International Journal of Humanities and Social Science Invention (IJHSSI)
ISSN (Online): 2319 – 7722, ISSN (Print): 2319 – 7714
www.ijhssi.org ||Volume 12 Issue 7|| July 2023 || PP. 22-28

Laws Governing Digital Signature in India: An Overview

Dr.Shashirekha Malagi*

Abstract
A digital signature is intended to solve the problem of tampering and impersonation in digital communications. Digital signatures can provide evidence of origin, identity and status of electronic documents, transactions or digital messages. Signers can also use them to acknowledge informed consent. In advancement of the growing industrial era, and increasing transactions in cyberspace over the recent years made it very necessary to have a legal framework dealing with e-signatures. This paper has been discussed the digital signature and the laws governing digital signature in India for effective protection.

Date of Submission: 25-06-2023 Date of Acceptance: 06-07-2023

I. Introduction

The world is witnessing a vast and rapid development in the field of technology in the world of communication, especially the Internet, have become indispensable means. After the communications depended on the phone and then fax, the Internet appeared and became the ideal means of communicating, transmitting, and presenting information, there has been an urgent need to protect, document, and prove this information's authenticity, as such the so-called Digital signature appeared in the year 1989. The first Digital signature was recognized in France in the field of credit cards with the aim of achieving this, the French Court of Cassation recognized the validity of the Digital signature as it considered that it consisted of two components, namely, showing the credit card and entering the card holder's secret number and confirmed that this method provides the existing guarantees in hand-signing, and it is even superior to it .This research paper has been discussed the laws governing digital signature in India for effective authentication and confidentiality of information ,data and document in the context of Information Technology Act 2000.

II. Definition of Digital Signature

*Section 2(1)(p):*According to Section 2(1)(p), Digital signature means '*authentication of any electronic record using an electronic method or procedure in accordance with the provisions of Section 3*'.

Further, authentication is a process for confirming the identity of a person or proving the integrity of information. Authenticating messages involves determining the source of the message and verifying that is has not been altered or modified in transit.[i]

According to the Information Technology Act, 2000, digital signatures mean authentication of any electronic record by a subscriber by means of an electronic method or procedure in accordance with the provisions of section 3.Further, the IT Act, 2000 deals with digital signatures under Sections 2, 3, and 15.

III. The Objectives of Digital Signature

a. To create authenticity of the originator

b. To create authenticity of the document - so that any recipient will not be in position to modify, change, alter, or tamper with the document created by originator.[ii]

IV. Characteristics' of Digital Signature[iii]

a. Evidential value: When the digital signature is affixed on electronic records then it gives recipient reason to believe that message or document was created by known sender and not altered during transaction and it is to be treated authenticate. Therefore, it makes the electronic record authenticate documentary evidence.

b. Proof of attached document: While affixing digital signature or electronic signature on electronic records is only to prove legality of certain other document's then affixing digital signature or electronic signature perform as proof of attached document/s.

* *Asst.Prof.of Law , KUSSK Law College, & Research Scholar, P.G.Dept.of Law, Karnatak University, Dharwad, Karnataka.580001*

c. Authentic execution of document: While performance of business transaction requires approval by using or affixing digital or electronic signature, then to make the document legally approved and authentic for execution the digital or electronic signature is important.

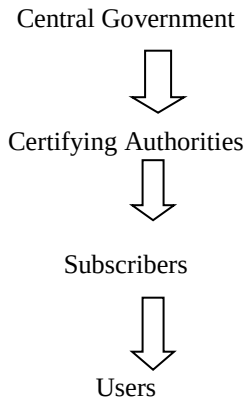
d. Efficiency: Digital signature as well as electronic signature make a document much efficient showing originators/senders and recipients and that the document has finality. Therefore, it can be executed immediately. As affixing signature only requires use of several click and hash function it is time saving too.

e. Integrity: The sender and receiver will be confident that the message has not been altered during transmission, because any alteration to document after signature will invalidate the signature.

