International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

Cyber frauds and scams

Sunaina Mondal
Symbiosis International (Deemed) University Maharashtra

Abstract - This fast growth in digital technologies has greatly contributed to the higher rate and level of cyber frauds and scams that have serious legal and regulatory challenges in India. The paper discusses the legal system that governs cyber fraud and specifically the liability to criminal liability through impersonation and electronic deception, the scope of liability of the financial institutions and middlemen and the resultant effect of such frauds to the fundamental right to privacy in Article 21 of the Constitution.

The paper estimates major legislative provisions in Information Technology Act, 2000, the Bharatiya Nyaya Sanhita, 2023, and the Digital Personal Data Protection Act, 2023, as well as, the applicable RBI direction and case laws. It assesses the liability to criminal acts committed by acts like phishing, and identity theft and impersonation online, and examines when banks and other intermediaries might be regarded liable to negligence or lack of reasonable care in line of duty. The paper also evaluates the overlap of cyber fraud and informational privacy, especially in the post-constitutionality privacy as a constitutional right.

By using the doctrinal analysis the paper will reach a conclusion that cyber fraud through impersonation is a cognizable offence in the Indian law and is liable by concurrent action through various statutes. It also concludes that there is a large amount of responsibility placed on financial institutions in preventing fraud and may lose statutory protection in situations where there is lack of due diligence. Lastly, the paper confirms that unauthorized gathering and misappropriation of personal information in instances of cyber fraud qualify as infringing on the right to privacy, and action can be taken against it both under the constitutional and statutory provisions.

1. LEGAL ISSUE(S) IDENTIFICATION

Legal Issue I

Was the impersonation and miscommunication on an electronic basis to achieve monetary gain a cognizable offence under the Information Technology Act, 2000 and the Bharatiya Nyaya Sanhita, 2023 and, in that case, what was the kind and scope of criminal responsibility?

Legal Issue II

Can a financial institution or financial intermediary, under Indian law, be held vicariously or separately liable in respect of damages sustained by a victim of cyber fraud as the result of failure to perform due diligence, ineffective security practises or by way of twice-me-too (facilitation) loss of transaction of a fraudulent act?

Legal Issue III

Does the act of collecting, exploiting, and unauthorisedly using personal information of individuals by cyber fraudsters amount to contravention of right over privacy being one of the fundamental rights in Article 21 of the Constitution of India and what are the legislative provisions on the same?

2. LEGAL FRAMEWORK / RULES

2.1 Statutory Provisions

A. The Information technology act, 2000 (IT Act).

The most significant law that regulates the cyber offences in India is the Information Technology Act, 2000. These are the applicable provisions:

- Section 43 - Penalty and compensation in respect of damage to computer, computer system, etc.: The sections offer civil liability in case of unauthorised access, downloading, introduction of computer contaminants, and disruption of computer systems.
- Section 43A - Failure to protect funds: Liability on body corporates working with sensitive personal information because of careless performance of reasonable security practises.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

- Section 66R - Computer related offences: Criminalises dishonesty acts or other acts involving fraudulent intention under Section 43 which is liable to imprisonment up to three years or fine up to five lakh rupees or any combination thereof.
- Section 66C -Identity theft:Breaks a fraudulent or dishonest use of the electronic signature, password, or other distinct identification feature of some other individual; imprisonment with a fine of one lakh rupees or less.
- Section 66D - Cheating by personation by the help of computer resource: Dertermines that a cheating by impersonation through communication devices or computer resource will be an offence that will be detained up to three years and fine up to one lakh rupee.
- Section 72-Breach of confidentiality and privacy- Penalises any individual breaking the law by bypassing any electronic record, book, register, correspondence, information, document, or other material access to an electronic record with the exception of access for a reason that has been stated in writing.
- Section 79 - Exemption of intermediary in some cases: Is a safe harbour to intermediaries upon the condition that due diligence measures are followed such as the necessity of knowing of the unlawful acts and the failure to promptly eradicate or block access.

