Library Progress International *Print version ISSN 0970 1052*
Vol.44 No. 3, Jul-Dec 2024: P.2303-2308 *Online version ISSN 2320 317X*

Original Article *Available online at www.bpasjournals.com*

Sustainable perspective of Information Technology Act, 2008.

Priyanka Hemal Shah[1*]

[1*]Teaching Assistant, The Maharaja Sayajirao University of Vadodara, Gujarat**.**

How to cite this article: Priyanka Hemal Shah (2024) Sustainable perspective of Information Technology Act, 2008. *Library Progress International,* 44(3), 2303-2308

ABSTRACT:
Through this research paper researcher has tried to narrate simply what is Information Technology? What is the basis of The Information Technology Act 2000? What was the need? What all are the nature and features? How it's useful in business transactions for data transfer and in maintaining privacy? What is Digital Signature? What is the role of Digital Signature? How it works? What are the Penalties involved in The Information Technology Act,2008. What are the amendments till date? In short it will be helpful to all those who want to understand IT.

Keywords - The Information Technology Act, Sustainability, digital signature, cryptography, private key, public key, E-governance, Penalties.

INTRODUCTION:

As technology evolved over time, the Indian Parliament recognized the need to revise the Act to align it with societal needs, resulting in its amendment. **Two significant amendments** were made to the **IT Act 2000** that one should know about. The Act deals with **e-commerce** and all the transactions made through it. It gives provisions for the **validity** and **recognition** of electronic records along with a **license** that is necessary to issue any digital or electronic signatures.

1. Amendment of 2008

The 2008 amendment came up with modifications to Section 66A of the IT Act, 2000. The section outlined penalties for sharing offensive messages electronically. This includes any message or information that incited hatred or compromised the integrity and security of the nation. However, the lack of clarity in defining 'offensive' messages led to unnecessary punishment of several individuals, ultimately resulting in the striking down of the section.

2. Amendment Bill 2015

In 2015, another bill was initiated to amend **Section 66A** with the aim of safeguarding the fundamental rights guaranteed to citizens by the country's Constitution. This was later accomplished by declaring it as violative of **Article 19** of the Constitution.

The Act was passed to deal with e-commerce and all the details involved with digital signatures and fulfill the following **objectives**:

- The Act seeks to **protect** all transactions done through electronic means.
- E-commerce **has reduced paperwork** used for communication purposes. It also gives legal **protection** to communication and the exchange of information through electronic means.
- It **protects** the digital signatures that are used for any sort of legal authentication.
- It **regulates** the activities of intermediaries by keeping a check on their powers.
- It **defines** various offences related to data privacy of citizens and hence protects their data.
- It also regulates and protects the sensitive data stored by social media and other electronic intermediaries.
- It provides **recognition** to books of accounts kept in electronic form regulated by the Reserve Bank of India Act, 1934.

1. Features of Information Technology Act, 2000

Following are the features of the Act:

- The Act is based on the Model Law on **e-commerce** adopted by **UNCITRAL.**
- It has extra-territorial **jurisdiction**.
- It **defines** various terminologies used in the Act like cyber cafes, computer systems, digital signatures, electronic records, data, asymmetric cryptosystems, etc under Section 2(1).

- It **protects** all the **transactions** and contracts made through electronic means and says that all such contracts are valid. (Section 10A**)**
- It also gives **recognition** to digital signatures and provides methods of authentication.
- It contains **provisions** related to the **appointment** of the Controller and its powers.
- It recognizes foreign certifying authorities (Section 19**).**
- It also provides various **penalties** in case a computer system is damaged by anyone other than the owner of the system.
- The Act also provides provisions for an **Appellate Tribunal** to be established under the Act. All the appeals from the decisions of the Controller or other Adjudicating officers lie to the Appellate tribunal. The limitation period for filing an appeal in the National Company Law Appellate Tribunal (NCLAT) is 30 days, which can be extended by up to 15 days if sufficient cause is shown, though **45 days** in toto.
- **Section 57** - The person who was wronged must file an appeal with the **Cyber Appellate Tribunal** within **twenty-five days** of receiving a copy of the order from the Controller or adjudicating officer. The appeal must be submitted in the prescribed format and include any applicable fees. If the Cyber Appellate Tribunal determines that there was adequate justification for the appeal's late filing, it may consider the appeal after the allotted time has passed.
- Further, an appeal from the tribunal lies with the **High Court**.
- The Act describes various **offences** related to data and defines their **punishment**.
- It provides circumstances where the intermediaries are not held liable even if the privacy of data is breached.
- A **cyber regulation** advisory committee is set up under the Act to advise the Central Government on all matters related to e-commerce or digital signatures.
- The Act permits companies to serve as certifying authorities and issue digital certificates. It empowers the Indian Government to issue notices on the internet through **e-governance**.
- Promotes the expansion and foster innovation and entrepreneurship in the Indian IT/ITES sector.

Electronic records and signatures

The Act defines **electronic records** under **Section 2(1)(t)**, which includes any data, image, record, or file sent through an electronic mode. According to **Section 2(1)k(ta)**, any signature used to authenticate any electronic record that is in the form of a digital signature is called an electronic signature. However, such authentication will be affected by asymmetric cryptosystems and hash functions as given under **Section 3** of the Act.