V. Benefits of Digital signatures[iv]:

- Security: Security capabilities are embedded in digital signatures to ensure a legal document isn't altered and signatures are legitimate. Security features include asymmetric cryptography, personal identification numbers (PINs), checksums and cyclic redundancy checks (CRCs), as well as CA and trust service provider (TSP) validation.
- Time stamping: This provides the date and time of a digital signature and is useful when timing is critical, such as for stock trades, lottery ticket issuance and legal proceedings.
- Globally accepted and legally compliant :The public key infrastructure standard ensures vendor-generated keys are made and stored securely. With digital signatures becoming an international standard, more countries are accepting them as legally binding.
- Time savings: Digital signatures simplify the time-consuming processes of physical document signing, storage and exchange, enabling businesses to quickly access and sign documents.
- Cost savings: Organizations can go paperless and save money previously spent on the physical resources, time, personnel and office space used to manage and transport documents.
- Positive environmental effects: Reducing paper use also cuts down on the physical waste generated by paper and the negative environmental impact of transporting paper documents.
- Traceability: Digital signatures create an audit trail that makes internal record-keeping easier for businesses. With everything recorded and stored digitally, there are fewer opportunities for a manual signee or record-keeper to make a mistake or misplace something.

VI. Grant of Digital Signature[v]



The central government of India assigns Controller of Certifying Authorities (CCA) under section 17 of the Act. Section 21(1)(g) under the Act of 2000 states a person who grants a license for the issue of electronic certificates. The IT act gives the authority to CCA for issuing license to the Certifying Authorities CA. The Controllergrants the licences to the 'Certifying Authority' which further issue 'digital signature' to the subscriber. Thus, Controller does not directly issue 'digital signature', but issues licenses to the 'Certifying Authority'.

The digital signature of the CCA is also included in every public key of the digital signature certificate provided as established under section 18(b) of the IT act. This helps to certify the originality of the certificate. The legitimate signatories of company and professionals, and people who signs manual documents and returns filed with ROC are required to obtain a Digital Signature Certificate (DSC). Hence the following officials should have DSC. (Digital Signature Certificate, 2013).

a. Directors of organizations.

b. CA's/Auditors.

c. Company Secretary.
d. Bank Officials - for Registration and Satisfaction of Charges.
e. Other Authorized Signatories. The people who have income more than a million rupees per annum can only file their tax return through eservice using digital signature.

VII. Types of Digital Signatures Certificates[vi]:

There are 4 different types of digital signatures certificates in India.
They are 1. Class 0 Certificates
2. Class 1 Certificates
3. Class 2 Certificates
4. Class 3 Certificates

Explanation:
Class 0 Certificate: This certificate is used only for demonstration purposes to test the certificate and get familiar with the various usage of the digital signature certificates over the different fields of applications.
Class 1 Certificate: This certificate is used to individuals or private subscribers. These certificates will confirm that users name or E-mail address form a clear subject within the Certifying Authorities database.
Class 2 Certificate: This certificate is used by both business personnel and private individuals. These certificates will confirm that the information in the application is given by the subscriber does not conflict with the information in well-recognized consumer databases.
Class 3 Certificate: This certificate is used by individuals as well as organizations. This is high affirmation certificate, primarily intended for e-commerce applications. This certificate is given to individuals only on their personal (physical) appearance before the Certifying Authorities.

VIII. Components of Digital Signature Certificate[vii]:

a. Public key: It is the reference for the digital certificate; this is provided to certify the document sent.
b. User name and e-mail address: This provides information about the person, to whom the signature relates.
c. Expiration date of the public key: The digital signature certificate is authentic until this date. Name of the company: This is used for identifying the company to which the signature belongs. Serial number of the Digital ID: This is a unique number that is included in the signature helps us for tracking.
d. Digital signature of the Certification Authority: This is the signature of the CA, used to certify the originality of the certificates.
e. Certifying Authorities: Certification Agencies are appointed by the office of the Controller of Certification Agencies (CCA) under the provisions of IT Act 2000 in India. There are a total of seven Certification Agencies authorized by the CCA to issue the Digital Signature Certificates.

IX. Applications of Digital Certificates in India[viii]:

The applicant may file an application of Digital Signature Certificate for the following Purposes:
a. For sending and receiving digitally signed and encrypted emails.
b. For carrying out secure web-based transactions and also to know other participants of web-based
c. E-Tendering for the various government projects.
d. E-Procurement of various kinds of commodities in the ecommerce applications.
e. Ministry of Corporate Affairs for registering the corporate companies.
f. E-Filing - Income tax returns filing for the government.
g. For signing documents like MS Word, MS Excel and PDFs.

