Ready Reckoner

Highlighting the Use of Technology in New Criminal Act

" Digitizing Justice, Elevating Credibility!"

Use of Technology is now envisaged in all stages (from e - FIR to investigation to submission of documents to trials). Further, Compulsory Forensic examination in all cases where offence attracts punishment of seven or more years has been envisaged. It has been provided that in offences prescribing imprisonment for 7 years or more, police officer shall cause forensics expert to visit the crime scene to collect forensic evidence. States may from such date, as may be notified by them, as early as possible but not later than 5 years, shall make it compulsory.

Some of the other highlights are as under:

a) A new definition of electronic communication 'for use of technology in investigation, trial and court proceedings and service of summons, notices, etc. has been introduced.

b) The definition of 'Documents' has been expanded to include an electronic or digital record on emails, server logs, documents on computers, laptop or smartphone, messages, websites, cloud locational evidence and voice mail messages stored on digital devices.

c) The definition of 'evidence' has been expanded to any information given electronically. This will permit appearance of witnesses, accused, experts and victims through electronic means. This will ease the process of trial, prevent delays in transporting accused from prisons to courts, and also help in preserving the trial process for future reference that may be necessitated during challenge in higher courts.

d) In the definition of primary document (Sec 57, BSA), new explanations have been added to cover:

   (i) If an electronic or digital record which is created or stored, and if such storage occurs simultaneously or sequentially in multiple files, each such file is an original.

   (ii) If an electronic or digital record is produced from proper custody, it is sufficient to prove its contents unless it is disputed.

   (iii) If a video recording is simultaneously stored in electronic form and transmitted or broadcast to another, each of the stored recordings is an original.

   (iv) If an electronic or digital record is stored in multiple in storage spaces computer resource, each such automated storage, including temporary files, is an original.

e) Scope of secondary evidence has been expanded. Now in addition to certified copies, copies made from original by mechanical processes, copies made from or compared with the original, counterparts of documents as against the parties who did not execute them and oral accounts of the contents of a document given by some person who has himself seen it, are included.

f) It has been permitted that accused (in custody) may be examined by a Magistrate through electronic means i.e. Video Conferencing / VC facility available in the police station, court, prison or any other such place notified by the State Government. It has been provided that if the accused has been examined through VC, his signature on the statement shall be taken within 72 hours.

g) A provision has been made wherein the Magistrate may order specimen or sample without the person being arrested. Further there is no existing provision in CrPC for taking finger impression or voice sample which has been provided for in BNSS.

Important sections of BNS, BNSS & BSA for a quick reference while dealing with crimes for police officers, in which technological methods were used. Also, it can assist the police officers in attributing the various offences falling under above Acts. In the same way, it can assist in the procedural aspects of cyber evidence collection from the various formal cyber sources in a manner that is admissible to the judiciary.

Bhartiya Nyaya Sanhita, 2023- **Highlighting the use of technology in crimes**

Bhartiya Nyaya Sanhita, 2023, emerges as a trailblazer in acknowledging and harnessing the power of technology in the realm of crime.

BNS defines the new trends of committing crimes by using electronic means/ communication.

BNS provide a comprehensive legal framework that adapts to the digital age, the legislation seeks not only to punish wrongdoers but also to protect the integrity of the justice system in an era dominated by technological advancements.

BNS	
	Section -2(8) Document - includes electronic and digital record, intended to be used, or which may be used, as evidence of that matter
	Section -152 Act endangering sovereignty, unity, and integrity of India Whoever, purposely or knowingly, by words, either spoken or written, or by signs, or by visible representation, or **by electronic communication** or by use of financial mean, or otherwise, excites or attempts to excite, secession or armed rebellion or subversive activities, or encourages feelings of separatist activities or endangers sovereignty or unity and integrity of India;
	Section-196 Promoting enmity between different groups on grounds of religion, race, place of birth, residence, language, etc., and doing acts prejudicial to maintenance of harmony.- Included or through electronic communication
	Section-197 Imputations, assertions prejudicial to national integration. Included or through electronic communication or

	otherwise
	Section-206 Absconding to avoid service of summons or other proceeding. Included or an electronic record.
	Section-294 Sale, etc., of obscene books, etc. including display of any content in electronic form
	Section-299 Deliberate and malicious acts, intended to outrage religious feelings of any class by insulting its religion or religious beliefs. Included or through electronic means.
	Section-308 Extortion. (e) threatens by sending a message through an electronic device to give him money, committed extortion.
	Section-335 Making a false document. New word “Electronic Document)
	Section-336 Forgery. Included or electronic record forged shall be used for the purpose of cheating,
	Section-337 Forgery of record of Court or of public register, etc Included Whoever forges a document or an electronic record, purporting to be a record or proceeding of or in a Court or an identity document issued by Government
	Section-353 Statements conducing to public mischief Whoever makes, publishes or circulates any statement, false information, rumour, or report, including through electronic means.

Bhartiya Nagrik Suraksha Sanhita 2023-

Integrating Technology Across the Legal Spectrum

The BNSS has introduced the use of technology at all stages, from Cime scene visit to Investigation till Trial. This is going to be a game changer in terms of speedy trial and introduces transparency in investigation. The inclusion of technology and forensics in investigation is a significant move geared towards modernizing the criminal justice system and harnessing the strength of modern scientific technologies. This will also ensure greater accountability in police investigation, improve quality of evidence and protect the rights of both the accused and victims.

BNSS
Sec.2(1) a (a) "audio-video electronic means" shall include use of any communication device for the purposes of video conferencing, recording of processes of identification, search and seizure or evidence, transmission of electronic communication and for such other purposes and by such other means as the State Government may, by rules provide (i) "electronic communication" means the communication of any written, verbal, pictorial information or video content transmitted or transferred (whether from one person to another or from one device to another or from a person to a device or from a device to a person) by means of an electronic device including a telephone, mobile phone, or other wireless telecommunication device, or a computer, or audio-video player or camera or any other electronic device or electronic form as may be specified by notification, by the Central Government;

