita*, 2023.

B. Section 344 of the *Bharatiya Nyaya Sanhita* (Falsification of Accounts) and the Offence of Identity Theft:

Section 344 of the *Bharatiya Nyaya Sanhita*[51] addresses account fabrication by a clerk, officer, or servant. According to this section, the accused person (a clerk, officer, or servant) wilfully makes a false entry in any book, electronic record, paper, writing, valuable security, or account that belongs to his employer or is received by him on his employer's behalf, or he intentionally destroys, alters, or falsifies any of these items in order to commit fraud. The punishment under this section is imprisonment up to seven years or fine or both. In the case of identity theft, this section may be used if the perpetrator dishonestly misuses private and important official information that is necessary for the functioning of his workplace. For example, a person may be charged under this section[52] and simultaneously for the offence of identity theft if, while working as a clerk, he writes in his officer's name or makes inaccurate entries in the official books without informing his superior officer.

However, it is to be noted that the *Bharatiya Nyaya Sanhita* simply treats identity theft as an extension of the crimes of forgery and cheating; it does not specifically criminalise identity theft. The *Information Technology Act*, 2000 is the only law in India that addresses cybercrimes directly; nevertheless, the offence of identity theft is nowhere mentioned in this Act. It was only in 2008, the *Information Technology Act* was amended to include the crime of identity theft in Indian law by adding Section 66C.[53] This is the only section that specifically addresses the offence of identity theft.

1.3.2 Enactment of the Information Technology Act, 2000

Since the use of information and communication technology has grown significantly in commercial transactions and for entering contractual relations worldwide, the *Information Technology Act* was formulated in India in 2000.[54] In India, e-commerce and electronic communication are governed primarily under the *Information Technology Act*. In addition to encouraging e-commerce, this Act gives legal recognition to electronic transactions, electronic records, and electronic/digital signatures. It lays out penalties for a number of cybercrimes, including identity theft, hacking, and illegal access to computer systems, and promotes law

enforcement agencies for a comprehensive investigation of cybercrimes. It also covers the most important aspects of privacy and data protection, such as safeguarding sensitive or private information and establishing a data protection policy that would be useful in preventing identity theft and other related online crimes.

1.3.3 Explanation of the Offence of Identity Theft under the Information Technology (Amendment) Act 2008

The *Information Technology (Amendment) Act* of 2008 was the first law to use the term "identity theft" in India. Section 66C of the amended Act stipulates penalties for the offence of identity theft. It provides that:

- any person who, 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 either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.[55]

In essence, Section 66C defined identity theft in connection with these three terms: password, electronic signature, or unique identification feature. These three elements make up an individual's personal identification information, over which he should have sole authority.

Usually the offence of identity theft is committed in two stages:

- Illegal Collection Of Personal Information Or Unique Identification Feature Of Some Other Person And
- Illegal Use Of Such Personal Information Or Unique Identification Feature.[56]

In a nutshell, identity theft or identity fraud, is a type of cybercrime that mainly entails the unlawful acquisition of an individual's data through dishonest or fraudulent means and use of that data for any kind of financial advantage. For instance, Mr. P may be prosecuted with financial identity theft under Section 66C of the *Information Technology (Amendment) Act*, 2008, if he copies the ATM card of Mr. R and takes 50,000 rupees out of his account. Likewise, if someone steals the Aadhar card of a person in order to obtain a bank loan in that person's name, then he will be prosecuted under Section 66C since it involves identity theft using the Aadhar card, which is the most significant identity verification document in India.[57]

1.3.4 Critical Analysis of the Information Technology Act, 2000 and the Information Technology (Amendment) Act, 2008

Although, there are a number of provisions under the *Information Technology Act* of 2000 and its amended version that can be utilised to prosecute identity thieves and other cybercriminals, yet none of the provisions clearly outline the behaviours and necessary components that would comprise the offence of identity theft. Section 66C which punishes the offence of identity theft, makes it illegal to fraudulently use someone else's password, electronic signature, or other unique identification feature. However, a person's identity is influenced by a number of other factors, including race, gender, age, sexual orientation, political affiliation, professional identity, etc., and any important information pertaining to these factors must be safeguarded. The only way to do this is to create a legislation specifically for the offence of identity theft, which would clearly define the crime and impose severe penalties on those who commit it.[58] Furthermore, the *Information Technology Act* of 2000 and its Amendment of 2008 do not provide adequate penalties or fines for identity theft and related offences to stop the enormous increase in identity theft cases.