X. What are the laws for Digital Signature in India?[ix]

Digital Signature in India are governed by :
a. Information Technology Act, 2000 (ITA)
b. Indian Contract Act of 1872 (ICA).
c. The Evidence Act
d. The Companies Act2013

These **e-signing laws** form the basis for all electronic signing activities.Primarily, the Act Information Technology 2000, (ITA) is the governing **law for e-signing in India**. The ITA sets basic benchmarks for the **rules of e-signing** to be followed.

10.1.Section 5 of the IT Act2000

The Information Technology Act, 2000 ("IT Act") provides for recognition of electronic records under Section 4, which illustrates that any document which is required by law to be in writing, typewritten or in printed form,

will be considered to be valid if it is rendered or made available in electronic form and accessible for a subsequent reference in future.[x]As per Section 10A of the IT Act, in case of a contract formation, where the communication of proposals and acceptance are expressed in electronic form or by means of an electronic record, such contract shall not be deemed to be unenforceable solely on the ground that such electronic form or means was used for that purpose. The aforesaid provision was introduced by the Information Technology (Amendment Act), 2008 taking into account the growing reliance on electronic means for executing commercial agreements/documents.There are a number of judicial pronouncements on this for instance in the matter of Trimex International FZE Ltd. Dubai v. Vedanta Aluminium, (2010) 3 SCC 1, the Supreme Court held that where the offer and acceptance has been made by the parties through e-mail the same shall not affect the implementation of such contract. Also, in the matter of Tamil Nadu Organic Pvt. Ltd. and Ors. v. State Bank of India, AIR 2014 MAD 103 wherein, the e- auction took place between the parties, the concerned High Court while applying the provisions of IT Act held that even if a contract is executed by electronic means it gives rise to a contractual liability and is enforceable under law.Further, as regards signing of the contracts, electronic signatures are treated as equivalent to traditional wet signatures and are also legally recognized under Section 5 of the IT Act

10.2. Section 3 of the Information Technology Act, 2000[xi]

Section 3 of the Information Technology Act, 2000 provides certain provisions for the authentication of electronic records. The provisions are:

- Subject to the provisions of this section, any subscriber can affix his digital signature and hence authenticate an electronic record.
- An asymmetric crypto system and hash function envelop and transform the initial electronic record into another record which affects the authentication of the record.
- Also, any person in possession of the public key can verify the electronic record.
- Further, every subscriber has a private key and a public key which are unique to him and constitute a functioning key pair.

10.3.Secure Digital Signature (Section 15)[xii]

Let's say that two parties agree to apply a certain security procedure. If it is possible to verify that a digital signature affixed was

1. Unique to the subscriber affixing it.
2. Capable of identifying the subscriber.
3. Created in a manner under the exclusive control of the subscriber.
4. Also, it is linked to the electronic record in such a manner that a change in the record invalidates the digital signature then It is a secure digital signature.

10.4. Subscriber's Liabilities[xiii]

Section 72 prohibits disclosure of electronic record, book, register, correspondence, information, document or other material by any authorized person who has access to those information to third person and impose punishment with upto 2 years imprisonment or up to one lakh rupees fine or with both. However, section 72A, was inserted vide IT(Amendment) Act, 2009, prescribes punishment for disclosure of information in breach of lawful contract with up to three years imprisonment, or upto five lakh rupees fine or with both. For subscribers always section 72A will be applicable because subscription of certificate always requires fulfilling some terms and conditions according to agreement between the Certifying Authority and the subscriber. Only after valid contract subscribers get authority to publish or authorise to publish or issue certificates. Therefore, fine for subscriber is five lakh i.e. more than for breach of confidentiality and privacy without contract.

10.5. Cyber Appellate Tribunal [xiv]

To deal with the disputes and to adjudicate the matters the Act provides for the establishment of Cyber Appellate Tribunal. However, section 64 of the Act empowers the appropriate authority under Cyber Appellate Tribunal to recover the penalty or compensation and the licence or the Electronic Signature Certificate where penalty or compensation is not paid and to suspend these till the penalty is paid.

10.6. Penalty for publishing false Digital Signature Certificate[xv]

Section 73 is applicable not only to subscribers but also every person who publishes false particulars of certificate. Under section 73(1) no person shall publish it or make it available to any other person knowingly that (a) the Certifying Authority has not issued the same certificate, (b) the subscriber listed in the certificate has no Authority immediately and till then he should have responsibility to maintain confidentiality and privacy as accepted. It can be done by the Certifying Authority or any other person including the subscriber. (c) The

certificate has been revoked or suspended. For example, in case of private key compromise it is the prime duty of the subscriber to inform the Certifying Authority.