	Section-54 Identification of person arrested Included the identification process shall be recorded by any audio-video electronic means.
	Section-63 Form of summons. (ii) in an encrypted or any other form of electronic communication and shall bear the image of the seal of the Court or digital signature
	Section-64 Summons how served Included may also be served by electronic communication in such form and in such manner, as the State Government may, by rules, provide.
	Section-70 Proof of service in such cases and when serving officer not present (3) All summons served through electronic communication under sections 64 to 71 (both inclusive) shall be considered as duly served and a copy of such summons shall be attested and kept as a proof of service of summons.
	Section-71 Service of summons on witness Included a Court issuing a summons to a witness may, in addition to and simultaneously with the issue of such summons, direct a copy of the summons to be served by electronic communication
	Section-94 Summons to produce document or other thing 1) Whenever any Court or any officer in charge of a police station considers that the production of any document, electronic communication, including communication devices, which is likely to contain digital evidence or other thing is necessary or desirable for the purposes of any investigation, inquiry, trial or other proceeding under this Sanhita
	Section-105 Recording of search and seizure through audio video electronic means. Included under this Chapter or under section 185, including preparation of the list of all things seized in the course of such search and seizure and signing of such list by witnesses, shall be recorded through any audio-video electronic means preferably mobile phone and the police officer shall without delay forward such recording to the District Magistrate, Sub-divisional Magistrate or Judicial Magistrate of the first class
	Section-173 Information in cognizable cases. Included or by electronic communication & (ii) by electronic communication, it shall be taken on record by him on being signed within three days by the person giving it
	Section-176 Procedure for investigation Included such statement may also be recorded through any audio-video electronic means including mobile phone. And also included (1) cause the forensic expert to visit

	the crime scene to collect forensic evidence in the offence and also cause videography of the process on mobile phone or any other electronic device:
	Section-183 Recording of confessions and statements Included or a special educator, shall be recorded through audio-video electronic means preferably by mobile phone;
	Section-185 Search by police officer. Included under this section shall be recorded through audio-video electronic means preferably by mobile phone
	Section-187 Procedure when investigation cannot be completed in twenty-four hours Included that the Magistrate may extend further detention in judicial custody on production of the accused either in person or through the audio-video electronic means and also included in explanation.
	Section-193 Report of police officer on completion of investigation, including through electronic communication to a Magistrate empowered to take cognizance of the offence on a police report, (h) whether the report of medical examination of the woman has been attached where investigation relates to an offence under sections 64, 65, 66, 67, 68, 70 or section 71 of the Bharatiya Nyaya Sanhita, 2023; (i) the sequence of custody in case of electronic device (ii) the police officer shall, within a period of ninety days, inform the progress of the investigation by any means including through electronic communication to the informant or the victim (8) Included Provided that supply of report and other documents by electronic communication shall be considered as duly served.
	Section-202 Offences committed by means of electronic communications, letters, etc 202. (1) Any offence which includes cheating, may, if the deception is practised by means of electronic communications or letters or telecommunication messages, be inquired into or tried by any Court within whose local jurisdiction such electronic communications or letters or messages were sent or were received;
	Section-209 Receipt of evidence relating to offences committed outside India included if it thinks fit, direct that copies of depositions made or exhibits produced, either in physical form or in electronic form, before a judicial officer,
	Section-210 Cognizance of offences by Magistrate b) upon a police report (submitted in any mode including electronic mode) of such facts;

	Section-227 Issue of process. Included Provided that summons or warrants may also be issued through electronic means
	Section-230 Supply to accused of copy of police report and other documents included may furnish the copies through electronic means or direct that he will only be allowed to inspect it either personally or through an advocate in Court:
	Section-231 Supply of copies of statements and documents to accused in other cases triable by Court of Session Provided further that supply of documents in electronic form shall be considered as duly furnished.
	Section-251 Framing of charge (2) Included through audio-video electronic means and the accused shall be asked whether he pleads guilty of the offence charged or claims to be tried.
	Section-254 Evidence for prosecution. Provided that evidence of a witness under this sub-section may be recorded by audio-video electronic means. (2) The deposition of evidence of any public servant may be taken through audio-video electronic means.
	Section-262 When accused shall be discharged (2) If, upon considering the police report and the documents sent with it under section 193 and making such examination, if any, of the accused, either physically or through audio-video electronic means, as the Magistrate thinks necessary
	Section-265 Evidence for prosecution (3) Provided further that the examination of a witness under this sub-section may be done by audio-video electronic means at the designated place to be notified by the State Government
	Section-266 Evidence for defence. Provided further that the examination of a witness under this sub-section may be done by audio-video electronic means at the designated place to be notified by the State Government
	Section-308 Evidence to be taken in presence of accused including through audio-video electronic means at the designated place to be notified by the State Government
	Section-316 Record of examination of accused (4) Provided that where the accused is in custody and is examined through electronic communication, his signature shall be taken within seventy-two hours of such examination
	Section-336 Evidence of public servants, experts, police officers in certain cases.

	Provided further that the deposition of such successor public servant, expert or officer may be allowed through audio-video electronic means.
	Section-355 Provision for inquiries and trial being held in absence of accused in certain cases. Explanation. —For the purpose of this section, personal attendance of the accused includes attendance through audio-video electronic means.
	Section-356 Inquiry, trial, or judgment in absentia of proclaimed offender. (5) Where a trial is related to a person under this section, the deposition and examination of the witness, may, as far as practicable, be recorded by audio-video electronic means preferably mobile phone and such recording shall be kept in such manner as the Court may direct
	Section-392 Judgment. (5) If the accused is in custody, he shall be brought up to hear the judgment pronounced either in person or through audio-video electronic means.
	Section-412 Procedure in cases submitted to High Court for confirmation. In cases submitted by the Court of Session to the High Court for the confirmation of a sentence of death, the proper officer of the High Court shall, without delay, after the order of confirmation or other order has been made by the High Court, send either physically, or through electronic means, a copy of the order, under the seal of the High Court and attested with his official signature, to the Court of Session.
	Section-497 Order for custody and disposal of property pending trial in certain cases. (3) The Court or the Magistrate shall cause to be taken the photograph and if necessary, video graph on mobile phone or any electronic media, of the property referred to in sub-section (1)
	Section-530 Trial and proceedings to be held in electronic mode. All trials, inquires and proceedings under this Sanhita, including— (i) issuance, service and execution of summons and warrant; (ii) examination of complainant and witnesses; (iii) recording of evidence

	in inquiries and trials; and (iv) all appellate proceedings or any other proceeding, may be held in electronic mode, by use of electronic communication or use of audio-video electronic means

Revolutionizing Evidence Presentation: A Transparent Approach

1. Considering the risk of manipulation of evidence, the mandatory inclusion of audio-video recording in search and seizure proceedings is an important inclusion in BNSS. In BNSS Sec 105, the scope of audio - video recording during search and seizure includes, among others, the process of preparing a list of seized items and the signature of witnesses. Transparency in search and seizure proceedings is likely to deter against fabrication of evidence and ensure the presence of independent witnesses in these proceedings.

2. Sec 105 requires that this audio video recording be submitted before the District Magistrate, Sub - divisional Magistrate or Judicial Magistrate of first class 'without delay'. In BNSS Sec 176 (3), the requirement for videography of the process of collection of forensic evidence is another move towards greater transparency and accountability in evidence gathering, and a safeguard against irregularities and manipulation.

3. Audio - video recordings have the potential to strengthen the quality of evidence and steps have to be taken to prevent its alteration, modification and transposition, through direct intervention or unintended corruption of a digital record. Appropriate guidelines will have to be formulated for adopting procedures to maintain authenticity and accuracy of electronic evidence.

Section 105 of BNSS 2023 introduces procedures for preparing lists of seized items and witness signatures. Audio-video recordings presented immediately before magistrates ensure transparency in evidence collection, discouraging coercion during custodial interrogation.