B. "Bharatiya Nyaya Sanhita, 2023 (BNS)"

Replacing the Indian Penal Code, 1860, the Bharatiya Nyaya Sanhita, 2023 bundles renewed general criminal law over cyber frauds:

- Section 318 - cheating: By cheating, this section defines cheating as any act of inducting one person to send any property or to modify or to undermine any document with unethical intentions which is punishable in accordance with Section 318(2) and 318(4) depending on the extent of damages.
- Section 319 - Cheating by personation: According to Section 319, it punishes the act of cheating through impersonation of another person or knowingly replacing another person.
- Section 336 - Forgery: Defines and punishes the issue of creating a false document or false electronic record by intentionally targeting to damage or injure.
- Section 340 - Forgery with intent to cheat: The section gives a better penalty in case of forgery whose purpose is to cheat.

C. The "Digital personal data protection Act, 2023" (DPDPA).

The Digital Personal Data Protection Act of 2023 regulates the manipulation of digital personal data, as well as the formation of an obligation to data fiduciary:

- Section 4 - Reasons why the personal data should be processed: Requires that the personal data can only be a lawful one that has to be processed either on the basis of consent or on a legitimate use that are set out in the statute.
- Section 8 - General obligations of data fiduciary: Provides that data fiduciaries must deploy suitable technical and organisational controls to make sure that compliance and data breach occurrences are avoided.
- Section 10 - Additional obligations of significant data fiduciary: Consists of additional obligations on significant data fiduciary, such as data protection impact assessment.
- Section 17 - Rights of data principals: Grants rights or data principals like the right to information, amendment, deletion as well as re-compensation of grievances.

D. Rules on Information Technology (Reasonable Security Practises and Procedures and Sensitive Personal data or information) 2011.

These Rules are framed and read together with Section 87 alongside Section 43A of the IT Act, these Rules stipulate the reasonable Rationale of security practises and procedures to be employed by body corporates to manage sensitive personal data.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

E. Guidelines of Reserve Bank of India

Master direction by the RBI on security measures controlling digital payment controls (2021) and the customer liability circular on electronic banking transactions without authorisation regulating the actions of regulated entities (DBR.No.Leg.BC.78/09.07.005/2017-2018) places liabilities on the regulated entities to protect the customers and the provision of chargebacks.

2.2 Constitutional Provisions

- Under the Constitution of India, article 21 - Protection of life and personal liberty, the protection of life is further explained as in the case of Justice K.S. Puttaswamy (Retd.). The right to privacy (Anr. v. Union of India & Ors. 2017) is an inherent right of the right to life and personal liberty. This contains the right to informational privacy and security against data surpasses and data misuse.
- Article 19(1)(g) - Right to practise any profession, or to practise any occupation, trade or business: Cyber fraud in direct relation to the right is a direct attack on the right when it is focused on commercial institutions or individuals operating their business online.

2.3 Contingent Judicial Precedents

- Justice K.S. Puttaswamy (Retd.) Anr. v. Union of India & Ors., (2017) 10 SCC 1 - Article 21 of the Constitution of India provides a fundamental right to privacy, which is unanimously provided by a 9 persons bench of the Supreme Court[1].
- Shreya Singhal v. Union of India, (2015) 5 SCC 1 - The Supreme Court also declared the constitutionality of Section 79 of the IT Act by interpreting down Section 66A. Explained the intermediary liability position and need of actual knowledge to have a claim[2].
- Shri Ram Prasad Gupta v. Criminal Appeal in a case involving a cyber-related fraud - Courts have always stated that any electronic data of electronic communication of phishing is admissible and that impersonation through electronic means will meet the requirements of Section 66D of the IT Act.
- State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601 - Again repeated determination of the admissibility of electronic records and electronic communications in criminal cases[3].

