WWW.IJRPR.COM

International Journal of Research Publication and Reviews

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

Reconceptualising Property Offences in the Digital Age: Digital Assets, Online Fraud and the Applicability of the Bharatiya Nyaya Sanhita, 2023.

Sakshi Dhiman, Taljinder Kaur, Navdeep Kaur.

B.A.LLB semester 7th , **Rayat-Bahra-University**

ABSTRACT

The expansion of digital payments, online platforms, virtual asset and remote financial services. Has revolutionized how people acquire, retain, transfer and pass on property. Property is no longer. Only seen in its physical form – such as. Cash, land jewellery or any other physical item. At a person can now hold To earn economic value, a cryptocurrency wallet is required, which is a token associated with a digital good, an online A stored balance, an account or a contractual entitlement, which is managed via a platform. These Information of interests can be compromised by deception, unauthorized access, manipulation of credentials Or a diversion of a transaction. The core question of the law is whether traditional offences were genuine offences. Can react appropriately if the nature of the offence is against property or the methodology of offending is against property. This paper looks at the ability of Bharatiya Nyaya Sanhita 2023 (BNS) in addressing Digital-asset framework, and that of the online fraud, as a different matter. The Bharatiya Sakshya Adhiniyam, 2023 (Bharatiya Sakshya Act) and Information Technology Act, 2000 (IT Act) (BSA). It takes into account the stealing under section 303, snatching under section 304, extortion, robbery, Criminal misappropriation, criminal breach of trust, receiving stolen property and cheating Under sections 308-319 with computer offences and identity based offences. Under the IT Act. It also reviews electronic evidence, attributive jurisdiction and territorial jurisdiction, Investigation, asset tracing and recovery of victims. It is a paper that has a doctrinal and analytical approach. It is based mainly on the texts of the laws, Official legal documents and judicial rules pertaining to dishonest enlistment, holding, and Electronic records and fair criminal process. It does not report original field data, or a Statistical survey. It is its central thesis that the BNS can solve a lot of these digitally manifested forms. Arises regarding the criminal intent behind it established the legal elements of an offence, but raises doubt about the criminal intent. Remains where the offence is one purely intangible and of the traditional type, namely, the theft of a birth certificate. remains where the offence is purely intangible and of the traditional kind, the stealing of a birth certificate. Requires 'movable property' or a specific type of possession. The best solution is: Coordinated framework: careful interpretation of existing provisions, clear treatment of digital. Evidence, better investigatory capacity, and specific legislative clarity which will not be taken away, Crafts arguments that are legally sound and does not over criminalise.

Keyword: Bharatiya Nyaya Sanhita, 2023, digital assets, cryptocurrency, online fraud were used. Cheating, Cybercrime, Electronic evidence, Information Technology Act, 2000.

1.INTRODUCTION

The shift of property offences towards the digital age. The digitalization of property offences. Traditionally, property offence explanations have revolved around familiar objects: somebody takes someone else's phone; they try to trick a buyer into paying money for a stolen phone; they accept stolen goods knowing they are the victim of a theft. In the digital setting, the way of offending is altered but not necessarily the intent for offending. An offender can attempt to obtain value dishonestly, may induce a person to provide money, misuse entrusted access to an account or may prevent a rightful user from controlling an account. Concurrently, not all technical failures or unauthorized use is a. The primary issue is a legal fit. While the BNS has detailed offences against property, many provisions are drafted on concepts like movable property and possession, taking and delivery and entrustment. Digital assets can be duplicated, moved around with a ledger, based on credentials, or be subject to platform rules. Sometimes the victim is a loser. The second issue is that of the general criminal law and the special legislation related to cybercrime. It can be a deception, an unauthorized access, the use of another person's password and the transfer of funds and hiding of the proceeds. Either the BNS or the IT Act may be applicable, but the investigators have to pinpoint the action under each provision of the two acts.

The first goal is to explore the operation of traditional notions of property, possession and dishonest appropriation in relation to the digital sphere. The second is to identify those BNS provisions that apply to common types of online fraud and not equate all online incidents with theft. The third is to discuss about the role of IT Act in.

The main research question is: Can the BNS, 2023, along with the IT Act, 2000 and BSA, 2023, effectively tackle digital-asset appropriation and online fraud?

However, the methodology and scope of this study will focus on the following:

The doctrinal approach to the study is used, analyzing statutory acts, judicial principles and official acts of law. Compares offences analytically to determine the differences in act requirements and mental elements. Suppose scenarios are employed to verify applying the law to online transactions. The paper is not intended to provide. Limited to any type of wrongdoing with regard to property in India and focusing on digital assets, online cheating and electronic evidence. It briefly talks about BNS, IT Act, BSA and related procedural aspects. It does not offer investment advice, a determination of the ownership of any particular token or a final answer for.

2. A digital re-conceptualization of property

2.1 The traditional view of property under the criminal law.

It is not the same treatment in criminal law for all interests. The offence charged and what must be proven in the prosecution will depend on how the object is classified. For section 303 of the BNS the offense requires that the property be taken from another party without permission and the property must have moved. This difference illustrates that the concept of 'property' must not be understood as an obvious concept. Ownership, possession, custody and control and the right to use are. Not the same. If the bank's records show a customer's balance, then he or she may have the right to that amount. Not having any particular bank notes. People can have their own laptop. That they do not always have physical control over that which they own.

2.2 classification of digital asset

Now that digital assets are defined, they can be classified. Classifying digital assets is possible once they have been defined.