	Section-105 Recording of search and seizure through audio video electronic means. Included under this Chapter or under section 185, including preparation of the list of all things seized in the course of such search and seizure and signing of such list by witnesses, shall be recorded through any audio-video electronic means preferably mobile phone and the police officer shall without delay forward such recording to the District Magistrate, Sub-divisional Magistrate or Judicial Magistrate of the first class

Similarly, Sec 176 (1) provides an option of audio - video recording of any statement made during police investigation. The scope of this proviso is wide enough to include disclosure statements of accused before the police, besides the statements of other witnesses (audio - video recording for which is already permitted under Sec.161 CrPC, retained in Sec 180 BNSS). This is an important safeguard to deter against torture and coercion of the accused during custodial interrogations.

Consistent with the CrPC, the BNSS retains the mandatory requirement for videography of police statements, and audio - video recording of statements before the magistrate for certain vulnerable victims with physical or mental disabilities, under Sec 173 (1) and 183 (6), respectively.

Sec 230 of BNSS requires the accused and victim (if represented by a lawyer) to be supplied with the police report and all necessary documents, including statements and confessions.

Bharatiya Sakshya Adhiniyam 2023 - Elevating Electronic Evidence: A Paradigm Shift

BSA, 2023 places electronic/digital evidence on equal footing with traditional documentation for admissibility.

Definitions of 'evidence' and 'documents' expand to include futuristic elements like server logs, locational evidence, and digital voice messages.

Admissibility of electronic records under BSA 2023 in Section 57 and 63 have clearly enunciated the nuances of the same.

BSA 2023 revolutionizes the law of evidence, treating electronic evidence as equivalent to physical evidence in courts.

BSA	
	Sec.2 d) "document" means any matter expressed or described or otherwise recorded upon any substance by means of letters, figures or marks or any other means or by more than one of those means,

	intended to be used, or which may be used, for the purpose of recording that matter and includes electronic and digital records. (vi) An electronic record on emails, server logs, documents on computers, laptop or smartphone, messages, websites, locational evidence, and voice mail messages stored on digital devices are documents. (e) "evidence" means and includes— (i) all statements including statements given electronically which the Court permits or requires to be made before it by witnesses in relation to matters of fact under inquiry and such statements are called oral evidence; (ii) all documents including electronic or digital records produced for the inspection of the Court and such documents are called documentary evidence.
	Section-57 Primary evidence. Explanation 4.—Where an electronic or digital record is created or stored, and such storage occurs simultaneously or sequentially in multiple files, each such file is primary evidence. Explanation 5.—Where an electronic or digital record is produced from proper custody, such electronic and digital record is primary evidence unless it is disputed. Explanation 6.—Where a video recording is simultaneously stored in electronic form and transmitted or broadcast or transferred to another, each of the stored recordings is primary evidence. Explanation 7.—Where an electronic or digital record is stored in multiple storage spaces in a computer resource, each such automated storage, including temporary files, is primary evidence.
	Section-63 Admissibility of electronic records. Computer in question and shall be admissible in any proceedings, without further proof or production of the original, as evidence or any contents of the original or of any fact stated therein of which direct evidence would be admissible. (2) The conditions referred to in sub-section (1) in respect of a computer output shall be the following, namely:— (a) the computer output containing the information was produced by the computer or communication device during the period over which the computer or communication device was used regularly to create, store or process information for the purposes of any activity regularly carried on over that period by the person having lawful control over the use of the computer or communication

	device; (b) during the said period, information of the kind contained in the electronic record or of the kind from which the information so contained is derived was regularly fed into the computer or communication device in the ordinary course of the said activities; (c) throughout the material part of the said period, the computer or communication device was operating properly or, if not, then in respect of any period in which it was not operating properly or was out of operation during that part of the period, was not such as to affect the electronic record or the accuracy of its contents; and (d) the information contained in the electronic record reproduces or is derived from such information fed into the computer or communication device in the ordinary course of the said activities. (3) Where over any period, the function of creating, storing or processing information for the purposes of any activity regularly carried on over that period as mentioned in clause (a) of sub-section (2) was regularly performed by means of one or more computers or communication device, whether— (a) in standalone mode; or (b) on a computer system; or (c) on a computer network; or (d) on a computer resource enabling information creation or providing information processing and storage; or € through an intermediary, all the computers or communication devices used for that purpose during that period shall be treated for the purposes of this section as constituting a single computer or communication device; and references in this section to a computer or communication device shall be construed accordingly. (4) In any proceeding where it is desired to give a statement in evidence by virtue of this section, a certificate doing any of the following things shall be submitted along with the electronic record at each instance where it is being submitted for admission, namely:— (a) identifying the electronic record containing the statement and describing the manner in which it was produced; (b) giving such particulars of any device involved in the production of that electronic record as may be appropriate for the purpose of showing that the electronic record was produced by a computer or a communication device referred to in clauses (a) to (e) of sub-section (3); (c) dealing with any of the matters to which the conditions mentioned in sub-section (2) relate, and purporting to be signed by a person in charge of the computer or communication device or the management of the relevant activities (whichever is appropriate) and an expert shall be evidence of any matter stated in the certificate; and for the purposes of this sub-section it shall be sufficient for a matter to be stated to the best of the knowledge and belief of the person stating it in the certificate specified in the Schedule (5) For the purposes of this section,—

	(a) information shall be taken to be supplied to a computer or communication device if it is supplied thereto in any appropriate form and whether it is so supplied directly or (with or without human intervention) by means of any appropriate equipment; (b) a computer output shall be taken to have been produced by a computer or communication device whether it was produced by it directly or (with or without human intervention) by means of any appropriate equipment or by other electronic means as referred to in clauses (a) to (e) of sub-section (3)
	Section-29 Relevancy of entry in public record or an electronic record made in performance of duty. An entry in any public or other official book, register or record or an electronic record, stating a fact in issue or relevant fact, and made by a public servant in the discharge of his official duty, or by any other person in performance of a duty specially enjoined by the law of the country in which such book, register or record or an electronic record, is kept, is itself a relevant fact
	Section-31 Relevancy of statement as to fact of public nature contained in certain Acts or notifications. When the Court has to form an opinion as to the existence of any fact of a public nature, any statement of it, made in a recital contained in any Central Act or State Act or in a Central Government or State Government notification appearing in the respective Official Gazette or in any printed paper or in electronic or digital form purporting to be such Gazette, is a relevant fact.
	Section-32 Relevancy of statements as to any law contained in law books including electronic or digital form. When the Court has to form an opinion as to a law of any country, any statement of such law contained in a book purporting to be printed or published including in electronic or digital form under the authority of the Government of such country and to contain any such law, and any report of a ruling of the Courts of such country contained in a book including in electronic or digital form purporting to be a report of such rulings, is relevant.
	Section-41 Opinion as to handwriting and signature, when relevant (2) When the Court has to form an opinion as to the electronic signature of any person, the opinion of the Certifying Authority which has issued the Electronic Signature Certificate is a relevant fact. Section-81 Presumption as to Gazettes in electronic or digital record

	The Court shall presume the genuineness of every electronic or digital record purporting to be the Official Gazette or purporting to be electronic or digital record directed by any law to be kept by any person, if such electronic or digital record is kept substantially in the form required by law and is produced from proper custody. Explanation.—For the purposes of this section and section 93 electronic records are said to be in proper custody if they are in the place in which, and looked after by the person with whom such document is required to be kept; but no custody is improper if it is proved to have had a legitimate origin, or the circumstances of the particular case are such as to render that origin probable.
	Section-85 Presumption as to electronic agreements. The Court shall presume that every electronic record purporting to be an agreement containing the electronic or digital signature of the parties was so concluded by affixing the electronic or digital signature of the parties.

