Information Technology Act, 2000

Brief Background of the Information Technology Act, 2000

The IT Act was enacted on 17th May 2000 primarily to provide **legal recognition for electronic transactions and facilitate e-commerce**. India became the 12th nation in the world to adopt cyber laws by passing the Act. When the IT Act was introduced, it was the **first** information technology **legislation** introduced in India. The IT Act is based on **Model law on e-commerce adopted by UNCITRAL of United Nations organization**.

In between 2003 and 2010, several amendments were made in the Act. Out of the total 94 sections in the Act, about 76 sections have been amended by addition, insertion, substitution, or omission of the provisions of the Act. About 30 new sections like 3A, 6A, 7A etc have been inserted, in addition to about 15 new definition clauses inserted in section 2. In this way, the total number of sections has gone to 120 in the Act. The amended Act is expected to create a paradigm shift in data protection and privacy regime in India as it provides for establishing **a self-regulation framework for maintenance of reasonable security practices and procedures for protecting "sensitive personal data or information"**, It also has provisions for **adjudication related to data protection and privacy (civil liabilities)** and provides for **criminal prosecution** visà- vis data protection and privacy.

The IT Act 2000 was enacted to ***provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as "electronic commerce"***, which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate ***electronic filing of documents with*** the Government agencies and further to ***amend*** the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.

The Act is **administered by** the Controller, Deputy Controllers and Assistant Controllers and the **disputes relating to Civil wrongs** are decided by the Controller and Adjudicating Officer and the **appeal** against them lies to the Cyber Appellate Tribunal and the High Court. The offences under this Act are investigated by the Police Officer not below the rank of Inspector and are decided by the Court of 1st Class Magistrate, Sessions Court and the High Court.

In modern enterprises, most of the critical information is input, processed and stored in computers even in case of small and medium enterprises. Hence, the regulatory provisions and impact of this data being available electronically, the risks of it being misused and regulatory provisions of such non-compliance has to be understood and also communicated to the client to mitigate the control weaknesses and ensure compliance.

Objectives of the Act

The Objectives of the Act are given as follows:

1. To grant **legal recognition for transactions carried out by means of electronic data interchange** and other means of electronic communication commonly referred to as "electronic commerce" in place of paper based methods of communication;

2. To give **legal recognition to Digital signatures** for authentication of any information or matter, which requires authentication under any law;

3. To facilitate **electronic filing of documents** with Government departments;

4. To facilitate **electronic storage of data**;

5. To facilitate and give legal sanction to **electronic fund transfers between banks and financial institutions**;

6. To give legal recognition for **keeping of books of accounts by banker's in electronic form**; and

7. To **amend** the Indian Penal Code, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891, and the Reserve Bank of India Act, 1934.

1. Short title, extent, commencement and application

(1) This Act may be called the Information Technology Act, 2000.

(2) It shall extend to the ***whole of India*** and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder ***committed outside India by any person***

(3) It shall come into force on such date as the Central Government may, by notification, appoint and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the commencement of that provision.

(4) Nothing in this Act shall apply to, —
(a) a ***negotiable instrument (other than a cheque)*** as defined in section 13 of the Negotiable Instruments Act, 1881;
(b) a ***power-of-attorney*** as defined in section 1A of the Powers-of-Attorney Act, 1882;
(c) a ***trust*** as defined in section 3 of the Indian Trusts Act, 1882;
(d) a ***will*** as defined in clause (h) of section 2 of the Indian Succession Act, 1925 including any other testamentary disposition by whatever name called;
(e) any ***contract*** for the sale or conveyance of immovable property or any interest in such property;
(f) any such class of documents or transactions as may be notified by the Central Government in the Official Gazette.

Extent

The operation of this Act has been extended to the **(a) whole of India and (b) outside India.**

Outside India
Clause (2) of article 245 of the Constitution of India lays down that a law made by the Parliament shall not be deemed to be invalid on the ground that it would have extra-territorial operation. For eg: **Section 75 of IT Act**

Section 75 of IT Act

75. Act to apply for offence or contravention committed outside India:-

(1) Subject to the provisions of sub- section (2), the provisions of this Act shall apply also to ***any offence or contravention committed outside India by any person irrespective of his nationality***.