2.4 Legal Acts and the Canon Law

- Doctrine of vicarious liability: The principal can be held responsible of the delinquent conduct of an agent or employee performed during the employment or other activity that has been authorised. Used in the presence of middlemen striving to make fraudulent deals.
- Doctrine of strict liability: Under Section 43 A of the IT Act, such doctrine applies to the relevant data fiduciaries, and where the sensitive personal data is wrongly handled due to negligence, it will lead to a wrongful loss or gain.
- Ital of mens rea: IT Act and the BNS all present cyber fraud offences demand the demonstration of an unscrupulous or fraudulent intendment, which is in line with general criminal law.

3. ANALYSIS / APPLICATION OF LAW

3.1 Analysis of Legal Issue I: Criminal Liability of Impersonation and Electronic Deception.

The form of cyber fraud is usually phishing, vishing, smishing, or social engineering attacks, when the fraudster impersonates a person or an entity the victim has faith in, lures the victim into providing credentials or money, and, as a result, commits a wrongful loss. The legal issue is whether this kind of behaviour will meet the definition criteria of the applicable criminal statutes.

[1] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1 (India)
[2] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India)
[3] State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601 (India)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

- **Use of Section 66D, IT Act:** Section 66D is specifically aimed at cheating via personation using computer resources or communication equipment. The provision needs

(i) the use of a computer resource or communication device

(ii) the use of personation;

(iii) the use of a dishonest or fraudulent intent. The phishing fraudsters who send messages in the form of a bank, a governmental department, or a trusted person fulfil all three requirements. Fraudulent use of a computer resource consists of the use of spoofed email addresses, cloned websites, or spoofed SMS messages. The pretence of an authoritative being occurs. Considering the nature of the scheme, the intent to defraud the victim into parting with money or credentials is obvious. Section 66D criminal liability is, therefore, evidently drawn.

- **Section 66C, IT Act applied:** Section 66C also applies whereby the fraudster uses digital identity, electronic signature, or other credentials of the victim to engage in unauthorised transactions. It does not involve actual loss of money and the fraudulent or dishonest utilisation of the unique identification feature of another individual is the crime. It is especially important regarding SIM-swapping and account takeover scams and OTPs abuse.

- **Application of BNS Provision:** The BNS 318 in Section 318 outlines the definition of cheating in a broad scope which includes cheating a person hence deceiving the person and thus serving as a means to coerce that person in receiving property. Impersonation through the internet is a direct form of deception. The transfer of money in the form of falsely caused digital transactions amounts to delivery of property. Personation is another area that is captured in Section 319 BNS. These clauses are applicable alongside the IT Act because the IT Act does not traversate the application of any other law (Section 81, IT Act read as a non-obstante clause).

- **Competing Interpretations:** There is an alternative interpretation that can be put forward involving competing interpretation in that Section 66D is based on the understanding of active personation, and this might be absent in the case of automated phishing systems that do not involve a human operator in personal contact with the victim. Nonetheless, it is a flimsy argument that the application of any computer resource by fraudulent intent suffices, and that direct human-to-human contact is not absent since the absence of said contact does not preclude the imposition of liability (see also similar logic in State of Maharashtra v. Dr. Praful B. Desai)[4]. The dishonest act required is the programming of the fraudulent system done by the perpetrator.

This can therefore be concluded to imply that digital impersonation with the intent of earning money is a cognizable offence qualifying concurring liability under Section 66C and Section 66D of the IT Act and Sections 318, 319 and 336/340 of the BNS provided the requisite elements of each article are proved.