Streamlining Secondary Evidence: A Futuristic Approach

The scope of secondary evidence broadens under BSA 2023, incorporating copies made through mechanical processes.

Two new forms introduced in the schedule to expedite the authentication and appreciation of digital evidence, addressing challenges under previous statutes.

BSA	
Sec-61	Section-61 Electronic or digital record. Nothing in this Adhiniyam shall apply to deny the admissibility of an electronic or digital record in the evidence on the ground that it is an electronic or digital record, and such record shall, subject to section 63, have the same legal effect, validity and enforceability as other document.

The most significant change in BSA is the introduction of evidentiary nature and admissibility of electronic evidence. The proposed changes include expansion of the definition of primary evidence to include

copies of electronic or digital files.

Admissibility of Electronic Records (Sec 57 and 63 BSA)

Similar to Sec 65B IEA, Sec 63 BSA provides a specific procedure for the admissibility of electronic records. Sec 2 (d) BSA which replaces Sec 3 IEA, defines documents to also include 'electronic or digital records'.

Sec 62 BSA, which replaces Sec 65A IEA, states that electronic records must be proved as primary evidence, unless mentioned. Newly introduced Sec 61 BSA, prescribes that the admissibility of electronic records cannot be denied on the basis of their nature as electronic records and their legal effect, validity and enforceability shall be at par with paper records. This will bring in a much - required change in the Evidence Law by treating electronic evidence as good as the physical evidences currently being dealt by courts.

Obviously, proper safeguards have to be built so that the legal sanctity of electronic evidence is maintained. Attention may also be provided towards building institutional and infrastructural capacity for its effective and mandatory implementation. This will include strengthening infrastructural facilities across States/UTs, providing the necessary gadgets collection - transmission - storage of electronic evidence, training of manpower in this regard, etc.

Guidelines will have to be framed by respective States / UTs to ensure high standard for the quality of the equipment, as well as to establish systems and infrastructure regarding the safe and secure storage and transfer of electronic evidence, besides ensuring that it is protected from being leaked, deleted or corrupted

TABLE 1: Crime committed by using Technology related Provisions in BNS:

Sl. No	Offences (B stands for Bailable offence and NB stands for Non Bailable offence) (C stands for Cognizable offence and NC for Non-Cognizable offence)	Section
1.1	Punishment for theft. (NB) (C)	Sec 303(2)
	Theft by clerk or servant of property in possession of master. (NB) (C)	Sec 306
	Dishonestly receiving stolen property. (NB)(C)	Sec 317(2)
	Punishment for extortion. (NB)(C)	Sec 308(2)
	Punishment for robbery. (NB)(C)	Sec 309(4)
	Punishment belonging to gang of thieves. (NB)(C)	Sec 313
	Punishment for dacoity. (NB)(C)	Sec 310 (2)
	Making preparation to commit dacoity. (NB)(C)	Sec 310(4)
	Punishment for belonging to gang of dacoits. (NB)(C)	Sec 310(5)
	Assembling for purpose of committing dacoity. (NB)(C)	Sec 310(5)
	Dishonest misappropriation of property. (B) (NC)	Sec 314
	Dishonestly receiving property stolen in the commission of dacoity. (NB) (C)	Sec 317(3)

	Assisting in concealment of stolen property. (NB)(C)	Sec 317(5)
	Punishment for criminal trespass. (B) (C)	Sec 329(3)
1.2	Punishment for Cheating. (B) (NC)	Sec 318(2)
	Cheating and dishonestly inducing delivery of property. (NB)(C)	Sec 318(4)
	Punishment for criminal Breach of Trust. (NB) (C)	Sec 316(4)
	Criminal breach of trust by clerk or servant. (NB)(C)	Sec 316(4)
	Criminal breach of trust by public servant or by banker, merchant or agent. (NB)(C)	Sec 316(5)
	Cheating with knowledge that wrongful loss may ensue to person whose interest offender is bound to protect. (B) (NC)	Sec 318(3)
	Punishment for cheating by Personation. (B) (C)	Sec 319 (2)
	Punishment for criminal intimidation. (B) (NC)	Sec 351(2)
1.3	Punishment for forgery. (B) (NC)	Sec 336(2)
	Forgery for the purpose of cheating. (NB)(C)	Sec 336(3)
	Destruction of document or electronic record to prevent its production as evidence. (B) (NC)	Sec 241
	Falsification of accounts. (B) (NC)	Sec 344
	Punishment for false evidence. (B) (NC)	Sec 229
	Threatening any person to give false evidence. (NB)(C)	Sec 232

	False Personation for purpose of act or proceeding in suit or prosecution. (B) (NC)	Sec 242
	Issuing or signing false certificate. (B) (NC)	Sec 234
1.4	Sale etc. of Obscene books etc. (B) (C)	Sec 294
	Sale etc. of Obscene objects to young person. (B) (C)	Sec 295
	Obscene acts and songs. (B) (C)	Sec 296
	Sexual harassment and punishment for sexual harassment. (NB)(C)	Sec 75
	Voyeurism. (Bailable in 1st Conviction and Non Bailable in 2nd Conviction) (C)(**B)**	Sec 77
	Stalking. (Bailable in 1st Conviction and Non Bailable in 2nd Conviction) (C) (NB)	Sec 78
	Punishment for Defamation. (B) (NC)	Sec 356(2)
	Printing or engraving matter known to be defamatory. (B) (NC)	Sec 356(3)
	Sale of printed or engraved substance containing defamatory matter. (B) (NC)	Sec 356(4)
	Intentional insult with intent to provoke Breach of peace. (B) (NC)	Sec 352
	Criminal intimidation by an anonymous communication. (B) (NC)	Sec 351(4)
	Uttering any word, gesture or act intended to insult the modesty of women. (B) (C)	Sec 79
	Kidnapping, abducting or inducing woman to compel her marriage etc. (NB) (C)	Sec 87