Digital assets include cryptocurrencies, -fungible tokens, in-game items, domain names, digital files, stored value balances, and online accounts and contractual rights that are managed electronically. Includes various legal and technical arrangements. A distributed ledger may be the place where a cryptocurrency token is stored. Controlled using a private key. An NFT could be a reference to a file, but the NFT is not the file.

The question with which the analysis of a legal document should begin is: What did the victim actually have? Was it a token, a right, an account credential, a file, a payment instruction or a right to receive services? Has accused person interfered with access to the item by copying it, changing it, obstructing access or misinforming individuals?

2.3 Tangibility, Ownership, Possession and Control

In most cases, possession can be determined by observation. The image depicts a person holding a watch. Has money in a wallet in the drawer. Digital control is more difficult to detect. Can be distributed to the user, the platform, a custodian and the network. The use of passwords does not establish ownership. It does not follow that "someone owns it" means that they have control of it.

The courts and investigators must distinguish between proof of identity and proof of control and proof of control and proof of ownership. Having an email address on a wallet could aid identify an individual. Does not demonstrate who possessed the private key at any given time. A transfer can be entered on a ledger account. Does not provide evidence of who had the authority to make it.

2.4 Reinterpreting for the digital economy

Where the language of the law can be reasonably interpreted to cover new situations, a technology neutral interpretation is preferred. The use of a digital device or platform should not be a defence to an offence. The digital method does not mean someone can't still be liable if they are tricked into allowing a bank transfer.

Interpretation has limits. The laws and regulations against criminal offences must be unambiguous and clear. The fact that a digital asset may have value should not lead courts to expand upon the meaning of terms such as " property. Legality principle must provide access to information on what is prohibited and against punishment by analogy. When there is a gap, in the law legislative clarification is needed.

3. The BNS are governed by the following laws: The BNS is subject to the following legislation:

3.1 Introduction to property offences

Offences against property is dealt with in Chapter XVII of BNS. Theft and snatching, theft in certain circumstances, extortion, robbery and dacoity, criminal misappropriation, receiving of stolen property, cheating, mischief and criminal trespass. Their relevance is significant as online fraud often seeks money and/or economic gain by. Section numbers should be verified by referring to the official enacted text prior to filing/citation.

For instance, Section 303 deals with theft, Section 304 deals with snatching, Sections 308-313 concern extortion, robbery and related offences and Sections 314-317 are regarding misappropriation, breach of trust and receiving of stolen property and Sections 318-319 are on cheating and cheating by personation.

3.2 Theft and Movable Property: Section 303

Section 303 focuses on theft in terms of “dishonest intention,” “movable property,” “possession,” “absence of consent” and “movement in order to take the property. They can be demonstrated in a physical case by witnesses, recovery and through CCTV and surrounding circumstances. In the digital case it is a different language that poses more questions. If a person takes. It may be a token transfer from one wallet to another which may have economic significance, but the prosecution must still establish that the object is of the kind described in the statute and that the alleged act is one of the kind.

3.3 Criminal Offenses of Snatching, Extortion, Robbery and Dacoity

S. 304 is an enactment that punishes the sudden, quick or forcible removal of a movable property from a person or from his or her possession.

Theft or extortion coupled with by the use or threat of violence or imminent injury is the statutory condition of robbery or dacoity and the prescribed number of persons acting in concert is the condition for dacoity.

3.4 Misrepresentation/ Breach of Trust

A breach of trust is a violation of one’s trust.A breach of trust is the breaking of one’s trust.

Section 314 relates to dishonest misappropriation of movable property and section 316 to criminal breach of trust involving the entrustment of property and the dishonest misappropriation or use of it “contrary to law or the governing direction”.

Section 317 covers “receiving” or “dealing in” stolen property in the situations provided by the statute. A person who, knowingly purchases or moves property obtained from an offence could be involved in an investigation but the prosecution must establish the knowledge or reason to believe on the part of the person and that the property was of the relevant classification.

3.5 Cheating, mischief and criminal trespass:

Section 318 is in relation to cheating (deception and thus the inducement) to which it refers. In online fraud, it is always important to determine if the bad purpose was present at the time of the representation, and if the fraud led the victim to give property or do an action. Bad investment, late payment or a faulty business deal. Cheating by personation is covered in Section 319. Someone posing as a customer-care representative, fake investment adviser, or a fake relative are all examples of how someone can impersonate you online. Mischief may be relevant where there is harm to a thing or a reduction in its value or usefulness which falls within the scope of the provision. The entry or otherwise of an individual to the property is the key to criminal trespass.

4. Such an appropriation, however, must occur in a digital context. The appropriation, however, must be through a digital medium.

4.1 **T**here is no specific definition provided for cryptocurrencies and virtual assets in India. Indian law has gone on a strange journey. There is no legislation stating cryptocurrencies are legal tender, nor any legislation prohibiting its use. In its judgment in **Internet and Mobile Association of India v. Reserve Bank of India ((2020) 10 SCC 274),** the Supreme Court upheld the circular directing regulated entities to not deal in virtual currencies on the primary basis of proportionality, since the RBI had not proven that businesses that it targeted have actually caused any harm to its regulated entities. The ruling did not resolve the question of the definition of crypto but declared that trading in it is a legal activity and can be constitutionally protected.

Since then, the State has been regulating and taxing crypto. The Finance Act, 2022 added the term ‘virtual digital asset' to the Income-tax Act, which also imposed a level tax on transferring a virtual digital asset and tax deduction at source on the payment of a virtual digital asset.

