Page 3800 - 3809 **DOI:** *https://doi.org/10.63108/IJLMH.13123*

INTERNATIONAL JOURNAL OF LAW MANAGEMENT & HUMANITIES

[ISSN 2581-5369]

Volume 9 | Issue 5

2026

© 2026 *International Journal of Law Management & Humanities*

Follow this and additional works at: https://www.ijlmh.com/
Under the aegis of VidhiAagaz – Inking Your Brain (https://www.vidhiaagaz.com/)

This article is brought to you for free and open access by the International Journal of Law Management & Humanities at VidhiAagaz. It has been accepted for inclusion in the International Journal of Law Management & Humanities after due review.

In case of **any suggestions or complaints**, kindly contact **support@vidhiaagaz.com**.

To submit your Manuscript for Publication in the **International Journal of Law Management & Humanities**, kindly email your Manuscript to **submission@ijlmh.com.**

Cheating and Forgery in the Digital Age under the Bharatiya Nyaya Sanhita, 2023: Fabricated Records, Online Personation and the Proof of Intention

K. DURGA DEVI[*] AND LEKSHMI V.S.[**]

ABSTRACT

Online dealings rest on two kinds of trust: trust in what people tell one another, and trust in the records that prove what was agreed. Cheating attacks the first, and forgery attacks the second. This paper studies how the Bharatiya Nyaya Sanhita, 2023 (BNS) treats both wrongs in digital settings, concentrating on Sections 318, 319, 335, 336, 337, 338 and 340. It asks how fabricated PDFs, altered electronic records and misused electronic signatures fit within those provisions, and where the line falls between a forged record and one that is merely untrue. The paper also considers the complementary provisions of the Information Technology Act, 2000 and the proof of electronic evidence under the Bharatiya Sakshya Adhiniyam, 2023. Its argument is that the BNS already speaks to digital wrongdoing in express terms, so the real difficulty lies in proving who made or used a record, what intention accompanied that act, and whether the record is authentic. Technology changes the offender's tools but not the ingredients of the offence, and those ingredients remain the safeguard against wrongful conviction. The paper closes with recommendations for investigators, courts and institutions.

Keywords: *Bharatiya Nyaya Sanhita, cheating, forgery, electronic records, electronic signature, personation, cybercrime, Bharatiya Sakshya Adhiniyam*

I. INTRODUCTION

A single e-mail can persuade someone to transfer money. A PDF can seem to certify a degree. A few typed lines can appear to authorise a payment. The same convenience that makes these tools useful also lets a dishonest person mislead a recipient or manufacture apparent authority. Criminal law has to tell these wrongs apart without treating every inaccurate file, or every failed online deal, as a fraud.

[*] Author is a Student at Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya, Kanchipuram, Tamil Nadu, India.

[**] Author is a Faculty at Anvikshiki School of Law, Sri Chandrasekharendra Saraswathi Viswa Mahavidyalaya, Kanchipuram, Tamil Nadu, India.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

The difference between cheating and forgery lies at the centre of the topic. A person can cheat by a dishonest spoken promise without producing any document at all. A forged record, in turn, may be made before anyone has been misled by it. One transaction may involve both wrongs, as when a fabricated record is used to obtain money or some other legally significant response from a victim.

This paper examines how the Bharatiya Nyaya Sanhita, 2023 (BNS) handles the overlap.[1] The analysis reads the text of the statute together with Supreme Court decisions on the ingredients of the two offences. Those decisions were given under the Indian Penal Code, 1860 (IPC) and are used here for the principles they state, not as rulings on the BNS itself. The digital scenarios discussed are hypothetical illustrations and not reports of decided cases.