	Punishment for criminal intimidation. (B) (NC)	Sec 351(2)
1.5	Punishment for criminal conspiracy. (Bailable or Non Bailable) (Cognizable or Non-Cognizable)	Sec 61
	Waging or attempting to wage war or abetting waging of war against the	Sec147
	government of India. (NB)(C)	
	Conspiracy to commit offence punishable by Sec 147 (NB)(C)	Sec 148
	Sedition. (NB)(C)	Sec 152
	Promoting enmity between different groups on ground of religion, race, place of birth, residence, language etc. and doing acts prejudicial to maintenance of harmony. (NB)(C)	Sec 196(1)
	Imputations, assertions prejudicial to national- integrity. (NB)(C)	Sec 197
	Intentional insult with intent to provoke breach of peace. (B) (NC)	Sec 352
	Collecting arms etc, with intention of waging war against the Government of India. (NB) (C)	Sec 149
	Punishment for unlawful assembly. (B) (C)	Sec 189(2)
1.6	Making or selling instrument for counterfeiting coin. (NB)(C)	Sec 181
	Making or selling instrument for counterfeiting Indian coin. (NB)(C)	Sec181
	Possession of instrument or material for the purpose of using the same for counterfeiting coin. (NB)(C)	Sec 181
	Counterfeiting currency notes or bank notes. (NB) (C)	Sec 178
1.7	Nonattendance in obedience to an order from public servant. (B) (NC)	Sec 208

	Omission to produce document to public servant by person legally bound to give it. (B) (NC)	Sec 210
	Omission to give notice or information to public servant by person legally bound to give it. (B) (NC)	Sec 211
	Refusing oath or affirmation when duly required by public servant to make it. (B) (NC)	Sec 213
	Refusing to answer public servant authorized to question. (B) (NC)	Sec 214
	False statement on oath or affirmation to public servant or person authorized to administer an oath or affirmation. (B) (NC)	Sec 216
	False information, with intent to cause public servant to use his lawful power to the injury of another person. (B) (NC)	Sec 217
	Omission to assist public servant when bound by law to give assistance. (B) (NC)	Sec 222
	Disobedience to order duly promulgated by public servant. (B) (C)	Sec 223
1.8	Abetment of a thing	Sec 45
	Punishment of abetment if act abetted is committed in consequence, and where no express provision is made for its punishment. (B/NB) (C/NC)	Sec 49

Table 2: Cyber offences and provisions in the IT Act

Sl. No	Nature of cyber offence	IT Act Provisions (B stands for Bailable offence and NB stands for Non Bailable offence) (C stands for Cognizable offence and NC for Non-Cognizable offence)	Reference of Provision in Bhartiya Nayaya Sanhita(BNS)
2.1	**Cheating**	Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B)	Sec 318 (2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2), 351 (2), 208, 210, 211, 213, 214, 216, 217, 222,

		(C) Sec 66D: Cheating by Personation by using Computer Resource. (B) (C) Sec 67: Publishing or transmitting of obscene material in electronic form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C) Sec 67A: Publishing or transmitting of material containing sexually explicit act etc. in electronic form. (NB) (C) Sec 67B: Publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form. (NB) (C) Sec 72: Breach of confidentiality and privacy. (B) (NC) Sec 72A: Punishment for disclosure of information in breach of lawful contract. (B) (C)	223
2.2	**Fraud**	Sec 43: Damage to computer, computer system etc. Sec 43A: Failure to protect data. Sec65: Tampering with computer source document. (B)(C) Sec 66: Computer related offences. (B)(C) Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or	318(2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2) ,351 (2), 336 (2), 336 (3), 241, 344, 229, 232, 242, 234, 208, 210, 211, 213, 214, 216, 217, 222, 223.

		any other unique identification feature of any other persons. (B) (C) Sec 66D: Cheating by Personation by using Computer Resource. (B) (C) Sec 72: Breach of confidentiality and privacy. (B) (NC) Sec 72A: Punishment for disclosure of information in breach of lawful contract. (B) (C)	
2.3	**Forgery**	Sec 43: Damage to computer, computer system etc. Sec 65: Tampering with computer source document. (B)(C) Sec 66: Computer related offences. (B)(C) Sec 72: Breach of confidentiality and privacy. (B) (NC) Sec 72A: Punishment for disclosure of information in breach of lawful contract. (B) (C)	336 (2), 336 (3), 241, 344, 229, 232, 242, 234, 208, 210, 211, 213, 214, 216, 217, 222, 223.
2.4	**Breach of trust**	Sec 43A: Failure to protect data. Sec 66B: Dishonestly receiving stolen computer resource or communication device. (B)(C) Sec 66D: Cheating by Personation by using Computer Resource. (B) (C) Sec 66E: Violation of privacy. (NB) (C) Sec 72: Breach of confidentiality and privacy. (B) (NC)	294, 295, 296, 75, 77, 78, 356 (2), 356 (3), 356 (4), 352, 351 (4), 79, 87, 351 (2), 208, 210, 211, 213, 214, 216, 217, 222, 223

2.5	**Counterfeiting**	Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B) (C)	Sec 181 & 178
2.6	**Threat**	Sec 43(C): Contamination and Virus. Sec 65: Tampering with computer source document. (B) (C) Sec 66B: Dishonestly receiving stolen computer resource or communication device. (B) (C) Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B)(C) Sec 66E: Violation of privacy. (B)(C) Sec 66F: Cyber Terrorism. (NB)(C) Sec 67: Publishing or transmitting of obscene material in electronic form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C) Sec 67A: Publishing or transmitting of material containing sexually explicit act etc in electronic form. (NB) (C) Sec 67B: Publishing or transmitting of material depicting	Sec 303 (2), 306, 317(2), 308 (2), 309 (2), 313, 310 (2), 310 (4), 310 (5), 314, 317 (3), 317 (5), 329 (3), 318 (2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2) ,351 (2), 294, 295, 75,77,78, 356 (2), 356 (3), 356 (4), 352, 351 (4), 79, 87, 61, 147, 148, 152, 196 (1), 197, 149, 189 (2), 208, 210, 211, 213, 214, 216, 217, 222, 223.

		children in sexually explicit act etc. in electronic form. (NB)(C) Sec 72: Breach of confidentiality and privacy. (B) (NC)	
2.7	**Intimidation**	Sec 43: Damage to computer, computer system etc. Sec 65: Tampering with computer source document. (B)(C) Sec 66B: Dishonestly receiving stolen computer resource or communication device. (B)(C) Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B) C) Sec 66E: Violation of privacy. (B) (C) Sec 67: Publishing or transmitting of obscene material in electronic form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C) Sec 67A: Publishing or transmitting of material containing sexually explicit act etc. in electronic form. (NB) (C) Sec 67B: Publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form. (NB) (C)	Sec 318(2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2), 351 (2), 336 (2), 336 (3), 241, 344, 229, 232, 242, 234, 294, 295, 296, 75, 77, 78, 356 (2), 356 (3), 356 (4), 352, 351 (4), 79, 87
2.8	**Obscenity**	Sec 66E: Violation of privacy. (B) (C) Sec 67: Publishing or transmitting of obscene material in electronic	Sec 318 (2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2), 351 (2), 294, 295, 296, 75, 77, 78, 356 (2), 356 (3),