The Central Government in March 2023 announced that some VDASP's are eligible to be covered by the Prevention of Money Laundering Act, 2002. For the purposes of today's post most importantly, say the High Courts, crypto is property. In a landmark judgment in 2025, a Madras High Court ruling in a case involving a crypto exchange customer's claim to his funds following a significant hack, ruled that a crypto asset is not necessarily tangible property or currency, but can also be owned, possessed and held in trust. Single judge decision of this type is persuasive but not binding throughout the country but would be referred to in criminal proceedings as well as civil proceedings as the English and Singaporean approach.

4.2 The term "unauthorised transfer, diversion and misappropriation of digital assets" is defined to include the following practices:

Reflect on typical situations. Hacker acquires a seed phrase and sweeps a wallet. Company tokens are diverted to employee's address by an employee with signing authority. A phishing page is used to steal a victim's exchange credentials and makes a withdrawal from the victim's holdings. Each has an issue about the facts, and each has a different fit to the BNS.

Cheating under section 318 is the natural charge where the victim was duped into the action, such as by a support call when the victim is tricked into approving a transfer. If it was the offender who simply took control, and moved the money with no action taken by the victim, then it is harder, "no one was deceived", and some courts hold that it is not the same as deceptive the person who was in control of the automated system. Theft is the textual candidate, but requires the interpretation of the definitions of "movable property" and "moving". The misappropriation of dishonest nature of section 314

has the same issue. The sections of the IT Act which require only unauthorised access and only cause loss or diminution of value, i.e. sections 43 and 66 then become the default, as they do not require property or movement.

4.3 Breach of the integrity or use of Digital Tokens, Online Wallets and Digital Account Credentials

Where this is done on the strict reading, what is taken is not what the statute recognizes; and an Indian court would be bound to say so, as it did in Avtar Singh. There are two arguments against. The purposive reading would be that Parliament with a 20-year history of digital commerce can write the new Sanhita as such without including digital assets and it did not do so. But from the civil cases, a private key is a type of exclusive control, similar to possession, as suggested by functional reasoning. In contrast there is the rule that penal statutes are strictly interpreted and the precedent of Avtar Singh.

It is easier to obtain a credential for the point. Once you steal a password, that password has no value, but when you use it to log in to an account it is your identity and/or persona being stolen, which is covered by the IT Act, and using it to make payments is normally considered cheating by personation (BNS section 319) or identity theft (IT Act section 66C). In practice, then, there is an overlap between the BNS and the IT Act in their respective coverage of credential theft offences and access offences.

In relation to the same, the Bombay High had addressed the issue in the case of **Gagan Harsh Sharma v. State of Maharashtra (2018)** where employees were accused of accessing confidential data. The court quashed IPC Section 379, 405 charges and directed that prosecution shall continue under the IT Act – because IPC was not intended to cover data and the IT Act was specifically written to cover it. The ruling has been attacked because it is written in favor of the accused, but it demonstrates the willingness of the courts to apply data property crime to the special statute.

4.4 Criminal Breach of Trust in Digital Asset Management

This is the area they're strongest in. Digital assets are held on behalf of others by exchanges, custodians, wallet providers and fund managers and corporate treasury staff. When elements 316 line up, it means that if a person in trust misappropriates the trust property or uses it for his own purposes contrary to the terms under which it is held; the elements of trust fit. The enhanced provisions for agents, bankers and merchants may apply, too, and this is crucial, as punishment for these provisions is harsher.

Unresolved issues are related to the structure of the entrustment. Many exchanges have terms which state that the customer deposits assets on the exchange and becomes an unsecured creditor. If that is the case, then there is no entrustment, and a debt which is not paid is not a crime. To that, Supreme Court has always emphasized that it is a case of substance, not labels, and a platform that offers to separate the money of its users and then spend them on itself is in violation of an express or implied trust. Whether the platform presented itself in a certain way, whether the assets were actually collected in a certain way, and whether the funds were commingled will be key issues in the question.

4.5 Receiving and Dealing in Illicitly Acquired Digital Assets

Crypto frauds are usually quickly washed, in a variety of methods, including through mixers, a series of wallets, peer-to-peer transactions, or the transformation into stable coins or cash. Section 317 can be passed to the ultimate recipient who knowingly receives them, where the proceeds are considered "stolen property" under the definition, which is most easily where the proceeds are derived from a cheat, extortion or breach of trust. Money laundering as an offence in PMLA is generally the better option because the offence is targeted directly at the concealment and utilization of the proceeds of a scheduled offence and because the offence permits attachment. The best combination is between the BNS and the PMLA, the former covering the predicate offence, and the latter following the money.

4.6 Evidence and jurisdiction issues in determining ownership and possession of a corporation, partnership or trust.

That the accused had the keys at the time of the offence must be proved to establish that the accused was the owner of that particular token. Public block chains don't record identities, only transactions. The association between an address and a person typically is derived from exchange know-your-customer records, device forensics or a confession. Where the keys are in the custody of a foreign custodian, the investigator must obtain the records of that custodian, which is likely to require assistance or co-operation. But when the assets have passed through multiple jurisdictions, even determining the place of the offence could be a matter of debate. These problems are discussed in detail in chapters 7 and 8.

5. Online Fraud, and the Growing Area of Property Offences

5.1 Online Cheating and Fraudulent Inducement –

Section 318 of the BNS Cheating is not discriminating, as to whether deception is expressed in a counter or a continent. A message, a call or a web page is sufficient; as long as the victim is made to give up property, including money and tokens. Dishonest intention at the time of the inducement, which is required by the Supreme Court in the case of Hridaya Ranjan Prasad Verma, is difficult to prove on the internet, because fake identities, fake numbers and fake accounts are all proof of planning.