II. Cheating, forgery and electronic records under the BNS

A. Cheating under Section 318

Section 318(1) describes two routes to cheating. On the first, the accused deceives a person and, by doing so, fraudulently or dishonestly induces that person to hand over property or to agree that someone else may keep it. On the second, the accused deceives a person and intentionally induces an act or omission which that person would not have undertaken but for the deception, and which causes or is likely to cause damage or harm to body, mind, reputation or property. An Explanation adds that dishonest concealment of facts is itself a form of deception.[2]

Two consequences follow. First, a false statement standing alone is not cheating, because the deception must be linked to the response it produced. The prosecution has to name the person deceived, show what that person was induced to do or not to do, and prove the statutory consequence together with the required state of mind. Second, cheating is not limited to financial loss, since the second route reaches certain non-financial harms as well. The aggravated form in Section 318(4) nevertheless has ingredients of its own and cannot be invoked merely because a quarrel involves money.

The sentencing structure is graded. Ordinary cheating under Section 318(2) carries imprisonment up to three years, a fine, or both. Section 318(3) raises the ceiling to five years, with a fine or both, where the accused knows that wrongful loss is likely to fall on a person whose interest in the transaction the accused was bound by law or by a legal contract to protect. Section 318(4) carries up to seven years and liability to fine for cheating that dishonestly induces

[1] Bharatiya Nyaya Sanhita, 2023, No. 45 of 2023, § 358 (India) [hereinafter BNS] (repealing the Indian Penal Code, 1860, No. 45 of 1860 (India) [hereinafter IPC]).
[2] BNS § 318(1) & Explanation.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

the delivery of property or the making, alteration or destruction of a valuable security, or of anything signed or sealed that can be converted into one.[3] The grading matters in digital cases. Sending a dishonest message does not automatically bring the seven-year offence into play. Investigators must show what the recipient actually did because of the deception and how that conduct meets the particular sub-section chosen.

B. Cheating and breach of contract

A broken promise is not cheating by itself. The Supreme Court has repeatedly held that criminal liability depends on a dishonest intention present when the inducement was made, so that a later failure to perform, without more, leaves the matter in the realm of civil law.[4] The principle applies directly to online trade. A seller who honestly accepts an order and later cannot supply the goods has committed, at most, a breach of contract. A seller who takes payment on a promise that he never meant to keep stands differently. The move to digital communication does not remove the need to prove that starting point.

C. Forgery under Sections 335 and 336

Section 336(1) defines forgery as the making of a false document or false electronic record, or part of one, with one of several specified intentions: to cause damage or injury to the public or to any person, to support a claim or title, to cause a person to part with property or enter into a contract, or to commit fraud or enable fraud to be committed.[5] A false statement is therefore not enough. The record must be false in the legal sense explained by Section 335, and the required intention must accompany its making. Whether the deception eventually succeeds is a separate matter from whether forgery has already been completed.

Section 335 recognises three routes to making a false document or record. The first covers dishonestly or fraudulently making, transmitting or authenticating a record so that it appears to come from a person or authority who did not make or authorise it, and it expressly extends to electronic records and electronic signatures. The second covers material alteration without lawful authority. The third covers dishonestly or fraudulently causing someone to execute, alter or electronically sign a record when that person, through unsoundness of mind, intoxication or a deception practised on him, does not understand its contents or the alteration.[6]

A useful distinction is that between authenticity and truth. A genuine author may put a false claim into a document of his own without necessarily falling within Section 335. By contrast,

[3] BNS § 318(2)–(4).
[4] *Hridaya Ranjan Prasad Verma v. State of Bihar*, (2000) 4 SCC 168, ¶ 15 (India).
[5] BNS § 336(1).
[6] BNS § 335(A)–(C).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

fabricating a certificate so that it seems to have been issued by a university raises directly the question of false authorship or authority. The Supreme Court has drawn the same line: executing a deed in one's own name while claiming a title one does not hold differs fundamentally from impersonating the owner or falsely claiming authority to act for the owner, and if what is executed is not a false document there is no forgery.[7] Other offences may apply to the first situation even where forgery cannot be established.