		form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C) Sec 67A: Publishing or transmitting of material containing sexually explicit act etc. in electronic form. (NB) (C) Sec 67B: Publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form. (NB) (C)	356 (4), 352, 351 (4), 79, 87, 351 (2),
2.9	**Vulgarity**	Sec 66E: Violation of privacy. (B) (C) Sec 67: Publishing or transmitting of obscene material in electronic form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C) Sec 67A: Publishing or transmitting of material containing sexually explicit act etc. in electronic form. (NB) (C) Sec 67B: Publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form. (NB) (C)	Sec 318 (2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2) 351 (2), 294, 295, 296, 75, 77, 78, 356 (2), 356 (3), 356 (4), 352, 351 (4), 79, 87
2.10	**Defamation**	Sec 66D: Cheating by Personation by using Computer Resource. (B) (C) Sec 67: Publishing or transmitting of obscene material in electronic form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C) Sec 67A: Publishing or transmitting of material containing	Sec 318 (2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2) , 351 (2), 294, 295, 296, 75, 77, 78, 356 (2), 356 (3), 356 (4), 352, 351 (4), 79, 87

		sexually explicit act etc. in electronic form. (NB) (C) Sec 67B: Publishing or transmitting of material depicting children in sexually explicit act etc. in	
2.11	**Cyber stalking**	Sec 67: Publishing or transmitting of obscene material in electronic form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C) Sec 67A: Publishing or transmitting of material containing sexually explicit act etc. in electronic form. (NB) (C) Sec 72: Breach of confidentiality and privacy. (B) (NC)	294, 295, 296, 75, 77, 78, 356 (2), 356 (3), 356 (4), 352, 351 (4), 79, 87, 351 (2),
2.12	**Terrorism**	Sec 66F: Cyber Terrorism. (NB) (C) Sec 69: Power to issue directions for interception or monitoring or decryption of any information through any computer resource. (NB) (C) Sec 69A: Sec 69A: Power to issue directions for blocking for public access of any information through any computer resource. (NB) (C) Sec 69B: Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security. (B) (NC) Sec 70: Protected System Sec 70B: Indian computer emergency response team to serve	61, 147, 148, 152, 196 (1), 197, 352, 149, 189 (2)

		as National agency for incident response.	
2.13	**Piracy**	Sec 65: Tampering with computer source document. (B)(C) Sec 66: Computer related offences. (B)(C) Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B) C)	318(2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2) ,351 (2), 336 (2), 336 (3), 241, 344, 229, 232, 242, 234,
2.14	**Theft (Including Banking Frauds)**	Sec 43: Damage to computer, computer system etc. Sec 43A: Failure to protect data. Sec 66B: Dishonestly receiving stolen computer resource or communication device. (B)(C) Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B)(C) Sec 72: Breach of confidentiality and privacy. (B) (NC) Sec 72A: Punishment for disclosure of information in breach of lawful contract. (B) (C)	Sec 303 (2), 306, 317(2), 308 (2), 309 (2), 313, 310 (2), 310 (4), 310 (5), 314, 317 (3), 317 (5), 329 (3), 208, 210,211, 213, 214, 216, 217, 222, 223.
2.15	**Software infringement**	Sec 43: Damage to computer, computer system etc. Sec 65: Tampering with computer source document. (B)(C)	318(2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2) ,351 (2),

		Sec 66: Computer related offence. (B)(C) Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B) C)	
2.16	**Hacking (Attack on password & Web defacement)**	Sec 43: Damage to computer, computer system etc. Sec 65: Tampering with computer source document. (B)(C) Sec 66: Computer related offences. (B)(C) Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B)(C) Sec 66F: Cyber Terrorism. (NB)(C)	Sec 303 (2), 306, 317(2), 308 (2), 309 (2), 313, 310 (2), 310 (4), 310 (5), 314, 317 (3), 317 (5), 329 (3), 318(2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2) ,351 (2), 61, 147, 148, 152, 196 (1), 197, 352, 149, 189 (2),
2.17	**Spoofing**	Sec 66D: Cheating by Personation by using Computer Resource. (B)(C)	318(2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2) ,351 (2),
2.18	**Tampering**	Sec 65: Tampering with computer source document. (B)(C)	336 (2), 336 (3), 241, 344, 229, 232, 242, 234,
2.19	**Phishing, data diddling etc.**	Sec 66: Computer related offences. (B)(C) Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B) (C) Sec 66D: Cheating by Personation by using Computer Resource. (B)	318(2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2) ,351 (2),

		(C)	
2.20	**Offences related to OTP, UPI etc.** (other than petition received within golden Hour of transaction, which shall be transferred to the online group of Nodal officers)	Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B) (C) Sec 66D: Cheating by Personation by using Computer Resource. (B) (C) Sec 72: Breach of confidentiality and privacy. (B) (NC)	318(2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2) ,351 (2), 336 (2), 336 (3), 241, 344, 229, 232, 242, 234
2.21	**Email / Logic bombing**	Sec 43: Damage to computer, computer system etc. Sec 66: Computer related offences. (B) (C) Sec 66F: Cyber Terrorism. (NB) (C)	Sec 303 (2), 306, 317(2), 308 (2), 309 (2), 313, 310 (2), 310 (4), 310 (5), 314, 317 (3), 317 (5), 329 (3), 318(2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2) ,351 (2),
2.22	**Web jacking**	Sec 66E: Violation of privacy. (NB) (C) Sec 66D: Cheating by Personation by using Computer Resource. (B) (C) Sec 66F: Cyber Terrorism. (NB) (C) Sec 43A: Failure to protect data.	Sec 303 (2), 306, 317(2), 308 (2), 309 (2), 313, 310 (2), 310 (4), 310 (5), 314, 317 (3), 317 (5), 329 (3),
2.23	**Child abuse**	Sec 66E: Violation of privacy. (NB) (C) Sec 67B: Publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form. (NB) (C) Sec 69A: Power to issue directions for blocking for public	Sec 318 (2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2) , 351 (2), 294, 295, 296, 75, 77, 78, 356 (2), 356 (3), 356 (4), 352, 351 (4), 79, 87, 351 (2) And Section 12,13,14 and 15 of POCSO Act

		access of any information through any computer resource. (NB) (C)	
2.24	**Fake profile**	Sec 66D: Cheating by Personation by using Computer Resource. (B) (C) Sec 67: Publishing or transmitting of obscene material in electronic form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C)	Sec 318(2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2) ,351 (2), 336 (2), 336 (3), 241, 344, 229, 232, 242, 234, 294, 295, 296, 75, 77, 78, 356 (2), 356(3), 356(4), 352, 351 (4),79, 87, 351 (2),
2.25	**ATM Online fraud**	Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B) (C)	Sec 303 (2), 306, 317(2), 308 (2), 309 (2), 313, 310 (2), 310 (4), 310 (5), 314, 317 (3), 317 (5), 329 (3), 318(2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2) ,351 (2),
2.26	**ATM Physical burglary**	- NIL -	Sec 303 (2), 306, 317(2), 308 (2), 309 (2), 313, 310 (2), 310 (4), 310 (5), 314, 317 (3), 317 (5), 329 (3), 318(2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2) ,351 (2),
2.27	**Failure to preserve and retain data by intermediaries**	Sec 67C: Preservation and retention of information by intermediary. (B) (C)	----
2.28	**Failure by the intermediary to assist the agency.**	Sec 69: Power to issue directions for interception or monitoring or decryption of any information through any computer resource. (NB) (C) Sec 69A: Power to issue directions for blocking for public access of any information through any computer resource. (NB) (C)	208, 210, 211, 213, 214, 216, 217, 222, 223.