1.4 Conclusion

Hence, it is suggested by the researcher that the Indian legislations regarding identity theft should be adequately amended to inflict harsher penalties for the aggravated types of identity theft, as the United States passed a separate law to prosecute the crime of aggravated identity theft.[59] The researcher also states that in order to assist the victims of identity theft, the Indian government should draft laws similar to those framed in the United States.[60] Because in order to truly assist the victims, it is necessary to compensate them for the immediate harm that the offence caused to them and provide them means to endure the after-effects of the crime.

REFERENCES

BOOKS

- Archer, Norm, Sproule, Susan, *et., al., Identity Theft and Fraud: Evaluating and Managing Risk* (University of Ottawa Press, Ottawa, Canada, 2012).
- Biegelman, Martin T., *Identity Theft Handbook: Detention, Prevention and Security* (John Wiley & Sons Publishing Co., New Jersey, United States, 2009).
- Collins, Judith M., *Investigating Identity Theft* (Wiley Publications, New Jersey, 1st edn., 2006).
- Dijck, Jose Van, *The Culture of Connectivity: A Critical History of Social Media* (Oxford University Press, United Kingdom, 1st edn., 2013).

- Finklea, Kristin M., *Identity Theft: Trends and Issues* (BiblioGov Publishers, 2010).
- McNally, Megan, *Identity Theft in Today's World* (Praeger Publishers, Santa Barbara, California, 2012).

ARTICLES

- Allen, Anita L., "Coercing Privacy" 40 *William and Mary Law Review* (1999).
- Allison, Stuart F.H., Schuck Amie, *et.al.*, "Exploring the Crime of Identity Theft: Prevalence, Clearance rates, and Victim/Offender Characteristics" 33 *Journal of Criminal Justice* (2005).
- Bisogni, Fabio and Asghari, Hadi, "More than a suspect: An investigation into the connection between data breaches, identity theft, and data breach notification laws" 10 *Journal of Information Policy* (2020).
- Cassim, F., "Protecting Personal information in the era of Identity Theft: Just how safe is our personal information from identity thieves?" 18 *Potchefstroom Electronic Law Journal* (2015).
- Davis, Erin Suzanne, "A Worldwide Problem on the World Wide Web: International Responses to Transnational Identity Theft via the Internet" 12 *Washington University Journal of Law & Policy* (2003).
- Federal Trade Commission, "Taking Charge: What to do if Your Identity is Stolen" *NCJRS Virtual Library* (January, 2012).

1 18 U.S.C. s. 1028(d)(7).
2 Newman & McNally, "Identity Theft Literature Review" (July, 2005).
3 Arizona Revised Statutes, Title 13-Criminal Code, s. 2008 (Taking identity of another person or entity; classification).
4 California Penal Code, s. 530.5.
5 18 U.S.C. s. 1028(d)(7): the term "means of identification" means any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual.
6 Identity Theft and Assumption Deterrence Act, Pub. L. No. 105-318, 112 Stat. 3007 (1998) (codified as amended at 18 U.S.C. s. 1028).
7 18 U.S.C. s. 1028 (a) (1)-(8).
8 Id., s. 1028(d)(2): the term "document-making implement" means any implement, impression, template, computer file, computer disc, electronic device, or computer hardware or software, that is specifically configured or primarily used for making an identification document, a false identification document, or another document-making implement.
9 Id., s. 1028(b)(6).
10 Id., s. 1028(b)(2).
11 Id., s. 1028 (d)(8): the term "personal identification card" means an identification document issued by a State or local government solely for the purpose of identification.
12 Id., s. 1028(b)(1).
13 Id., s. 1028(b)(3).
14 Id., s. 1028(b)(4).
15 Id., s. 1028(b).