(2) For the purposes of sub- section (1), this Act shall apply to an offence or contravention committed outside India by any person if the act or conduct constituting the offence or contravention ***involves a computer, computer system or computer network located in India***

Section 75 of this Act lays down three conditions:-

(i) Offence on contravention of this Act is committed *outside India*;
(ii) It is committed by any person *irrespective of his nationality*; and
(iii) It *involves a computer, computer system or computer network located in India*

Think Through

A question may arise in case of acts or omission which may amount to an offence in India, but may be a lawful act or omission in other countries. For instance – Section 67

Documents or transaction to which the Act shall not apply

Digital Signature and Electronic Signature

Section 3 Authentication of Electronic Records:

(1) Subject to the provisions of this section, ***any subscriber*** may ***authenticate an electronic record by affixing his Digital Signature.***

(2) The authentication of the electronic record shall be effected by the use of ***asymmetric crypto system and hash function*** which envelop and transform the initial electronic record into another electronic record.
Explanation -
For the purposes of this sub-section, "Hash function" means an algorithm mapping or translation of one sequence of bits into another, generally smaller, set known as "Hash Result" such that an electronic record yields the same hash result every time the algorithm is executed with the same electronic record as its input making it computationally infeasible
(a) to derive or reconstruct the original electronic record from the hash result produced by the algorithm;
(b) that two electronic records can produce the same hash result using the algorithm.

(3) Any person by the ***use of a public key of the subscriber*** can verify the electronic record.

(4) ***The private key and the public key are unique to the subscriber and constitute a functioning key pair***.

Analysis of the Section:

What is an electronic record?

Section 2(t) – Electronic Record

(t) "Electronic Record" means data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche

According to the definition of this term, when the following record ie (i) data (ii) record (iii) data generated (iv) image or sound stored, received or sent in an electronic form is kept in (a) electronic form (b) micro film (c) computer generated micro fiche, it is called Electronic Record.

Authentication of Electronic Record by Subscriber by Affixing his Digital Signature
The opening words of this sub-section begins with the words ***"subject to the provisions of this section"***, which means that every authentication of electronic record by a subscriber must ***conform*** to the ***requirements of other sub-sections of this section*** and if it does not conform to the said requirement, it would not be legal and may be declared so by the High Court under its power of judicial review.

The requirements of authentication of electronic record by a subscriber in all the sub-sections of Section 3 are as follows:

(i) ***Any subscriber may authenticate an electronic record by affixing his Digital Signature.***
(ii) ***It shall be affected by the use of (a) asymmetric crypto system and (b) hash function.***
(iii) ***Any person by the use of a public key of the subscriber can verify the electronic record.***
(iv) ***The private key and the public key are unique to the subscriber.***

What is Digital Signature

Section 2(p) – Digital Signature

(p) "Digital Signature" means ***authentication of any electronic record by a subscriber***

by means of an electronic method or procedure in accordance with the provisions of section 3;