Penalties follow the purpose of the forgery. Ordinary forgery under Section 336(2) attracts imprisonment up to two years, a fine, or both. Forgery committed for the purpose of cheating, under Section 336(3), attracts up to seven years and liability to fine. Forgery intended, or known to be likely, to harm the reputation of any person, under Section 336(4), attracts up to three years and liability to fine.[8] The prosecution should therefore explain whether a forged digital file was made to obtain property, support a claim, damage reputation or serve some other prohibited end. The software used to produce the file has no bearing on the sentence.

D. Electronic records and digital documents

The BNS recognises electronic material in express terms. Section 2(8) brings electronic and digital records within the definition of "document," and Section 2(39) gives any word that the Sanhita does not define the meaning assigned to it in the Information Technology Act, 2000 or the Bharatiya Nagarik Suraksha Sanhita, 2023.[9] Together these provisions connect the traditional documentary offences with modern records. A fraudulent electronic record need not be printed before the forgery provisions apply. Equally, a file is not forged merely because it was edited, and the court must separate an authorised correction, a plainly labelled draft or an innocent error from dishonest fabrication or unauthorised material alteration.

"Electronic signature" is itself a legal term. A pasted image of a handwritten signature is not automatically an electronic signature in the statutory sense.[10] Yet using such an image to manufacture an appearance of approval may still amount to making a false document or electronic record where the ingredients of Section 335 are made out.

Consider an applicant who creates a PDF that purports to be a degree certificate issued by a university and submits it to obtain a job. The apparent issuing authority and the purpose of the record are central to the forgery inquiry. If the aim is to deceive the employer, Section 336(3)

[7] *Mohammed Ibrahim v. State of Bihar*, (2009) 8 SCC 751 (India).
[8] BNS § 336(2)–(4).
[9] BNS § 2(8), (39); *see also* Information Technology Act, 2000, No. 21 of 2000, § 2(1)(t) (India) [hereinafter IT Act] (defining "electronic record").
[10] IT Act § 2(1)(ta) (defining "electronic signature"); *see also* BNS § 335, Explanation 3 (adopting the IT Act meaning of "affixing electronic signature," IT Act § 2(1)(d)).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

may be relevant, while a charge of cheating would need separate proof of the inducement and its consequences. Now consider an employee who receives a genuine electronic invoice, changes the payment details without authority and sends it on for approval. The unauthorised material alteration may engage Section 335, and whether other offences also arise depends on the employee's intention, the use made of the altered record and the transaction that followed. Neither example shows that every private certificate falls within the graver public-record provision, whose application has to be established separately.

E. Public records, valuable securities and use of forged records

Section 337 deals expressly with forged court records, government-issued identity documents, public registers and similar records, including their electronic forms, and its Explanation brings electronically maintained entries within the meaning of "register." The punishment extends to seven years and liability to fine.[11] Section 338 prescribes a heavier range for specified valuable securities, wills and certain authorities and acknowledgements: imprisonment for life, or for up to ten years, with liability to fine.[12] Whether Section 338 applies turns on the legal character of the document, not on the fact that a file is digital or that a large sum is involved. Digital forgery is therefore not a single offence with a single penalty. The nature of the record and the prohibited purpose select the provision.

Section 340(2) separately punishes the fraudulent or dishonest use, as genuine, of a document or electronic record which the user knows or has reason to believe to be forged, and the user is punished as if he had forged it.[13] Maker and user can be different persons. One who knowingly submits a forged digital certificate cannot escape merely by saying that someone else created it. An innocent recipient who forwards a record without the required knowledge, and without dishonest or fraudulent use, is not guilty by that fact alone.

F. Personation and the Information Technology Act

Section 319 deals with cheating by personation. A person commits it if he cheats by pretending to be someone else, by knowingly substituting one person for another, or by representing that he or another person is someone other than the person he or she really is. It makes no difference whether the person impersonated is real or imaginary. The punishment extends to five years, a fine, or both.[14] A message from someone who falsely claims to be a bank officer therefore raises a question of personation, but a fake profile does not by itself prove completed cheating. The

[11] BNS § 337 & Explanation.
[12] BNS § 338; *see also* BNS § 2(31) (defining "valuable security").
[13] BNS § 340(2).
[14] BNS § 319.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

prosecution must still identify the deception and the legally required inducement. Likewise, an unsolicited message is not forgery unless a false record within Section 335 can be pointed to.