3.2 Analysis of Legal Issue II: Liability of Financial Institutions and Intermediaries

- **Section 43A, IT Act – Negligence Standard:** Section 43A imposes liability on a body corporate which possesses, deals with, or handles sensitive personal data in a computer resource owned, controlled, or operated by it, and is negligent in implementing and maintaining reasonable security practices and procedures, thereby causing wrongful loss or gain to any person. Banks and payment intermediaries, as body corporates handling sensitive financial data, fall squarely within this provision. Where a bank fails to implement two-factor authentication, does not flag suspicious transaction patterns, or neglects to issue real-time alerts, it may be held liable under Section 43A.
- **RBI Framework and Customer Liability:** The RBI circular on customer liability significantly limits the liability of customers in unauthorised electronic banking transactions when the deficiency lies with the bank. Zero liability is imposed on customers where the fraud results from bank negligence or a third-party breach without customer fault. This regulatory framework effectively transfers liability to financial institutions in cases of systemic failure.
- **Section 79, IT Act – Intermediary Safe Harbour and Its Limits:** Section 79 provides that intermediaries shall not be liable for third-party information, data, or communications links made available by them if they have no role in initiating

[4] State of Maharashtra v. Dr. Praful B. Desai, (2003) 4 SCC 601 (India)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

the transmission, do not select the receiver, and do not modify the information. However, the safe harbour is lost where the intermediary

(i) has actual knowledge of the unlawful act and fails to expeditiously remove or disable access, or

(ii) fails to comply with due diligence guidelines. As affirmed in Shreya Singhal v. Union of India (2015)[5], the intermediary's passive role is protected only so long as it does not have actual knowledge. Payment aggregators and e-commerce platforms that continue to host fraudulent sellers after receiving complaints may lose this protection.

- **Doctrine of Vicarious Liability:** Where a bank employee or agent facilitates a cyber fraud through negligence or complicity, the institution may also face vicarious liability under general agency law principles. Courts have recognised that financial institutions owe a duty of care to their customers that extends to the conduct of their agents.

The analytical conclusion on this issue is that financial institutions and intermediaries are exposed to independent liability under Section 43A of the IT Act for negligence, and lose safe harbour protection under Section 79 upon acquisition of actual knowledge of ongoing fraud. The RBI regulatory framework additionally creates a presumption of bank liability in unauthorised transaction cases absent customer negligence.

3.3 Legal Issue III : Data Privacy and Cyber Fraud, Article 21.

- **Fundamental Right of Right to Privacy:** Justice K.S. Puttaswamy (Retd.) v. Union of India (2017)[6] authoritatively stated that the right to privacy is a fundamental right that derives out of Article 21. Including the explicit concurring a view by Justice D.Y. Chandrachud, it was established that informational privacy, i.e. the right to information over oneself are provided. This informational privacy is directly infringed by the cyber fraudsters who collect personal data on a phishing attack, malware or data breach.

- **Legislative Framework -** DPDPA, 2023: DPDPA, 2023 is an act that realises the constitutional right to privacy on the digital platform. Section 4 does not allow processing personal data without consent or without a legitimate use. Section 8 commits affirmative responsibilities to the data fiduciaries to avoid unauthorised access. Section 17 grants the statutory power of the data principals to seek erasure and grievance redressal. A direct statutory violation is carried out when cyber fraudsters obtain and process personal data under conditions other than legal ones. More importantly, in case data fiduciary can be involved in avoidable breach as a result of insufficient security measures, the Data Protection Board can impose liability under Section 25.
- **Interaction of Article 21 and Statutory Remedies:** An important analytical question would be whether statutory remedies, together with Article 21 against the State to a direct failure to provide informational privacy, are available to a victim of cyber fraud. The Puttaswamy ruling suggests that the State activity or inactivity that allows private data breaches can be prone to constitutional responsibility. But the extrapolation of basic rights down to common law litigants (individual fraudsters), is a jurisdictional dilemma. The closer solution is the framework of the DPDPA and IT act.
- **Adequacy of Statutory Protection:** It can be said that current statutory provisions, i.e. the IT Act, DPDPA, and RBI directions give a satisfactory protection of informational privacy and do not necessitate constitutional adjudication in any instance. Such an argument is justified in practical terms: the Data Protection Board established by the DPDPA is the relevant place where matters of data privacy can be raised. However, the constitutional underlining is still significant as an interpretive authority and also as a means of challenge in cases where frameworks of statutes fail.