It means authentication of any electronic record by a subscriber by means of –

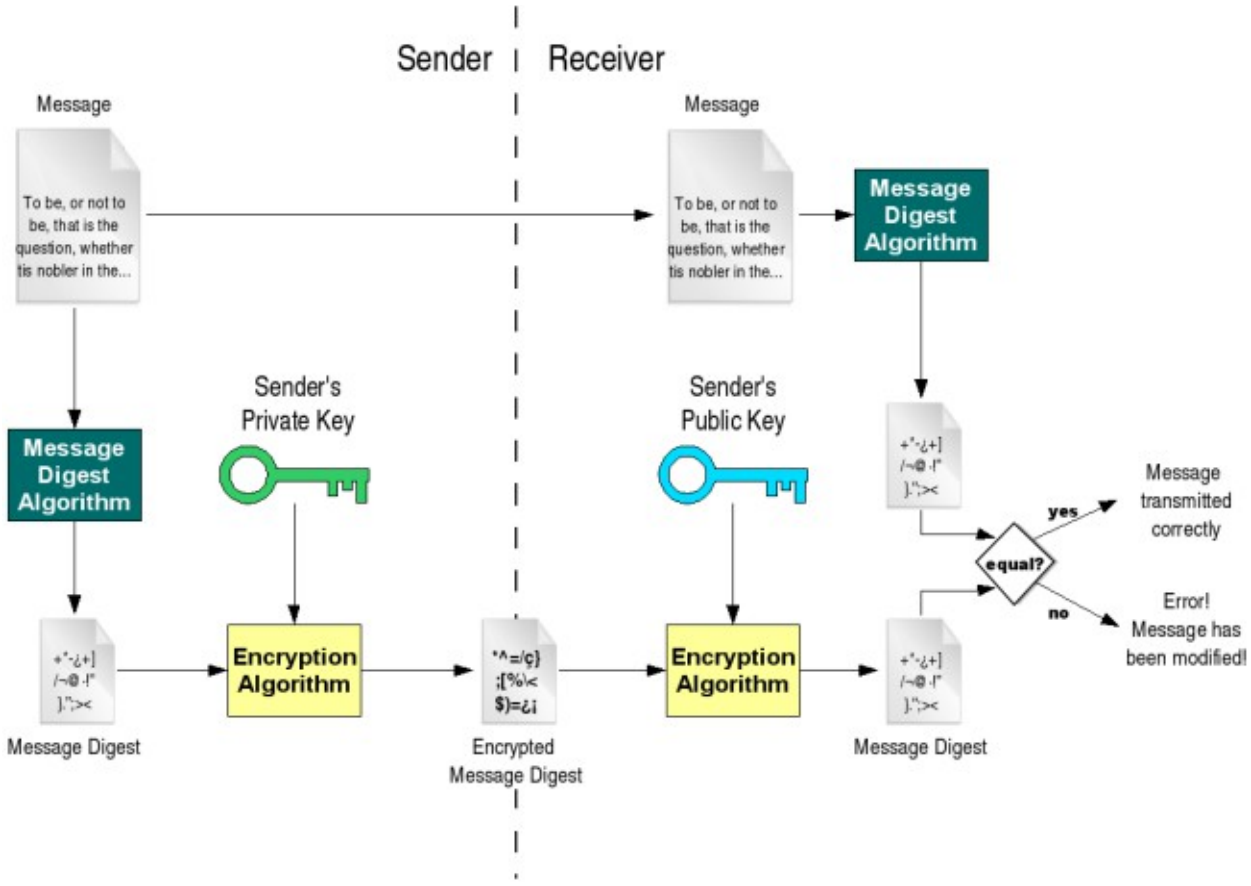
(i) ***An electronic method***
(ii) ***Procedure in accordance with the provisions of Section 3***

Functioning of Digital Signature
Digital Signature is used to ***verify the authenticity of the document*** and the ***identity of the sender or originator***.

The document or message is encrypted with the originator's private key to generate the signature. The document is thereafter sent to the addressee alongwith the signature. The addressee decrypts signature using the originator's public key and if the result matches with the document received from the originator, the addressee can be sure that the document was sent by the same originator and that it was not changed during the transmission.

To reduce the processing load, the ***hash function*** is used. The hash function operates on large documents as it generate message digest of fix smaller length. It has the property that any change in the original document will cause the digested document to be different. This is highly secure and protected way of sending document with digital signature.

The following chart illustrates the creation and transmission of digitally signed document -



The above chart reveals that the digital signature is created in two distinct steps:

First, the electronic record is converted into a message digest by using a mathematical function known as "hash function" which digitally freezes the electronic record thus ensuring the integrity of the content of the intended communication contained in the electronic record. Any tampering with the contents of the electronic record will immediately invalidate the digital signature.

Secondly, the identity of the person affixing the digital signature is authenticated through the use of a private key which attaches itself to the message digest and which can be verified by anybody who has the public key corresponding to such private key. This will enable anybody to verify whether the electronic record is retained intact or has been tampered with since it was so fixed with the digital signature. It will also enable a person who has a public key to identify the originator of the message.

Other provisions / definitions

Asymmetric Crypto System

Section 2(f) – Asymmetric Crypto System

(f) "Asymmetric Crypto System" means ***a system of a secure key pair*** consisting of a private key for creating a digital signature and a public key to verify the digital signature;

It means a system of a secure key pair consisting of –

(a) A private key for creating digital signature; and

(b) A public key to verify the digital signature.

The private key is used for creating a digital signature and the public key is to be used to verify the digital signature. The system of such a secure key pair is known as asymmetric crypto system

In an ACS, key pair means a private key and its mathematically related public key which are so related that private key creates and public key verifies the digital signature.

The Controller shall ensure that the secrecy and security of the digital signature are assured. He shall also maintain a computerized database of all public keys in such a manner that such database and the public keys are available to any member of the public.

Key pair

Section 2(x) – Key pair

(x) "Key Pair", in an asymmetric crypto system, ***means a private key and its mathematically related public key***, which are so related that the public key can verify a digital signature created by the private key

Private key

Section 2(zc) – Private key

(zc) “Private Key" means the key of a key pair ***used to create a digital signature***

Public key

Section 2(zd) – Public key

(zd) “Public Key" means the key of a key pair ***used to verify a digital signature*** and listed in the Digital Signature Certificate

It consist of 2 keys viz

(a) a private key; and

(b) its mathematically related public key.