The Information Technology Act, 2000 (IT Act) continues to matter. Section 66C punishes the fraudulent or dishonest use of another person's electronic signature, password or other unique identification feature, and Section 66D punishes cheating by personation through a communication device or computer resource. Each carries imprisonment up to three years and a fine of up to one lakh rupees.[15] These provisions do not displace the BNS whenever a computer is involved, and charges should not be piled up mechanically. The ingredients of each offence, and the relationship between the special statute and the general code, have to be considered on the facts proved.

An example shows how the offences interact. Misuse of another person's login may raise an identity-misuse issue. A fabricated authorisation created through that access may separately raise forgery. A payment obtained by deception may raise cheating. How these relate to one another is a matter for analysis of proved conduct, not for the loose label of "online fraud."

G. Electronic evidence and attribution

Liability under the BNS and admissibility of evidence are separate inquiries. A forged record may be punishable, but the prosecution must still prove the record, the accused's connection with it and the mental element through admissible evidence. Sections 61 to 63 of the Bharatiya Sakshya Adhiniyam, 2023 (BSA) recognise electronic records and govern proof of their contents, and Section 63 sets conditions for computer output together with a certificate framework for records tendered under it.[16] A screenshot, standing alone, does not establish authenticity, authorship or the truth of what it shows.

A sound investigation preserves the original files, available metadata, transaction records and communications, together with a documented account of how they were collected and handled.[17] Forensic examination can help to detect alteration or to compare versions. A hash value can support verification of a file's integrity, but it cannot identify who created the file or show dishonest intention.[18]

---

[15] IT Act §§ 66C–66D; *see also* IT Act § 81.

[16] Bharatiya Sakshya Adhiniyam, 2023, No. 47 of 2023, §§ 61–63 (India) [hereinafter BSA].

[17] *See Anvar P.V. v. P.K. Basheer*, (2014) 10 SCC 473, ¶ 16 (India) (describing electronic records as "more susceptible to tampering, alteration, transposition, excision, etc."); KAREN KENT ET AL., NAT'L INST. OF STANDARDS & TECH., GUIDE TO INTEGRATING FORENSIC TECHNIQUES INTO INCIDENT RESPONSE, Special Publication 800-86, §§ 3.1.2, 4.2.3 (2006), https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-86.pdf (on a clearly defined chain of custody, with a log of each person who held the evidence and the actions taken, and on preserving file times).

[18] Kent et al., *supra* note 17, §§ 3.1.2, 4.2.2 (a message digest identifies the data and changes if a single bit changes, so comparing digests verifies that a copy matches the original); *see also* BSA sch., pts. A–B (certificate to state the

Attribution is hardest where devices or accounts are shared or compromised. That an account is registered in a person's name is relevant information, but it does not prove the person's involvement. The maker, the knowing user and the recipient of a record should each be analysed separately.

H. Strengths and weaknesses of the present scheme

The express treatment of electronic records is a real strength of the BNS. It removes any artificial assumption that documentary protection applies only to paper, and its separate provisions for making, forging and knowingly using records allow attention to the different roles played in a digital transaction.

The main difficulty is usually evidentiary rather than the absence of an offence. Files are copied, forwarded and altered by several hands. Courts should therefore require a clear account of the alleged deception, the false record, the maker or user, and the evidence of intention. Technical complexity must not lower the standard of proof. The likely outcome is continued reliance on the settled IPC-era principles, now applied to a new generation of records.