16 Id., s. 1028 note.
17 28 U.S.C. s. 994.
18 National Criminal Justice Reference Service/Newman and McNally, "Identity Theft Literature Review" (July, 2005).
19 18 U.S.C. s. 1028 (a)(7).
20 Heith Copes and Lynne M. Vieraitis, "Bounded rationality of identity thieves: Using offender-based research to inform policy" 8 Criminology and Public Policy (2009).
21 18 U.S.C. s. 1028A.
22 Supra note 19.
23 18 U.S.C. s. 1028A(c)(1) to (11).
24 Id., s. 1028A(a)(1).
25 18 U.S.C. s. 1028A (b)(1).
26 Id., s. 1028A (b)(2).
27 H.R. REP. NO. 108-528, at 27 (2004), as reprinted in 2004 U.S.C.C.A.N. 779.
28 Former Vice President Protection Act of 2008, s. 202, Criminal Restitution (Amendment to 18 U.S.C. s. 3663(b)): It provides that an offender "in the case of an offence under ss. 1028(a)(7) or 1028A(a) of title 18, pay an amount equal to the value of the time reasonably spent by the victim in an attempt to remediate the intended or actual harm incurred by the victim from the offence."
29 18 U.S.C. ss. 1028, 1028A.
30 Id., s. 1029.
31 Id., s. 1029(e)(1): the term "access device" means any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number, or other telecommunications service, equipment, or instrument identifier, or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds.
32 18 U.S.C. s. 1030.
33 Id., s. 1030(e)(2).
34 Id., s. 1028A(c)(4).
35 CAN-SPAM Act of 2003, Pub. L. No. 108-187, 117 Stat. 2699 (codified at 18 U.S.C. s. 1037). "CAN-SPAM" is an abbreviation for "Controlling the Assault of Non-Solicited Pornography and Marketing."
36 Supra note 34.
37 Black's Law Dictionary (9th edn., 2009).
38 18 U.S.C. ss. 1341, 1342.
39 Id., s. 1028A(c)(5).
40 Id., s. 1343.
41 Supra note 39.
42 The Information Technology Act, 2000 (Act 21 of 2000).
43 The Information Technology (Amendment) Act, 2008 (Act 10 of 2009).
44 The Bharatiya Nyaya Sanhita, 2023 (Act 45 of 2023).
45 Id., s. 2(21).
46 The Indian Penal Code, 1860 (Act 45 of 1860).
47 Supra note 44, ss. 335 to 344.
48 Debargha Chatterjee "Laws that govern ID Theft in India" (August, 2021), available at: https://blog.ipleaders.in/laws-that-govern-id-theft-in-india/ (last visited on March 29, 2024).
49 Commentary under s. 29A, IPC in Chapter II.
50 Earlier legislation the Indian Evidence Act, 1872 was amended.
51 S. 477A of the Indian Penal Code, 1860 dealt with falsification of accounts.
52 Supra note 44, s. 344.
53 Supra note 43, s. 66C.
54 Supra note 42.
55 Supra note 53.
56 Dr. Jyoti Rattan, Cyber Laws and Information Technology 79 (Bharat Law House, New Delhi, 9th edn., 2022).
57 Ramnath, N.S., Assisi Charles, The Aadhaar Effect: Why the World's Largest Identity Project Matters (Oxford University Press, India, 2018).
58 Adv. Narmada Singh, "Law relating to digital identity theft in India and its invasion of privacy" 3 International Journal of Advanced Legal Research (2022).
59 The Identity Theft Penalty Enhancement Act, 2004.
60 The Identity Theft Penalty Enhancement Act, 2004 and The Identity Theft Enforcement and Restitution Act, 2008.