They are related with each other i.e the private key creates a digital signature and the public key verifies the digital signature. They key paid must be understood with reference to asymmetric crypto system. Cryptography is a discipline which transforms data into another version so as to hide its information or to prevent the misuse of information.

Generally, the validity period for the subscribers private key has been fixed at 3 years.

Originator

Section 2(za) – Originator

(za) Originator" means a person who sends, generates, stores or transmits any electronic message or causes any electronic message to be sent, generated, stored or transmitted to any other person ***but does not include an intermediary;***

Verify

Section 2(za) – Originator

(zh) "Verify" in relation to a digital signature, electronic record or public key, with its grammatical variations and cognate expressions means to determine whether

(i) *the initial electronic record was affixed with the digital signature by the use of private key corresponding to the public key of the subscriber;*

(ii) *the initial electronic record is retained intact or has been altered since such electronic record was so affixed with the digital signature.*

The authentication of electronic record is to be done by the Subscriber. What do you mean by a Subscriber? How to become a Subscriber?

Section 2(zg) – Subscriber

(zg) "Subscriber" means a person in whose name the Digital Signature Certificate is issued;

License granted

A person in whose name the Digital Signature Certificate is issued shall be known as a Subscriber

According to Section 36, while issuing a DSC, the certifying authority shall certify, inter-alia, that the subscriber holds the private key corresponding to the public key, listed in the DSC and that the subscriber's private key and public key constitute a functioning key pair.

The subscriber shall be deemed to have accepted the DSC, if he publishes the DSC in the manner laid down under section 41 (Acceptance of DSC)

Secure Electronic Record

Section 14 – Secure Electronic Record

Where any ***security procedure*** has been applied to an electronic record at a specific point of time, then such record ***shall be deemed to be a secure electronic record*** *from such point of time to the time of verification*

What is a security procedure?

Section 2(zf) – Security Procedure

(zf) "Security Procedure" means the security procedure ***prescribed under section 16*** *by the Central Government;*

This section deals with the application of security procedure to an electronic record. The security procedure is based on ***Cryptography***. It is a mathematical science used to secure the confidentiality and authentication of data by replacing it with a transformed version that can be reconverted into the original data by someone holding the proper cryptographic algorithm and key. It can encrypt the message and thereafter the receiver of the electronic message can decrypt making the information readable once again.

For example: If the characters are to be shifted by 3 places then:

Information: *A* *B* *C*
Encrypt: *D* *E* *F (using Cryptography)*

There are two basic types of Cryptographic Systems –

(i) Symmetric – The Symmetric system is based on a single secret key which is shared by the parties engaging in secure communication.

(ii) Asymmetric – The Asymmetric system is based on a pair of keys one private and other public (also refer Section 3 above)

Section 3A Electronic Signature:

1) ***Notwithstanding anything contained in section 3***, but subject to the provisions of subsection, a subscriber may authenticate any electronic record ***by such electronic signature or electronic authentication technique which*** -
a) *is considered reliable*; ***AND***
b) *may be specified in the Second Schedule*

2) For the purposes of this section any electronic signature or electronic authentication technique ***shall be considered reliable if*** -
a) the signature creation data or the authentication data are, within the context in which they are used, *linked to* the signatory or , as the case may be, the authenticator and of no other person;
b) the signature creation data or the authentication data were, at the time of signing, *under the control of* the signatory or, as the case may be, the authenticator and of no other person;
c) any alteration to the *electronic signature* made after affixing such signature is detectable
d) any alteration to the *information* made after its authentication by electronic signature is detectable; and
e) it fulfills such other conditions which may be prescribed.

3) The Central Government may prescribe the procedure for the purpose of ascertaining whether electronic signature is that of the person by whom it is purported to have been affixed or authenticated

4) The Central Government may, by notification in the Official Gazette, add to or omit any electronic signature or electronic authentication technique and the procedure for affixing such signature from the second schedule

Provided that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable

5) Every notification issued under sub-section (4) shall be laid before each House of Parliament

What is an Electronic signature?

Section 2(ta) – Electronic Signature

(ta) "electronic signature" ***means*** authentication of any electronic record by a subscriber by means of ***the electronic technique specified in the second schedule*** ***and includes digital signature***

Section 3A deals with electronic signature whereas section 3 deals with digital signature. According to the definition of 'electronic signature', the term 'electronic signature' includes the term 'digital signature', whereas the term 'digital signature' does not include the term 'electronic signature'. Given this, ***the term 'electronic signature' is a wider concept***.