III. Statutory Framework

Table 1 sets out the principal offences discussed above, their IPC predecessors and their maximum punishments.[19]

Offence	BNS provision	IPC provision	Maximum punishment
Cheating	Section 318	Sections 415, 417, 418, 420	Up to 3 years, fine or both (s. 318(2)); up to 5 years, fine or both (s. 318(3)); up to 7 years and fine (s. 318(4))
Cheating by personation	Section 319	Sections 416, 419	Up to 5 years, fine or both
Forgery	Section 336	Sections 463, 465, 468, 469	Up to 2 years, fine or both (s. 336(2)); up to 7 years and fine if for cheating (s. 336(3)); up to 3 years and fine if to harm reputation (s. 336(4))
Forged court or public record	Section 337	Section 466	Up to 7 years and fine
Forged valuable security or will	Section 338	Section 467	Imprisonment for life, or up to 10 years, and fine

hash value of the record and the algorithm used).

[19] For the IPC correspondence, *see* National Crime Records Bureau, Ministry of Home Affairs, *Corresponding Section Table of Bharatiya Nyaya Sanhita 2023 (BNS)*, https://www.ncrb.mha.gov.in/uploads/SankalanPortal/SectionTableBNS.html.

Offence	BNS provision	IPC provision	Maximum punishment
Using a forged record as genuine	Section 340(2)	Section 471	Punished as if the user had forged the record

Table 1: Principal offences on cheating and forgery, their IPC counterparts and maximum punishments

Two points of reading deserve emphasis. A provision that raises punishment, such as Section 318(4) or Section 338, applies only when its own ingredients are proved. And the choice between provisions depends on the legal character of the document and the purpose of the accused, not on the technology used to produce it.

IV. JUDICIAL DECISIONS

A. *Hridaya Ranjan Prasad Verma v. State of Bihar*

In this decision the Supreme Court addressed the borderline between a contractual default and criminal deception. It described the distinction as a fine one that depends on the intention of the accused at the time of the inducement. That intention may be inferred from later conduct, but later conduct is not the only test. Unless a fraudulent or dishonest intention is shown right at the start of the transaction, a failure to keep a promise remains a civil matter.[20] The ruling governs the Section 318 analysis in online commerce as much as in offline dealings, since the first question is still what the accused intended when the counterparty was induced to act.

B. *Mohammed Ibrahim v. State of Bihar*

The question was whether executing sale deeds for property that did not belong to the executant amounted to forgery. The Supreme Court drew a basic distinction between a person who executes a deed claiming that the property is his own and a person who executes a deed by impersonating the owner or by falsely claiming authority to act for the owner. Where what is executed is not a false document, there is no forgery.[21] The decision supplies the legal basis for the distinction between authenticity and truth discussed in Part II, and it explains why a bare false claim of title does not by itself amount to forgery.

C. *Sheila Sebastian v. R. Jawaharaj*

The complainant alleged that the first accused, with the help of an impostor who posed as the owner of a property, had a power of attorney created in his favour and then used it to execute a mortgage deed. The trial court and the first appellate court convicted him and a second accused, who was charged with abetment, but the High Court acquitted both, and the Supreme Court upheld that acquittal. It held that forgery cannot be charged against a person who did not make

[20] *Hridaya Ranjan Prasad Verma*, *supra* note 4, ¶ 15.
[21] *Mohammed Ibrahim*, *supra* note 7.

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

the false document, and that the record contained no finding that either accused had made one. It was the impostor who could be said to have done so.[22] For digital cases the lesson is plain. Benefiting from a forged record, or being connected with its use, does not prove that the beneficiary made it. Other bases of liability, such as knowing use under Section 340(2), have to be established on their own ingredients.

D. *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*

This decision was given under Section 65B of the Indian Evidence Act, 1872, whose subject matter is now dealt with in Section 63 of the BSA. A three-judge bench held that the certificate required by Section 65B(4) is a condition precedent to the admissibility of electronic records tendered as secondary evidence. It added that the certificate is unnecessary where the original device or document is itself produced, and that a court can direct production of the certificate from the person who is required to give it.[23] For prosecutions based on fabricated files, the ruling is a reminder that a printout or screenshot cannot safely be tendered without the supporting certificate, and that the certificate should be secured early.