5.2 Avoiding digital deception, impersonation and identity theft.

The vast majority of online frauds start with impersonation – as a fake bank representative, courier company, government official, or some family member in distress. The forgery provisions (sections 336 and 340) may apply to a cloned website or forged electronic message as the Sanhita regards electronic messages as documents, as could also Section 319 of the BNS which covers cheating by personation. SIM-swap fraud involves both personation, before it issues the duplicate SIM, and unauthorised access, after it issues the duplicate SIM — typically covered by both the BNS and the IT Act.

5.3 The final category is phishing, UPI Fraud, Payment Fraud and Banking-Related Offences

The last category is Phishing, UPI Fraud, Payment Fraud and Banking-Related Offences. Indian courts took the lead when it came to phishing. NASSCOM v. Ajay Sood (2005) 119 DLT 596) Delhi High Court lifted the ban on email messages that impersonate a genuine organization for the purpose of collecting personal information. Since then, the methods have increased in number; voice and SMS phishing, collect-request and QR-code schemes on UPI messages, and remote-access applications, but most recently "digital arrest" messages stating that individuals are being investigated and they must pay for verification. These scams were brought to the notice of Supreme Court through suo motu cognizance in late 2025 and it sought a coordinated investigation.

One constant problem is that the victim typically made the authorization, but was tricked into doing so. Banks will sometimes say that this takes the end of their responsibility.

On one hand, RBI's circular dated 6 July 2017 on "Limited Liability in Unauthorised Electronic Banking Transactions" has been an attempt to solve part of the issue by providing the customers with zero liability for any unauthorised transactions done by third parties within three working days, and limited liability thereafter. That is civil/civilian and civil/criminal protection of the fraudster under section 318 are separate from each other.

5.4 Students will learn to recognize the signs of investment scams, cryptocurrency fraud and ponzi schemes.

Ponzi schemes pay early investors with money from later investors, and fall apart when there is a decline in recruitment. Indian laws are targeting them from various angles: Prize Chits and Money Circulation Schemes (Banning) Act 1978, state deposit-protection laws and in the BNS section 316 and 318(4). If a group is running the scheme, the provisions for organised crime, now included in section 111 of the Act (which include Cyber-crime and Economic Offences), may be invoked. Crypto variants like the GainBitcoin, which the CBI delved into, abided by the same formula – only with different terminology – offering guaranteed payouts in bitcoin and commissions for recruiting. The modern day alternatives are fake trading applications and bogus "mining" offers. Typically, money laundering cases are filed simultaneously with a PMLA case and can afford the investigators the ability to attach assets.

5.5 Extortion and Ransomware attack

Ransomware is textbook extortion: attacker places victim in fear of continuing loss, typically by encrypting or threatening to leak data and demands ransom, typically in cryptocurrency. This is because Section 308 of the BNS fits, its object being 'any property or valuable security', and the intrusion is dealt with by the sections of the IT Act dealing with 'exploitation' in section 43 and 'breach of privacy' in section 66. There is a possibility of applying section 66F where critical infrastructure is attacked. The ransomware attack on AIIMS Delhi in 2022 was an eye opener of the value of what was at stake. CERT-In's guidelines from April 2022 now mandate reporting such events within 6 hours which will assist in the tracking but does not impose any liability on the victim. Extortion under s. 308 is also "sextortion" (where intimate images are used as leverage), and the extra offences under the IT Act for private images.

5.6 Difference between Cheating under the BNS & Offences under the Information Technology Act, 2000.

Both offences are similar, but not exactly the same. Deception or inducement is required in section 318 and delivery of property is required for the aggravated form of the section. Section 66D of the IT Act makes cheating by means of a computer resource or by means of a communication device a requirement and section 66C of the IT Act requires fraudulent or dishonest use of another's electronic signature, password or unique identification feature. The IT Act offences are much less far reaching in terms of what they cover and are less stringent in terms of penalties: on up to three years for the IT Act offences as opposed to seven years for section 318(4) and five years for section 319(2). The difference in punishment would also change the procedure under the Act as the three year offences will be treated as bailable under the IT Act.

5.7 The role of intermediaries, platforms and other digital actors in the process of crime.

Criminal liability of intermediaries, platforms and other digital actors. Intermediates have a "conditional" shield. Even if they provide access to third party content without initiating it or selecting it, and they perform due diligence, they are also under the protection of Section 79 of the IT Act and are not liable for the content.

In **Shreya Singhal v Union of India (2015) 5 SCC** 1 the Supreme Court interpreted the provision as mandating some form of actual knowledge – either by a court order or by a government notification – before a platform can be compelled to act. The Delhi High Court has ruled that the protection of a marketplace shall be withdrawn from one that is active in the market

(Christian Louboutin SAS v. Nakul Bajaj, 2018). It is a question of knowledge and participation: whether there is a platform that is criminally liable for those that make scam ads on it, or for platforms hosting mule accounts. While the mental state can be of the controlling officer**s (Iridium India Telecom Ltd. V. Motorola Inc. (2011) 1 SCC 74**) the mental state of the individual directors requires a specific allegation and where the mental state is derivative, the Court has insisted that the company be arraigned **(Aneeta Hada v. Godfather Travels (2012) 5 SCC 661).** There is a distinction between negligence by a bank or by a platform and crime: a crime requires showing that the bank or platform was knowingly complicit.