10.7. Revocation and Suspension of the Certifying Authority[xvi]

If comes to know about misuse or abuse of certificate then he may revoke affected keys and certificates. During this revocation period if the subscriber certifies and uses the certificate as valid then it will be treated as criminal offence unless such publication is for the purpose of verifying a electronic signature created prior to such revocation or suspension of certificate. There may be temporary revocation or suspension of certificate for the purpose of periodical change of key pairs and in such case the authority should immediately inform about new key pairs to the subscribers. But during this suspended period no one should publish certificate to other person with knowledge. Therefore, here mensrea is very important factor. If knowledge is absent, it is not a crime because there are two elements of crime actus reus and mens-rea. Except exceptional cases, if both are present then only the human conduct will be treated as crime. Here exceptional situation is, if such publication is for the purpose of verifying a electronic signature created prior to such suspension or revocation. Section 73(2) prescribes punishment for the contravention of the provisions of section 73(1) with upto two years imprisonment or upto one lakh rupees fine or with both. Under sections 25 and 26 the Controller may suspend licence or revoke it with due notification.Fraudulent Publication of Electronic Signature Certificate Fraudulent Publication of Electronic Signature Certificate or making available of it knowingly for fraudulent or unlawful purpose is offence punishable with upto two years imprisonment or upto one lakh rupees fine or with both. Examiner of Electronic Evidence: Chapter XXA was inserted by the Information Technology (Amendment) Act, 2009 after Chapter XII and section 79A is the only section of this new chapter. It empowers the Central Government to notify the examiner of electronic evidence about related matters. According to this section the Central Government may specify by notification in the official gazette any department, agency of the Central Government or a State Government as an examiner of electronic evidence for the purpose of providing expert opinion on electronic evidence. This provision is in conformity with the Indian Evidence Law.

XI. The Indian Contract Act 1872[xvii]

It derives its validity from Section 10 of the Indian Contract Act, 1872 and is governed by the basic principles of contract like offer and acceptance, free consent, capacity and lawful consideration. Similarly, in the case of clickwrap agreements, the terms and conditions are provided as an offer and upon confirmation by the user by clicking on "I Agree" gives the acceptance. Section 4 of the Information Technology Act, 2000 any legal requirement of physical records that requires information to be in the typewritten form/printed, is deemed to be satisfied if it is in electronic form and accessible from future reference. In addition to that, Section 10(A) of the IT Act provides validity by recognizing the contract formation, acceptance, revocations in electronic form. After its execution, an e-contract is stored/recorded with the involved parties in electronic form as an electronic record. It shall not be unenforceable only on the ground that it is an electronic form. These provisions have been applied and upheld by the Chennai High Court in the case of *Tamil Nadu Organic v. State Bank of India* [xviii](2019). The outcome of the electronic auction was upheld and the Court said that liabilities may arise from such electronic contracts and means as long as general principles of the contract are being fulfilled and are enforceable under law as provided in the Contract Act. Therefore, e-contracts are largely legally valid and can be enforced in a court of law.

XII. The Indian Evidence Act, 1872[xix]

The Indian Evidence Act, 1872 was also amended to bring it in consonance with the electronic methods of execution of documents introduced by the IT Act. Section 65A of the Indian Evidence Act, 1872, recognizes admissibility of electronic records as evidence. It states that the contents of electronic records may be proved in accordance with the provisions of Section 65B of the said Act. Section 65B of the Indian Evidence Act, 1872 provides for acceptance of electronic evidence and further states that any information stored in an electronic mode that can be printed on a paper, stored, recorded or copied in optical or magnetic media produced by a computer shall be deemed to be a document and such documents 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. In addition to the above, section 65B(4) states that a certificate needs to be presented that recognizes the electronic record having the statement and explicates the way in which it is to be presented. Section 73A of the Evidence Act, 1872 provides that in order to ascertain whether a digital signature is that of the person by whom it purports to have been fixed, the Court may direct that person or the Controller or the Certifying Authority or any other person to apply the public key listed in the Digital Signature Certificate and verify the digital signature purported to have been affixed by that person. Section 47A of the Evidence Act, 1872 provides that where the Court is required to give its opinion on the electronic signature of any individual, the opinion of the certifying

authority which has issued the electronic signature certificate is a relevant fact. Section 85B of the Evidence Act, 1872 provides that, unless it is proved otherwise, the court shall presume that -

a. The secure electronic record has not been altered since the specific point of time to which the secure status relates;

b. The secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record.