The authentication technique of both, digital or electronic signature is different. According to section 3, any subscriber may authenticate an electronic record by affixing his digital signature. It shall be effected by the use of *(i) asymmetric crypto system and (ii) hash function*. Any person by the use of the public key of the subscriber can verify the electronic record. ***Whereas, according to Section 3A, the authentication technique of electronic signature is different. The said technique may be made available in the second schedule of this Act by the Central Government.***

Second Schedule

ELECTRONIC SIGNATURE OR ELECTRONIC AUTHENTICATION TECHNIQUE AND PROCEDURE

Sr No	Description	Procedure
(1)	(2)	(3)

Such procedure has still not been laid down in the Second schedule. Such electronic authentication technique shall be added to this section by the Central Government by notification in the Official Gazette, and the procedure for affixing such signature shall be laid down in the Second Schedule. Such powers have been given to the Central Government. The proviso under sub-section (4) provides that no electronic signature or authentication technique shall be specified in the Second Schedule unless such signature or technique is reliable.

When is an electronic signature or electronic authentication technique be considered reliable –

When is an electronic signature or electronic authentication technique be considered reliable

Key difference between electronic signature and digital signature –

A digital signature, often referred to as advanced or standard electronic signature, falls into a sub-group of electronic signatures that provides the highest levels of security and universal acceptance. Digital signatures are based on Public Key Infrastructure (PKI) technology, and guarantee signer identity and intent, data integrity, and the non-repudiation of signed documents. The digital signature cannot be copied, tampered with or altered. In addition, because digital signatures are based on standard PKI technology, they can be validated by anyone without the need for proprietary verification software.

On the other hand, an electronic signature is a proprietary format (there is no standard for electronic signatures) that may be a digitized image of a handwritten signature, a symbol, voiceprint, etc., used to identify the author(s) of an electronic message. An electronic signature is vulnerable to copying and tampering, and invites forgery. In many cases, electronic signatures are not legally binding and will require proprietary software to validate the e-signature.

Secure Electronic Signature

Section 15 - Secure Electronic Signature

An electronic signature shall be deemed to be a secure electronic signature if -
(i) The signature creation data, at the time of affixing signature, was under the exclusive control of signatory and no other person; and
(ii) The signature creation data was stored and affixed in such exclusive manner as may be prescribed.

Explanation - In case of digital signature, the "signature creation data" means the private key of the subscriber

Section 15 requires that an information or matter in an electronic form shall be “deemed to be secure” if the requirement mentioned in clauses (a) and (b) are met.

The parties may either ***agree to lay down their own security procedure*** or ***may agree to implement the security procedure laid down under the rules***. ***If the parties agree to apply their own security procedure, then the conditions laid down under section 15 shall be applicable.***

Section 16 – Security procedures and practices

The Central Government, may, *for the purposes of section 14 and 15*, ***prescribe the security procedure and practices***:

Provided that in prescribing such security procedures and practices, the Central Government ***shall have regard to*** –

- *the commercial circumstances,*
- *nature of transaction*
- *and such other related factors as it may consider appropriate.*

Section 16 provides for the power of the Central Government to prescribe the security procedure in respect of secure electronic records and secure digital signatures. In doing so, the Central Government shall take into account various factors like *nature of the transaction, level of sophistication of the technological capacity of the parties, availability and cost of alternative procedures, volume of similar transactions entered into by other parties etc*.

The Information Technology (Security Procedure) Rules, 2004 have laid down rules for security procedure.

Electronic Governance

Section 4 provides for ***"legal recognition of electronic records"*** also known as ***'E-Governance'***. It provides that where any law requires that any information or matter should be in the typewritten or printed form then such requirement ***shall be deemed to be satisfied if it is in an electronic form***. This section is as follows:

Section 4 - Legal Recognition of Electronic Records

Where any law provides that information or any other matter ***shall be in writing or in the typewritten or printed form***, then, notwithstanding anything contained in such law, such requirement shall be ***deemed to have been satisfied*** if such information or matter is

(a) rendered or made available in an electronic form; and
(b) accessible so as to be usable for a subsequent reference

Why law requires the submission of the documents in writing

The reason could be as follows –

- There should be some tangible evidence of the existence of the intention of the parties to bind themselves;
- It would bring the rights and liabilities of the parties in existence in those cases where writing is required for validity purposes;
- It would facilitate subsequent audit for accounting, tax, regulatory or evidential purpose