6. Relationship of BNS 2023 with Information Technology Act 2000

6.1 The use of both general criminal law and special cybercrime law.

The IT Act supplements the penal code for offences which are also punishable under the penal code. Section 77 of the IT Act states that compensation and penalties under the IT Act shall not bar other penal consequences under other laws and section 81 provides that the IT Act shall prevail over any inconsistent laws. There is a bar on prosecution under both acts, both for the same individual and for the same act, in terms of section 26 of the General Clauses Act, 1897 and article 20(2) of the Constitution and section 337 of the BNSS. The real issue is would two charges be considered for the same offense. The question in the test in State of Bombay v. S.L. Apte (AIR 1961 SC 578) is not whether the facts coincide but whether they are substantially the same.

6.2 Section 43 and Section 66 of the IT Act:

Unauthorised Access and Computer-Related Offences law is also known as the Information Technology (Access to Computer and Related Services) Act, 1994.

Section 43 prohibits access to a computer resource, downloading or copying data, introducing a virus, causing damage to information and data or reducing the value or usefulness of information without permission of the owner of the computer resource. Establishes civil responsibility for a compensation payment. Where any of the foregoing acts are done dishonestly or fraudulently, it becomes a crime under Section 66, punishable by up to 3 years imprisonment and a fine of N100,000. These are the offences which come closest to the unauthorised-transfer gap mentioned above as it does not involve any property, movement, or deception.

6.3 Section 66C: Identity Theft

Section 66C is a criminal section that provides protection against the use of another person's electronic signature, password or other unique identification feature that is fraudulent or otherwise dishonest. It detects unauthorized access, the very thing bank-account takeovers rely on. It's silent on what the wrongdoer then does with the account, hence the addition of the charges of cheating or breach of trust.

6.4 The definition of 'cheating by personation using computer resources' is clarified in Section 66D.

Section 66D is a penalty for cheating by means of a communication device or computer resource involving personation. Recreates section 319 of the BNS in most aspects but with a less severe punishment. It is not unusual to charge both of them and defendants attack it.

6.5 Offences Overlapped, Double Jeopardy and Statutory Interpretation.

There are two conflicting decisions. In **Sharat Babu Digumarti v. Government of NCT of Delhi, (2017) 2 SCC 18,** Supreme Court relied on the special-over-general principle and under section 81 of the IPC rejected its application in view of the comprehensive provisions in the IT Act for the electronic transmission of obscene material.

In **Gagan Harsh Sharma, the Bombay High Court** had ruled along the same lines with respect to data theft. But Digumarti was for committing offences of almost the same nature. If the BNS offence has an extra element - for example, inducing delivery of property - then the offences are different according to the Apte test and both can be charged. The better reading is of course the one that the Courts should subscribe to, which is that the IT Act replaces the BNS when the ingredients of the offences are substantially the same.

6.6 A multi-statutory case is an investigation or prosecution involving more than one statutory agency

A multi-statutory case is one that involves more than one statutory agency. It is noted that the IT Act, section 78, calls for an officer of at least inspector rank to investigate BNS offences while investigations of IT Act can be done by officers of a lower rank. Charges in both fields lead to procedural conflict, conflicting skills and, at times, motions to quash charges on the basis of the other. Much of this friction could be eliminated by having a brief, consistent charging procedure.

7. Digital Evidence & Proof of Property Offences.

7.1 The ability to recognize and document the ownership and transactions involving electronic records.

To identify and record ownership and transactions with electronic records. The ownership and loss are established in digital cases by bank statements, wallet logs, transaction hashes, chat messages and images of the devices. In the BSA 2023 electronic records are treated as documents and section 61 provides that electronic records are treated as other documents.

7.2 Under the Bharatiya Sakshya Adhiniyam, 2023, the admissibility of Electronic evidence was discussed.

The certificate requirement of the BSA, which is now identical to the one in the Evidence Act, is kept under section 63 of the BSA, instead of section 65B.

The case law shall continue to be the basis. In the above case, **State (NCT of Delhi) v. Navjot Sandhu (2005) 11 SCC 600,** the Court has accepted the printout without the certificate. It has been overruled by Anvar P.V. v. P.K. Basheer ((2014) 10 SCC 473) and the necessity of the certificate has been laid down.

In **Shafhi Mohammad v. State of H.P. ((2018) 2 SCC 801)**, the rule that a party could not get the certificate has been relaxed and in Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal ((2020) 7 SCC 1), the decision in Shafhi has been overruled and the rule of Anvar has been restored with directions that the certificate be produced at an appropriate stage. An objection against the absence of a certificate has to be raised at the trial in Sonu v. State of Haryana ((2017) 8 SCC 570).

7.3 The knowledge and skills needed to package, collect and preserve data with integrity and authenticity is a chain of custody and forensic integrity.

The BNSS provides assistance to the process. The details of searches and seizures have to be captured by audio visual recording under section 105 and section 176(3) requires that the scene of a crime is forensically examined where the offence carries a maximum term of 7 years or more. Electronic records may be ordered or summoned by summons or order as provided in section 94. All investigators create forensic images, record hash at time of seizure, document all hands over and securely store originals. There is no loss of admissibility of evidence because of a break in the chain, only a reduction in the weight of the evidence.