V. SUGGESTIONS

The following suggestions follow from the analysis above.

First, charges should be framed by mapping the facts to the ingredients of the offence. For each count, the prosecution should be able to state who was deceived, what the person was induced to do, which record is alleged to be false, who made or used it and what evidence shows intention. Technical complexity should not be allowed to lower the standard of proof.

Second, investigators need to separate ordinary commercial failure from fraud, and unauthorised falsification from legitimate editing. Early verification with the apparent issuer of a certificate or authorisation can show quickly whether the record was genuinely issued and whether it was materially altered.[24]

Third, evidence handling should be treated as part of the offence analysis from the first day. Original files, metadata, transaction records and communications should be preserved with a documented chain of handling, and the certificate required under Section 63 of the BSA should be obtained early rather than at the trial stage.

---

[22] *Sheila Sebastian v. R. Jawaharaj*, (2018) 7 SCC 581 (India).

[23] *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal*, (2020) 7 SCC 1 (India); *see also* Indian Evidence Act, 1872, No. 1 of 1872, § 65B (India) (repealed).

[24] *See* PRESS INFORMATION BUREAU, GOVERNMENT OF INDIA, *National Academic Depository (NAD)* (July 7, 2026), https://www.pib.gov.in/FactsheetDetails.aspx?Id=150733&reg=48&lang=1 (authorised organisations can verify academic records directly through NAD/DigiLocker; employers are among the verifying entities).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]

Fourth, institutions should strengthen their verification of electronically submitted documents and of changes to payment instructions. Clear audit trails and timely preservation of records would assist both prosecution and defence.[25] These measures supplement criminal enforcement and do not shift responsibility for fraud onto its victims.

Fifth, the BNS and the IT Act should not be stacked mechanically. Where both could apply, the charging authority should identify why each provision is needed and how the ingredients of each are met by the proved conduct.

Sixth, legal education and police training should present cheating and forgery as connected but distinct offences.[26] Describing every false online statement as forgery, or every failed digital transaction as cheating, obscures the statutory requirements and risks unfair criminalisation.

VI. Conclusion

Cheating and forgery protect related but different aspects of trust. Section 318 addresses deception and its legally specified inducement and consequences. Sections 335 and 336 address false documents or electronic records made with a prohibited intention, and Section 340 reaches the knowing fraudulent or dishonest use of such records as genuine. The BNS expressly accommodates electronic and digital records, so these offences can apply to fabricated certificates, altered electronic documents and false authorisations once their ingredients are established. The IT Act adds specific provisions on identity misuse and computer-assisted personation, and the BSA supplies the framework of proof.

The decisive question is not whether a document is digital. It is who created or used it, what made it legally false, what intention accompanied the conduct, and what deception or harm followed. Careful statutory analysis and reliable electronic evidence are what make digital enforcement both effective and fair, and the settled principles of the Supreme Court remain the guide for applying the new code to new technology.

*****

[25] *Cf.* Indian Computer Emergency Response Team, *Directions under Sub-section (6) of Section 70B of the Information Technology Act, 2000*, No. 20(3)/2022-CERT-In, direction (iv) (Apr. 28, 2022), https://www.cert-in.org.in/PDF/CERT-In_Directions_70B_28.04.2022.pdf (requiring service providers, intermediaries, data centres, body corporate and Government organisations to maintain logs of their ICT systems securely for a rolling period of 180 days).

[26] *Cf.* Press Information Bureau, Ministry of Home Affairs, *Assistance to States to Tackle Cyber Incidents* (Mar. 24, 2026), https://www.pib.gov.in/PressReleasePage.aspx?PRID=2244504&reg=48&lang=2 (describing the CyTrain online platform for building the capacity of police and judicial officers in cybercrime investigation, forensics and prosecution).

© 2026. International Journal of Law Management & Humanities [ISSN 2581-5369]