Key differences between digital signature and electronic signature[1]

Sr.No.	Basis	Digital Signature	Electronic Signature
1	Meaning	It involves public key cryptography to sign a message.	It's just a representation of a person in from of an electronic picture of handwritten sign, symbol or voice print etc.
2	Scope	It's an electronic signature	The term 'electronic signature' is broader than digital signature. An electronic signature is not necessarily a digital signature,
3	Security	More secure than electronic signature.	Less secure than digital signature, it does not have secure coding.
4	International Standards	Accepted globally because they do comply with the international standards of security.	It's not regulated like digital signatures. Each vendor must make his own standards.
5	Copying, Tampering with or Alteration	It cannot be copied, tempered or altered.	It can be copied, tempered or altered.

Section 3A further gives the conditions of a reliable electronic signature. These are:

- If the signatures are linked to the signatory or authenticator, they are considered reliable.
- If the signatures are under the control of the signatory at the time of signing.
- Any alteration to such a signature must be detectable after fixation or alteration.
- The alteration done to any information which is authenticated by the signature must be detectable.
- It must also fulfill any other conditions as specified by the Central Government.
- The **government** can anytime make rules for electronic signatures according to Section 10 of the Act.

ELECTRONIC GOVERNANCE[2] –

Electronic governance, often known as e-governance, refers to the use of ICT (information and communications technology) in government operations. Therefore, e-Government is essentially a step towards **SMART governance**, which stands for **straightforward, moral, responsible, responsive, and transparent governance.**

What is SMART Governance:

Straightforward refers to streamlining governmental policies and procedures and avoiding convoluted ICT application procedures, all of which contribute to the provision of a user-friendly government.

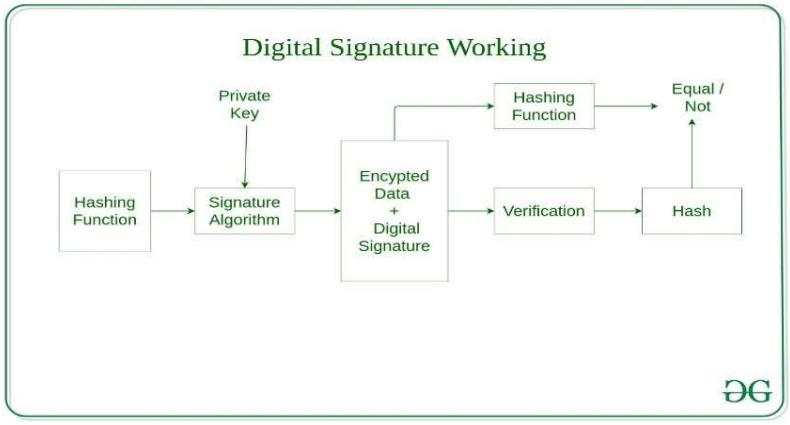
Moral: this refers to the introduction of a new administrative and political structure that uses technological interventions to increase the effectiveness of different government agencies.

Responsible: To guarantee public sector employees' accountability, create efficient information management systems and additional performance assessment tools.
Responsive: The system is more responsive when processes are streamlined to expedite them.

Transparent means that government functions and procedures are made available to the public through the provision of information on websites or other public portals.[3]

Provisions Applicable to E - Governance
Electronic documents are recognised legally by **Section 4** of the Indian IT Act, 2000.If paper records are made available electronically and are accessible enough to be used for future reference, they are equivalent to electronic records.
Section 5 gives digital signatures the same legal standing as handwritten signatures. Digital signatures attached in the way specified by the Central Government will guarantee the authenticity of these digital signatures. The goal of **Section 6** is to get rid of red tape and encourage the government and its agencies to employ digital signatures and electronic records. It facilitates the online submission of paperwork with government agencies, the granting of licenses and permissions, and the collection and payment of funds. To comply with the legal obligation for record retention, **Section 7** permits the retention of electronic records that are comparable to documents on paper.
Section 8 states that the publication of rules, regulations, and notices in the Electronic Gazette should likewise be legally recognised in the case of the traditional printed gazette as well as the electronic one. For this reason, any rule, regulation, by law, or notification that needs to be published in the Official Gazette can be published electronically and still fulfil the requirement.
Additionally, the date of publication for an Official Gazette that is published in both print and electronic format will be the date the publication of the original Official Gazette, regardless of format.
However, no one can demand that returns or records be filed electronically because the government requires time to build up the infrastructure necessary to do electronic transactions in the future according to **Section 9**.
The authority to establish regulations regarding digital signatures, including the format, type, and method of affixing them, as well as the process by which they must be processed, has been granted to the Central Government under **Section 10**.[4]

Digital Signature –
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 of Information Technology Act.
A digital signature is a **mathematical technique** used to validate the **authenticity** and **honesty** of a digital document, message or software. It's the digital equivalent of a handwritten signature or stamped seal, but it offers far more inherent security.
A digital signature is intended to solve the problem of **tampering** and **impersonation** (when someone pretends to be another person) 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 many countries, including the U.S., digital signatures are considered legally binding in the same way as traditional handwritten document signatures.
Role of Digital Signature
Digital signatures are based on public key cryptography, also known as asymmetric cryptography**.** Using a public key algorithm -- such as Rivest-Shamir-Adleman, or RSA -- two keys are generated, creating a mathematically linked pair of keys: one private and one public.
Digital signatures work through **public key** cryptography's two mutually authenticating cryptographic keys. For encryption(encoding) and decryption(decoding), the person who creates the digital signature uses a private key to encrypt signature-related data. The only way to decrypt that data is with the signer's public key.
If the recipient can't open the document with the signer's public key, that indicates there's a problem with the document or the signature. This is how digital signatures are authenticated.