		Sec 69B: Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security. (B) (NC)	
2.29	**Offences relating to Digital signature certificate.**	Sec 71: Penalty for Misrepresentation. (B) (NC) Sec 73: Penalty for publishing Electronic Signature Certificate false in certain particulars. (B)(NC)	Sec 303 (2), 306, 317(2), 308 (2), 309 (2), 313, 310 (2), 310 (4), 310 (5), 314, 317 (3), 317 (5), 329 (3), 318(2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2) ,351 (2), 336 (2), 336 (3), 241, 344, 229, 232, 242, 234, 208, 210, 211, 213, 214, 216, 217, 222, 223.
2.30	**Offences relating to religion.**	Sec 66D: Cheating by Personation by using Computer Resource. (B)(C) Sec 66F: Cyber Terrorism. (NB)(C) Sec 69B: Power to authorize to monitor and collect traffic data or information through any computer resource for cyber security. (B) (NC)	318(2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2) ,351 (2), 61, 147, 148, 152, 196 (1), 197, 352, 149, 189 (2),
2.31	**Mis- representation**	Sec 66C: Fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other persons. (B)(C) Sec 66D: Cheating by Personation by using Computer Resource. (B) (C) Sec 66E: Violation of privacy. (NB) (C) Sec 71: Penalty for	Sec 303 (2), 306, 317(2), 308 (2), 309 (2), 313, 310 (2), 310 (4), 310 (5), 314, 317 (3), 317 (5), 329 (3), 318(2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2) ,351 (2), 336 (2), 336 (3), 241, 344, 229, 232, 242, 234, 208, 210, 211, 213, 214, 216, 217, 222, 223.

		Misrepresentation. (B) (NC) Sec 72: Breach of confidentiality and privacy. (B) (NC)	
2.32	**Sale of illegal articles and Trafficking**	Sec 66E: Violation of privacy. (B) (C) Sec 67: Publishing or transmitting of obscene material in electronic form. (Bailable in 1st Conviction and Non Bailable for subsequent offence, if convicted in the 1st offence) (C) Sec 67A: Publishing or transmitting of material containing sexually explicit act etc. in electronic form. (NB) (C) Sec 67B: Publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form. (NB) (C) Sec 72: Breach of confidentiality and privacy. (B) (NC)	Sec 318(2), 318 (4), 316 (4), 316 (5), 318 (3), 319 (2) ,351 (2), 336 (2), 336 (3), 241, 344, 229, 232, 242, 234, 294, 295, 296, 75, 77, 78, 356 (2), 356 (3), 356 (4), 352, 351 (4), 79, 87, 351 (2),
2.33	**Internet time theft**	Sec 43(h): charge the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network. Sec 65: Tampering with computer source document. (B)(C)	Sec 303 (2), 306, 317(2), 308 (2), 309 (2), 313, 310 (2), 310 (4), 310 (5), 314, 317 (3), 317 (5), 329 (3),

TABLE 3 : <u>Related Provisions in the POCSO Act, etc</u>

Sl. No	Offence (B stands for Bailable offence and NB stands for Non-Bailable offence) (C stands for Cognizable offence and NC for Non-Cognizable offence)	Section
3.1	Punishment for Sexual harassment. (NB) (C)	Sec 12 of POCSO Act
	Use of child for Pornographic purpose. (NB) (C)	Sec 13 of POCSO Act
	Punishment for using child for Pornographic purpose. (NB) (C)	Sec 14 of POCSO Act
	Punishment for storage of pornographic material involving Child. (NB) (C)	Sec 15 of POCSO Act

Note-1: Certain sections from the following Acts can also be found relevant to the petition received by the SHO.

1. The Copyright Act, 1957
2. Trade Marks Act., 1999
3. The Patents Act, 1970
4. The Immoral Traffic (Prevention) Act, 1956
5. Indecent representation of women (prohibition) Act,1985
6. Prevention of terrorism Act, 2002
7. Terrorist and Disruptive Act,1987
8. Negotiable instruments Act, 1881
9. Foreign Exchange Management Act, 1999
10. Arms Act, 1959
11. Narcotic drug and psychotropic substance Act, 1985
12. Theft Act, 1968
13. Currency notes forgery Act, 1899.
14. Indian explosives Act,1884
15. Protection of civil rights Act, 1955
16. The Banker's Books Evidence Act, 1891
17. Reserve Bank of India Act, 1934

TABLE 4: Provisions of collection of Evidence in BNSS & BSA related to Cyber Crime through Cyber Forensics

Sl. No	Platform	Evidence to be collected	Sources of evidence	Procedure and Admissibility
4.1	Online Banking	1. Debit card number. 2. Name of the account holder. 3. Bank with branch. 4. SMS received regarding the transfer. 5. Cash transfer details from bank. 6. Recipient's bank A/C details / E-wallet details.	Items 1 to 4 to be collected from the account holder. Item 5 to be collected from the account holder's bank. Item 6 to be collected from the recipient's bank.	See Sec 94,112 & 113 of BNSS and Sec 61 & 63 of BSA.
4.2	Card details theft using a Wi-Fi Modem spliced on the broadband cable.	1. Wi-Fi modem details. 2. Date and time stamps of spicing to be obtained from the event logs of the bank network server. 3. Stolen data to be recovered from the criminal's computer.	ATM fraudulently spliced, Wi-Fi modem, camera, bank network server etc.	See Sec 94,112 & 113 of BNSS and Sec 61 & 63 of BSA.
4.3	Card details theft using skimmer and PIN theft using camera.	Skimmer details and camera details.	ATM, skimmer, camera.	See Sec 94,112 & 113 of BNSS and Sec 61 & 63 of BSA.