7.4 The process of block chain records, transaction trails and cryptocurrency tracing is known as Attribution and is taught in lesson

Help is on hand with the block chain's public, permanent records. Specialist software clusters addresses and tracks funds throughout wallets and the output is ordinarily given in the shape of an expert beneath the BSA's stipulation on expert opinion. The weakest link is the attribution, that is the connection between an address and a person. These links are usually traceable to an exchange's "custodial records," the forensics of the devices, IP records and/or banking records and each would require an independent authentication.

8 The extent of jurisdictional challenges and enforcement difficulties. Magnitude of jurisdictional challenges and enforcement challenges.

8.1 Internet and Network Security Practices and Standards

The BNS also has an extraterritorial application and applies to offences against a computer resource located in India (Section 1(4)) which is similar to section 75 of the IT Act. Domestically, the BNSS continues the principle that an offence may be tried at the scene of the offence, or at the place where the offence was felt to have resulted: however, there will be specific rules for offences of cheating involving telecommunication messages. The Supreme Court cautioned against extending territorial jurisdiction with trifling connection (Y. Abraham Ajith v. Inspector of Police, (2004) 8 SCC 100) and such cases frequently being initiated in the wrong police station.

8.2 The anonymity, encryption, DeFi and Attribution of Conduct (AOC)

It is hard to determine who to arrest or to which court to apply for freezing orders, in view of the privacy tools, mixers, foreign exchanges and decentralised protocols, which lack an identifiable operator. Bank accounts may be frozen as "property" under the seizure power of the CrPC as laid down in **Tapas D. Neogy v. State of West Bengal ((1999) 7 SCC 685)** and the seizure and attachment of proceeds of crime has now been covered by the BNSS sections 106 and 107. When keys are not in the custody of the Freezer, it will be more difficult to freeze tokens.

8.3 This section focuses on the issue of international cooperation, mutual assistance and evidence sharing

In this section, the emphasis is on international cooperation, mutual assistance and sharing of evidence.

The India is not a signatory to the Budapest Convention, but the UN Convention against Cybercrime, which was adopted in December 2024, could provide a framework in the future. In fact, investigators make use of mutual legal assistance treaties, and Letters of Request under the BNSS, which are

not as rapid as the movement of funds. The platforms and I4C's national reporting portal and helpline (1930) have achieved better results in the freezing of funds in a prompt manner.

8.4 Issues confronting the police and prosecutor

The recurring issues include inadequate forensic capabilities, inequal training of technical officers of the district police, inability to get hold of records from intermediaries, under reporting by victims and lack of jurisdiction over many fraudsters. Captures of cyber-fraud continue to be low.

9. New judicial Decision and development in the law

9.1 Judicial Approaches to Property & Dishonest Inducement

The analysis of cases on property offences is often the interpretation of the words of the offence and evidence of intent/possession/trust/inducement. In online cases, the courts should exercise the same discipline keeping in mind the possibility of electronic recording of the relevant conduct. It's not like a digital interface will get rid of the need to establish a dishonest intention. Equally.

Different from civil dispute and criminal cheating is particularly important in commercial transactions. At the time of the relevant acts, did the accused have a dishonest intention or did it lead the victim to believe a representation was deceptive or did it lead to the victim taking an action? If another breach occurs, it might be in context but it is not sufficient proof. In digital.

9.2 The use of electronic evidence and fair trial.

There must be a concern with the admissibility of electronic records in court as well as the reliability of the specific record. The courts should investigate who created the record, how it was kept, if it is complete, if it is known what technical process created the record, and whether the opposing party can challenge the record. Where expert evidence is required it will be used.

In digital cases, the importance of fair-trial protections is much the same, as records may seem objective and yet be misinterpreted. A connection could be an IP address, a wallet transfer could be a movement of funds and a screenshot may not contain pre-existing messages. In the judicial level, judicial reasoning should differentiate between what the record was and what is.

9.3 Cryptocurrency and gaps in the existing interpretation

The interpretation of cryptocurrencies under the law might differ depending on the issue under consideration. There is room for an economy in a non-legal tender currency! It can be held on a custodial contract, transferred on a distributed ledger or be represented by a tokenised contract. The court needs to pinpoint the legal interest at.

A court should recognize the interpretive challenge when the language of a criminal statute does not explicitly address a new digital object, instead of deciding the issue by making an analogical extension based on the statute's text.

9.4 Avoid relying on precedent. Take care not to follow precedent

It is good research paper to not make up cases or assume propositions as a judgment without checking the actual judgment. There are basic ideas that can be applied from the existing criminal law, but a case involving physical property or a different law may not be the right case to determine the meaning of cryptocurrency under the BNS. The author should review the article prior to publishing.

This paper thus does not attempt to offer illustrations in hypothetical situations as judicial precedents. It recognizes that judicial interpretation is an evolving process and suggests that any discussion of a specific case be included only in light of a thorough search of a reliable legal information system or a court. This would be better than adding lots of unverified citations to a reference list and make it less credible.

9A. The importance of relevant judicial decisions and how they apply.

The State of Bihar v. **9A.1 Hridaya Ranjan Prasad Verma (2000)**

Cheating implies dishonest or fraudulent intention at the time of the act of inducing to commit the offence, and if there is failure to perform the act of promise after the inducement, it does not of itself lead to the conclusion of the dishonest or fraudulent intention. This is a very relevant to the issues of online investment and marketplace conflicts.

9A.2 Anvar P.V. v. P.K. Basheer (2014)

The Supreme Court in Anvar P.V. v. P.K. Basheer, (2014) 10 SCC 473, discussed the evidence of e-documents in terms of the then Indian Evidence Act, section 65B. The judgment highlighted that computer output offered as an electronic record has to meet the sown conditions.