Digital certificates, also called **public key certificates,** are used to verify that the public key belongs to the issuer. Digital certificates contain the public key, information about its owner, expiration dates and the digital signature of the certificate's issuer. Digital signature technology requires all parties to trust that the person who creates the signature image has kept the private key secret. If someone else has access to the private signing key, that party could create fraudulent digital signatures in the name of the private key holder.

1.1.

1.1. What are the benefits of digital signatures?

Digital signatures offer the following benefits:

1. **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.
2. **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.
3. **Globally accepted and legally compliant.** The public key infrastructure (PKI) 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.
4. **Time savings.** Digital signatures simplify the time-consuming processes of physical document signing, storage and exchange, enabling businesses to quickly access and sign documents.
5. **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.
6. **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.
7. **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.[5]

Process of creation of Digital Signature

To create a digital signature, signing software -- such as an email program -- is used to provide a one-way hash of the electronic data to be signed.

A **hash** is a fixed-length string of letters and numbers generated by an algorithm (mathematical code). The digital signature creator's private key is used to encrypt the hash. The encrypted hash -- along with other information, such as the hashing algorithm (process) -- is the digital signature.

The reason for **encrypting** the hash instead of the entire message or document is because a hash function can convert an uninformed input into a fixed-length value, which is usually much shorter. This saves time, as hashing is much faster than signing.

The value of a hash is unique to the hashed data. Any change in the data -- even a modification to a single character -- results in a different value. This attribute enables others to use the signer's public key to decrypt the hash **to validate** the **integrity** of the data.

If the decrypted hash matches a second computed hash of the same data, it proves that the data hasn't changed since it was signed. But, if the two hashes don't match, the data has either been tampered with in some way and is compromised or the signature was created with a private key that doesn't correspond to the public key presented by the signer. This signals an issue with authentication.

Penalties under Information Technology Act, 2000

Penalties under Information Technology Act, 2000.

The Act provides penalties and compensation in the following cases:

1.1. Penalty for damaging a computer system -

If a person other than the owner uses the computer system and damages it, he shall have to pay all such damages by way of compensation (Section 43**).** Other reasons for penalties and compensation are:

- If he downloads or copies any information stored in the system.
- Introduces any virus to the computer system.
- Disorganize the system.
- Denies access to the owner or person authorized to use the computer.
- Tampers or manipulates the computer system.
- Destroys, deletes or makes any alteration to the information stored in the system.
- Steals the information stored therein.
- Animation of witnesses.
- Review decisions.
- Dismissal of any application.
- Penalty applicable for "damage to computer/ computer system"

It includes a maximum **3-year jail** sentence or a fine of **up to Rs. 2. lakh** liable to compensate damages up to a **maximum of Rs. 1. Crore** to the impacted individual.

Offences and their punishments under Information Technology Act, 2000.[6]

Sr.no.	Offences	Section	Punishment
1	Tampering with the documents stored in a computer system	Section 65	Imprisonment of 3 years or a fine of Rs. 2 lakhs or both.
2	Offences related to computers, or any act mentioned in **Section 43.**	Section 66	Imprisonment of 3 years or a fine that extends to Rs. 5 lakhs or both.
3	Punishment for sending offensive messages	Section 66A	Imprisonment up to 3 years & with fine.
3	Receiving a stolen computer source or device dishonestly	Section 66B	Imprisonment for 3 years or a fine of Rs. 1 lakh or both.
4	Identity theft	Section 66C	Imprisonment of 3 years or a fine of Rs. 1 lakh or both
5	Cheating by execution	Section 66D	Either imprisonment for 3 years or a fine of Rs. 1 lakh or both.
6	Violation of privacy	Section 66E	Either imprisonment of up to 3 years or a fine of Rs. 2 lakhs or both
7	Cyber terrorism	Section 66F	Life imprisonment
8	Transmitting obscene material in electronic form.	Section 67	Imprisonment of 5 years and a fine of Rs. 10 lakhs.
9	Transmission of any material containing sexually explicit acts	Section	Imprisonment of 7

	through an electronic mode.	67A	years and a fine of Rs. 10 lakhs.
10	Depicting children in sexually explicit form and transmitting such material through electronic mode	Section 67B	Imprisonment of 7 years and a fine of Rs. 10 lakhs.
11	Failure to preserve and retain the information by intermediaries	Section 67C	Imprisonment for 3 years and a fine.