This analysis shows that such some cyber frauds that entail the use of data amount to an infringement of the right to privacy against Article 21, and that the statutory law in this matter is detailed through the DPDPA and IT Act. The remedies of the victim work both on the constitutional and statutory levels.

[5] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India)
[6] Justice K.S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors., (2017) 10 SCC 1 (India)

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 15 Issue 04 , April - 2026

4. CONCLUSIONS / FINDINGS

4.1 On Legal Issue I: Criminal Liability on Cyber Fraud and Impersonation is as follows.

There is an ultimate finding that impersonation and fraudulent communication via electronics to gain financial benefit is a cognizant crime in the law of India. The information technology act, 2000 attracts concurrent criminal liability for Section 66C (identity theft) and Section 66D (cheating by personation) and the Bharatiya Nyaya Sanhita, 2023, attracts concurrent criminal liability in Sections 318, 319 and 336. These are the key factors: The presence of an unscrupulous or scamming motive, utilisation of a computer device, and the act of personation, all that the habitual behaviour of cybercriminals gives. Smartphone presence of the culprit is not a defence.

4.2 On Legal Issue II: Finnancial Intermediaries and Financial Institutions Liability.

It is definitively held that financial entities and digital intermediaries could not be relieved of their liability due to the fact that the person who caused the loss by committing a third-party fraud is merely a proximate cause of the loss. On negligent security practises in Section 43A of the IT Act, body corporates that deal with sensitive personal data have an independent liability of wrongful loss. Under Section 79 the protection of safe harbour under intermediate loses when the intermediaries have actual knowledge of an on-going fraudulent activity. RBI regulatory guidelines also provide a guideline of shifted responsibility to banks when the case is of unauthorised transactions that cannot be blamed on the negligence of the customers. In other instances of vicarious liability, the general agency principles may also be relevant in the case of complicity of employees or even agents.

4.3 Data privacy On Legal Issue III: Data privacy and Article 21.

It is conclusively held that the personal data collection and exploitation by cyber fraudsters with no authorisation is a contravention to the right to privacy as a fundamental right in Article 21 of the Constitution of India, as adopted by the Supreme Court of Justice in Justice K.S. Puttaswamy (Retd.). v. Union of India (2017). The main legislative protection mechanisms given by the “Digital personal data protection Act, 2023” and the Information Technology Act, 2000 hereby enforce payment and duty against data fiduciaries and methods of enforcement, such as the Data Protection Board. The victims still have both constitutional and statutory remedies.

5. BIBLIOGRAPHY

[1] **Statutes and Legislation**

- “Bharatiya Nyaya Sanhita, 2023”, No. 45 of 2023 (India).
- “Digital personal data protection Act, 2023”, No. 22 of 2023 (India).
- “Information Technology Act, 2000”, No. 21 of 2000 (India).
- “Information Technology (Reasonable Security Practices and Procedures and Sensitive” Personal Data or Information) Rules, 2011, G.S.R. 313(E) (India).

[2] **Constitutional Provisions**

- Constitution of India, 1950, art. 19(1)(g), 21.

[3] **Regulatory Directions**

- Reserve Bank of India. (2017, July 6). Customer protection – Limiting liability of customers in unauthorised electronic banking transactions [Circular DBR.No.Leg.BC.78/09.07.005/2017-18]. Reserve Bank of India.
- Reserve Bank of India. (2021, February 18). Master directions on digital payment security controls [RBI/DPSS/2021-22/82]. Reserve Bank of India.

[4] **Secondary Sources**

- Nappinai, N. S. (2020). Cyber law simplified (3rd ed.). LexisNexis India.
- Prasad, A. (2022). Cyber crime and information technology law. Universal Law Publishing.
- Sharma, V. (2018). Cyber laws in India: A commentary on the Information Technology Act (4th ed.). Snow White Publications.