Section 85C of the Indian Evidence Act, 1872 provides that if a digital signature is affixed to a particular document then the court shall presume that such document is true and correct.

XIII. The Companies Act, 2013[xx]

Under the provisions of the Companies Act, 2013 and the Companies (Registration Office and Fees) Rules, 2014, electronic documents must be authenticated by authorized signatories using digital signatures. As per sub-rule 5 of Rule 8 of the Companies (Registration Offices and Fees) Rules, 2014, the electronic forms required to be filed under the Act or the rules there under shall be authenticated on behalf of the company by the Managing Director or Director or Company Secretary of the Company or other Key Managerial Personnel as defined in Section 2(51) of the Act. Further, as per sub-rule 6 of Rule 8, the scanned image of documents shall be of original signed documents relevant to the e-forms or forms and the scanned image must not be left blank without bearing the signature of the authorized person.

XIV. Digital Signatures and the Indian Penal Code

Indian penal code 1860 (IPC) is in operation in India very successfully for the last 152 years. Due to development of information technology a need was felt for addition of certain provisions to take care of the new developments in the field of electronics and information technology. Thus through the Information Technology Amendment Act 2008 IPC was also amended. Section 73A has been inserted to provide the same provision as in section 47A of the Indian evidence Act. Section 464 has also been amended to provide that the said section shall be made applicable to electronic records and electronic signatures also. Section 464 deals with situations when a person is said to make false document or electronic record. Section 466 provides for forging of electronic records also. There are amendments to sections 4, 40,118,119 of IPC. [xxi]

XV. Conclusion

Protection of Digital signature under the Information Technology Act,2000, has not only proved an essential techno-legal requirement, but it has made the e-commerce-contracts are meaningful and valid as like conventional contracts . The development of information technology across the world, it is essential to reconsider the importance of "electronic signature" in the legal books as it ensures greater level of safety and security in electronic environment.

Reference

[i] Section 2(1)(p), of The Information Technology Act 2000.

[ii] Menon A, "Information Technology Act 2000-An Overview", 1st edtion. (Swami law house ,kochi,2011),p.2

[iii] S.R.Subramanya and Byung k.y.Digital Signatures, .https://www.researchgate.net/publication/3227862_Digital_signatures#fullTextFileContent, (Visited on 18.5.2023)

[iv] Ruzica Mastelic, 7 Key Benefits of Digital Signature For Your Business, https://contractbook.com/blog/digital-signature-benefits,(visied on 18.5.2020)

[v] Ministry of Corporate affairs, https://karnatakabank.com/sites/default/files/2022-10/FAQs.pdf,(Visited on 20.5.2023)

[vi] Dr. Vijaykumar Shrikrushna Chowbe, 'DIGITAL SIGNATURE : NATURE & SCOPE UNDERTHE IT ACT, 2000 - SOME REFLECTIONS', https://www.researchgate.net/publication/228226336_Digital_Signature_Nature_Scope_Under_the_IT_Act_2000_-_Some_Reflections,(Visited on 15.5/2023)

[vii] Digital Signature Certificate,https://www.certificate.digital/certificate/,(Visited on 19/5/2023)

[viii] Ibid,

[ix] Ibid,

[x] Manish Kumar Sharma, Sudhanshu Gupta, https://singhania.in/blog/e-signing-of-contract-and-documents-in-india,(Visited on 2023)

[xi] Ibid,

[xii] Section 15 of The Information Technology Act2000

[xiii] Section 43A in The Information Technology Act, 2000, https://indiankanoon.org/doc/76191164/,(visited on 20.5/2023)

[xiv] Section 64 of The Information Technology Act 2000,

[xv]73(1) of The Information Technology Act 2000.

[xvi]Digital Signature Certificates, https://www.meity.gov.in/content/digital-signature-certificates,(Visited on 19/5/2023)

[xvii] Validity and enforceability of electronic contracts and electronic signatures, https://blog.ipleaders.in/validity-and-enforceability-of-electronic-contracts-and-electronic-signatures/

[xviii]High Court of Tamilnadu 2019.

[xix] https://singhania.in/blog/e-signing-of-contract-and-documents-in-india

[xx] Ibid

[xxi] Shivadas, The Law of Digital Signature, https://www.caclubindia.com/articles/the-law-of-digital-signature-15485.asp,(Visited on 19.5.2023)