4.4	ATM withdrawal through victim's A/C.	Handles, user ID, password, IP address, date and time stamps and bank details.	From the respective bank manager.	See Sec 94,112 & 113 of BNSS and Sec 61 & 63 of BSA.
4.5	Steganographic images / videos/ audio.	1. Name and version of the software tool used for fabrication, date and time stamps and other details from the hex dump of image/video. 2. The software codes inserted through Steganographic technique have to be separated from the image / video and then to be analyzed with the objective of finding the fraudulent motives of the codes.	Hex dump of the image. Note: These evidence are unlikely to exist in the hex dump of the compressed images / videos / audio received through social media apps like whatsapp, facebook etc. Try only from the originally fabricated / forged images / videos/ audio.	See Sec 94,112 & 113 of BNSS and Sec 61 & 63 of BSA.
4.6	CCTV Video Clippings	1. Required scenes 2. Date and time stamps of the required scenes. 3. Original video creation details from the hex dump of the video clipping obtained from the hard disk of	Hardisk of the CCTV system	See Sec 94,112 & 113 of BNSS and Sec 61 & 63 of BSA.

		the CCTV system.		
4.7	RAM Analysis	Necessary Artifacts from RAM	RAM of Mobile, Computer, Electronic weighing machines, Electronic meters etc.	See Sec 94,112 & 113 of BNSS and Sec 61 & 63 of BSA.
4.8	Ransomware attacks	Handles, User ID, password , IP address, date and time stamps of the source, decryptions keys, related activity logs etc.	1. Source device, related network devices etc. 2. Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc.	See Sec 94,112 & 113 of BNSS and Sec 61 & 63 of BSA.
4.9	Hacking	Handles, User ID, password, IP Address, date and time stamps of the source, related activity logs etc.	1. Related devices and networks,	See Sec 94,112 & 113 of BNSS and Sec 61 & 63 of BSA.
4.10	Cyber spoofing	Handles, User ID, password, Original IP address, details of the software tool used for spoofing, date and time stamps of spoofing.	1. The App and the Device used for spoofing, related networks etc. 2. Operating system event logs etc obtained from the Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash	See Sec 94,112 & 113 of BNSS and Sec 61 & 63 of BSA.

			memory etc.	
4.11	Theft of documents using the Outbox of the E-mail system.	Handles, User ID, password, Date and time stamps of uploading to and the subsequent downloading from the Outbox.	Outbox of the E-mail system.	Sec 61 & 63 of BSA.
4.12	E-mail communication	Handles, User ID, password, E-Mail address, IP addresses, date and time stamps of the sender and other dispatch details.	Source code of the received Email. Additional information: Sender's details are to be collected from Email service provider.	See Sec 94,112 & 113 of BNSS and Sec 61 & 63 of BSA.
4.13	Cyber attacks	Handles, User ID, password, IP Address, date and time stamps of source, related activity logs etc.	1. Related devices and networks, CDR, IP dump, IPDR dump. 2. Operating system event logs etc obtained from the Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc.	See Sec 94,112 & 113 of BNSS and Sec 61 & 63 of BSA.
4.14	Cyber warfare and Cyber Terrorism	Handles, User ID, password, IP Address, date and time stamps of the source of communication, content of	1. Related devices and networks, CDR, IP dump, IPDR dump. 2. Operating	See Sec 94, 97,112 & 113 of BNSS and Sec 61 & 63 of BSA.

		communication (encrypted or not), related activity logs etc.	system event logs etc obtained from the Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc.	
4.15	Audio fabrication	1. Name and version of the software tool used for fabrication, date and time stamps and other details. 2. Evidence to establish the ownership of the voice as required by forensics linguistic methods.	1. Hex dump of the Audio file obtained from the Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc. Note: These evidence are unlikely to exist in the hex dump of the compressed audios received through social media apps like whatsapp, facebook etc. Try only from the originally fabricated / forged audios. 2.Voice samples from the Audio File.	See Sec 94,112 &113 of BNSS and Sec 61 & 63 of BSA.
4.16	Image / Video fabrication / forgery	Name and version of the software tool used for fabrication, date	Hex dump of the Image/Video obtained from the Storage devices like hard disk,	See Sec 94,112 &113 of BNSS and Sec 61 & 63 of BSA.

		and time stamps and other details from the hex dump of image/video.	DVD, CD, Pendrive, SD Card, flash memory etc. Note: These evidence are unlikely to exist in the hex dump of the compressed images / videos received through social media apps like whatsapp, facebook etc. Try only from the originally fabricated / forged images / videos.	
4.17	Counterfeiting	Name and version of the software tool used for fabrication, date and time stamps and other details from the hex dump of image.	Hex dump of the non-compressed image obtained from the Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc. Note: These evidence are unlikely to exist in the hex dump of the compressed images received through social media apps like WhatsApp, facebook etc. Try	See Sec 94,97, 98 112 &113 of BNSS and Sec 61 & 63 of BSA.

			only from the originally fabricated / forged images.	
4.18	Fund misappropriation	Evidence of addition of a record or deletion of a record or modification of a record in the tables of fund databases.	Fund data base, operating system event logs etc.	See Sec 94,97,112 &113 of BNSS and Sec 61 & 63 of BSA.
4.19	Deleted Data recovery	Deleted file	Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc.	See Sec 94,97,112 &113 of BNSS and Sec 61 & 63 of BSA.
4.20	Data Piracy	Evidence of plaintiff's original possession of the data and evidence of defendant's illegal possession of the data (Sec 328).	Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc of plaintiff and defendant.	See Sec 94,97 of BNSS and Sec 61 & 63 of BSA.
4.21	Software Theft	Evidence of plaintiff's original possession of the software and evidence of defendant's illegal possession of the software (Sec 328 of IPC).	Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc of both plaintiff and defendant.	See Sec 94,97 & 98 of BNSS and Sec 61 & 63 of BSA.
4.22	Software Copyright Infringement	Evidence of copyright infringement after	Plaintiff and defendant software	Sec 64 of Copyright Act and See Sec Sec 61 & 63 of BSA.

		comparing the 2 sets of software by subjecting them through AFC OR POSAR Test.	packages in the Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc.	
4.23	VOIP (Net telephone)	IP Dump/IPDR	Telecom service	Sec 94,112 &113 of BNSS and Sec 61 & 63 of BSA.
4.24	Call / SMS details	Call details record (CDR)	Telecom Service Provider	Sec 94,112 &113 of BNSS and Sec 61 & 63 of BSA.
4.25	Data base	Evidence of addition of a record or deletion of a record or modification of a record in the tables of database.	Data base, transaction log of the data base, operating system event logs etc.	Sec 61 & 63 of BSA.
4.26	Operating system	Transaction logs	Operating systems like android, IOS etc. in the source device, event logs.	See Sec 61 & 63 of BSA.
4.27	Client-Server-technology-Based Social Media apps like facebook, TikTok etc.	1. Handles, User ID, password, IP address, date and time stamps. 2. 2.Owner details (CAF) of the phone number.	1. Social media service provider. 2. Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc. 3.Telecom Service	Sec 94,112 &113 of BNSS and Sec 61 & 63 of BSA.

			Provider	
4.28	Peer-to- Peer-technology-based Social Media Apps like Whatsapp, Instagram, Snap chat, Telegram, IMO etc.	1. Handles, User ID, password, IP address, date and time stamps, phone number, IMEI Code. 2. Owner details (CAF) of the phone number.	1.Social media service provider 2. Source device 3. Storage devices like hard disk, DVD, CD, Pendrive, SD Card, flash memory etc. 4.Telecom Service Provider	Sec 94,112 &113 of BNSS and Sec 61 & 63 of BSA.