9A.3 Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)

In Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1 a Constitution Bench discussed the requirement for a certificate with respect to electronic records under section 65B of the old Evidence Act and drew lessons from the decision of the then Privy Council in Anvar P.V. The case highlights why it's crucial to determine the origin and how the electronic material was made. In.

9A.4 The Internet and Mobile Association of India v. Reserve Bank of India, 2020 (9A)

The case of 9A.4 – Internet and Mobile Association of India v. Reserve Bank of India, 2020, involved a similar situation.

The Reserve Bank of India had issued a circular restricting regulated entities from providing services in relation to virtual currencies in 2018 which was considered by the Supreme Court in the case of Internet and Mobile Association of India v. Reserve Bank of India, (2020) 10 SCC 274. The Court ruled that the circular is disproportionate. The ruling is important because it's an example of (supply above) were provided to help clarify the intent of the statute.

9A.5 State (NCT of Delhi) v. Navjot Sandhu (2005) and subsequent explanation were given to assist in clarifying the intent of the statute.

The case of State (NCT of Delhi) v. Navjot Sandhu, 2005 11 SCC 600 has been quoted while in relation to electronic evidence. Later, the way of proving electronic records was rethought in Anvar P.V. and the main principles were elaborated in Arjun Panditrao Khotkar. The case is of limited use other than as a reminder that legal positions.

10 The BNS is not adequate to handle these issues. These issues cannot be addressed by the BNS.

10.1 Must have a definition for existing Definitions and Digital Assets.

The BNS can tackle numerous types of online dishonesty as the harm is likely to be a familiar one – such as money, property, assets that are entrusted to another, or a person who is deceived and forced to act.

A limited reading can leave some instances of appropriation unreachable with the existing crimes and a broad reading can jeopardize the rule of law. The answer doesn't lie in simply ramping up the definition of "property crime," but in highlighting patterns and pinpointing them with great specificity. The use of digital representations of can be clarified through legislation.

10.2 Conduct that depends on or is enabled by technology. Cyber-Dependent and Cyber-Enabled Conduct

In cyber-dependent offences, the computer systems or networks are an essential part of the offence—whether the object or instrument of the conduct—such as when committing certain kinds of unauthorized access or interference with data.

Clear classification enhances charging and allocation of resources. This will also help to eliminate the false notion that all frauds involve hacking. Others are scams that are entirely based on voluntary action brought about by a false representation. There are also those that have a direct intrusion into the accounts. The actual method should be mirrored by the legal option. There can be more than one offence in a case, but each.

10.3 The process of classification, punishment and decentralized transactions are incomplete.

New technologies generate situations that don't fit into the old categories. A smart contract can make the transfer after a misleading input, a compromised wallet can be emptied without any interaction with the victim, an NFT can be transferred without any changes to the copyright. All these examples pose a different set of questions of control and consent.

Any reform should be technology neutral, but not at the same time as it is vague. Should include definition of relevant conduct, protected interest, required mental element and defences. It must also differentiate between intentional appropriation and errors, protocol lapses, and bona fide rights issues. Penalties should be commensurate with culpability, harm and planning and repeat offending, Recovery.

10.4 Overall Assessment

The BNS should not be considered as a comprehensive cybercrime legislation. Where the conduct meets their elements, its current provisions continue to be helpful. The IT Act deals with certain harms relating to the use of computers, the BSA prescribes evidence-related issues. Sufficient is therefore not just measured by the words of one offence, but. The biggest challenge is the lack of clarity at the edges: how unfixed digital interests can be incorporated into the framework of property concepts and in the context of the old property law; how electronic proof can be used to demonstrate control and intention; and how cross-border cases can be swiftly and legally investigated.

11. Recommendations

11.1 Proposals for legal and policy change Describe and explain digital property concepts.

Parliament should think about whether there is a need for a careful wording or a focused provision to deal with digital representation of value and control of certain types of property offences.

Any definition must make a clear distinction between who owns the token and who owns the content it references; and between an account on a platform and the contractual rights that it represents.

11.2 Ensure that the BNS and IT Act are in harmony with each other.

Explicit guidance should be provided on how both general offences and the special offences relating to cybercrime overlap in common cases. A practical guide to the charging under section 318 of the BNS and personation under section 319 and sections 66C and 66D of the IT Act; and an explanation of sections 43 and 66 are all possible ingredients of a practical charging guide. Such guidance. Prosecutors should keep a record of the grounds for the necessity of each charge and the elements of the facts which are being charged. In cases where it is alleged that provisions are being infringed in more than one respect, the case file shall point out whether the allegations are for separate conduct or for different aspects of the same conduct. Joinder training, principles of double-jeopardy, and fair notice would decrease overcharging and make the clarification of.

11.3 Explain how to make Digital Evidence Standards better.

It should convey the fact that a tool can set a precedent and it cannot stop a trend. The guidance should be kept up to date with changing technology, and created in consultation with forensic experts, prosecution and judges and defence practitioners and service. Electronic evidence reports should be clear and concise and identify the source, the way the evidence was obtained (including tools and versions used), methods used to ensure integrity of evidence, limitations of the method, and any assumptions made to derive the conclusion.

11.4 Enhance Investigative and Inter-Agency Co-ordination.

Cybercrime investigations often involve the coordination of local police, specialised cybercrime units as well as banks, payment networks, telecom operators, exchanges and digital platforms. One person designated as a case coordinator may keep a timeline and ensure preservation requests are made to the parties in a timely fashion, and may follow up on responses. Having secure means of communication to share relevant information can minimise the duplication of information and limit the unnecessary exposure of personal information.

Training should be hands-on and on-going. Knowing how to identify common social engineering techniques, digital wallets, payment flows and account takeover, along with the fact that IP addresses have limited evidence, is important for officers. The prosecutor must participate at an early enough stage in the process to detect when evidence is lost and to see if there are elements in the case that are missing from the legal elements of the crime. Technical experts should be on hand to discuss complicated systems; their findings.

11.5 Funding for victims' compensation, restitution and asset recovery is provided by Victim Compensation, Restitution and Asset Recovery.

A clear reporting pathway and realistic information on what can be done now is needed by a victim. If a prompt report is made, it may enable an institution to mark a beneficiary account, keep records or trigger a dispute process these will depend on the facts and the rules that apply. Vitamins should be provided to victims to keep the references, communications and.

The use of lawful freezing, seizure, restitution and compensation procedures as they exist and are appropriate should be utilized by courts and authorities. There is a need to ensure that asset recovery does not infringe on the rights of other people and does not make the assumption that any asset in a destination account is the accused's. There needs to be a clear way to inform impacted individuals and contest errors and incorrect freezes while protecting innocent customers.

11.6 The following legislative review and judicial guidance are pertinent to this case:

There is potential to outline common themes in digital-property cases in judicial training materials, such as identifying what constitutes the asset, determining ownership and control, determining consent, understanding electronic records and avoiding an assumption of identity based on a transaction trace.

There should be regular legislative oversight to gather anonymous data on charging issues, gaps in evidence, the outcomes of charging, and recurring questions for interpretation. This review should be done with the accurate facts and not based on an assumption. If there is a regular disparity between the two, then Parliament may consider a specific amendment. This is better than hasty and technology-specific criminalization which can turn into.

12. CONCLUSION

12.1 The significant findings from the study are presented in section

This paper has explored application of BNS, 2023 in the context of property based wrongdoing in the digital economy. It identifies that there are a large number of online frauds that can be analysed under the existing offences as it is in essence a wrong – deception, dishonest appropriation, misuse of entrusted property or taking of value without lawful authority. The Evidence changes in the online setting. The study also reveals that not everything that is digital is legal. Different interests are a bank balance, a cryptocurrency token, a platform account, a private key and a digital file. They can have different ownership, control, transfer and legal status. Therefore, it would be wrong to say that all unauthorized digital transfers.

12.2 Property offences in the digital economy have to be reconsidered.

The proof of inducement and financial loss, and identity and control are now at the heart of electronic evidence. However, technical records need to be analyzed carefully. A transaction hash can prove a transfer was made; it can't prove the address the transfer was made from (or to) was controlled by someone, or that the transfer was dishonest. The login record might indicate that an account was. Issues of jurisdiction and enforcement also arise when the victims, the offender and the accounts and providers of the service are located in various places. The chances of obtaining evidence and recovering assets can be enhanced through swift preservation, meticulously drafted requests, well-trained investigators and the collaboration of public and private institutions. Such measures must be accompanied with privacy protection, proportionate and fair procedures. Efficiency.

12.3 towards a coherent and technology-responsive framework

The central thrust is a balanced approach of interpretation, institutional enhancement and specific legislation elucidation. The approach of the courts is to invoke preexisting offences if the language of the statute is reasonably susceptible to the offences in question; but to not extend criminal liability by analogy when it is not supported by the language of the statute. Parliament needs to provide greater clarity on the uncertainty that surrounds digital currencies if there is evidence. There needs to be a cohesive structure that is designed to safeguard the rights of accused individuals and victims. It should benefit the ease of fraud reporting, record keeping, tracing assets and obtaining restitution, and ensure fair proof of ownership, intention, and identity. Legislation will not be able to keep up with the pace of digital technology change and the best lasting legal effect.

References:

A. STATUTES

Bharatiya Nyaya Sanhita, 2023.

Indian Penal Code, 1860.

Information Technology Act, 2000.

Income-tax Act, 1961.

B. BOOKS

The Bharatiya Nyaya Sanhita, 36th Edition, LexisNexis, 2024, Ratanlal & Dhirajlal.

P.S.A. Pillai, Criminal Law, 14th edn.

The Textbook on the Bharatiya Nyaya Sanhita has been written by K.D. Gaur.

Computers, Internet and New Technology Laws, by Karnika Seth.

C. ARTICLES / REPORTS

New Criminal Laws – Justice K.T. Thomas on Cyber Crimes and Property Offences (2024).

The NITI Aayog Blockchain and Digital Assets: Regulatory and Policy Materials document

provides an overview of the regulatory and policy landscape.

Reconceptualising theft and criminal law in the digital age, Abhinav Sekhri.

D. CASE LAWS

Internet and Mobile Association of India v. Reserve Bank of India ((2020) 10 SCC 274),

Gagan Harsh Sharma v. State of Maharashtra (2018)

NASSCOM v. Ajay Sood (2005) 119 DLT 596)

State (NCT of Delhi) v. Navjot Sandhu (2005) 11 SCC 600

Shafhi Mohammad v. State of H.P. ((2018) 2 SCC 801)

Tapas D. Neogy v. State of West Bengal ((1999) 7 SCC 685)

The State of Bihar v. 9A.1 Hridaya Ranjan Prasad Verma (2000)

Anvar P.V. v. P.K. Basheer (2014)

Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal (2020)

Sonu v. State of Haryana ((2017) 8 SCC 570).