Which law requires the submission of the documents in writing

The following are the examples of such law –

Act	Earlier Law	Amended Law
Evidence Act	Entries in the books of account	Entries in the books of account ***including those maintained in an electronic form***
Right to Information Act, 2005		Every public authority shall maintain all its records duly catalogued and indexed in a manner and the form which facilitates the right to information under this Act and ***ensure that all records that are appropriate to be computerized are, within a reasonable time and subject to availability of resources, computerized and connected through a network***

		all over the country on different system so that access to such records is facilitated

Electronic form

Section 2(r) – Electronic Form

(r) "Electronic Form" with reference to information means any information generated, sent, received or stored in media, magnetic, optical, computer memory, micro film, computer generated micro fiche or similar device;

Access

Section 2(a) – Access

(a) "Access" with its grammatical variations and cognate expressions means ***gaining entry into, instructing or communicating with*** the logical, arithmetical, or memory function resources of a computer, computer system or computer network;

The term “access” has been defined in clause (a) of Section 2 to mean any kind of entry of information or matter into the computer by input support devices shall be known as ‘access’ into computer.

If conditions at clauses (a) and (b) of section 4 are satisfied, then such electronic record shall be known as legally recognized record.

Section 5 - Legal recognition of Electronic Signature

Where any law provides that information or any other matter ***shall be authenticated by affixing the signature or any document should be signed or bear the signature of any person*** then, notwithstanding anything contained in such law, such requirement ***shall be deemed to have been satisfied, if such information or matter is authenticated by means of electronic signature affixed in such manner as may be prescribed by the Central Government.***

Explanation -
For the purposes of this section, "Signed", with its grammatical variations and cognate expressions, shall, with reference to a person, mean affixing of his hand written signature or any mark on any document and the expression "Signature" shall be construed accordingly.

Section 4 deals with legal recognition of electronic records whereas this section deals with legal recognition of electronic signature.

Where the law requires that certain documents in writing and must be signed by its author or by all the parties by putting their signatures, then in addition to the traditional handwritten signature or thumb impression, the said section provides that the requirement of law for affixing the signature would be deemed to be satisfied, if the document is authenticated by means of using the new technology ie by affixing the electronic signature

Affixing electronic signature

Section 2(d) – Affixing Electronic Signature

(d) "Affixing Electronic Signature" with its grammatical variations and cognate expressions means ***adoption of any methodology or procedure by a person for the purpose of authenticating an electronic record by means of Electronic Signature;***

Section 6 - Use of Electronic Records and Electronic Signature in Government and its Agencies

(1) Where any law provides for -
(a) the ***filing*** of any form, application or any other document with any office, authority, body or agency owned or controlled by the appropriate Government in a particular manner;
(b) the ***issue or grant*** of any license, permit, sanction or approval by whatever name called in a particular manner;
(c) the ***receipt or payment of money*** in a particular manner, then,
notwithstanding anything contained in any other law for the time being in force, such requirement ***shall be deemed to have been satisfied*** if such filing, issue, grant, receipt or payment, as the case may be, is ***effected by means of such electronic form as may be prescribed by the appropriate Government***.

(2) The appropriate Government may, for the purposes of sub-section (1), by rules, prescribe -
(a) the ***manner and format*** in which such *electronic records shall be filed, created or issued*;
(b) the ***manner or method of payment*** of any *fee or charges* for filing, creation or issue any electronic record under clause (a).

Section 6 lays down the foundation of Electronic Governance. It provides that the filing of any form, application or other documents, creation, retention or preservation of records, issue or grant of any license or permit or receipt or payment in Government offices and its agencies may be done through the means of electronic form. The ***appropriate Government*** office has the power to prescribe the manner and format of the electronic records and the method of payment of fee in that connection.

Think Through

The heading of section 6 has used two terms *viz.* Electronic Records and Electronic Signature,

however, in the whole body of sub-section (1), the two terms have not been used.

Where a statue declares that the legal requirement of a document in writing shall be deemed to have been satisfied, if the information is made available in an electronic form, it shall have to be treated as so during the entire course of the proceedings.

Appropriate Government

Section 2(e) - Appropriate Government

(e) "Appropriate Government" means as respects any matter -
(i) enumerated in List II of the Seventh Schedule to the Constitution;
(ii) relating to any State law enacted under List III of the Seventh Schedule to the Constitution, the State Government
and in any other case, the Central Government;

It is pertinent to note that the Central Government has issued ***'Information Technology (Use of Electronic Records and Digital Signatures) Rules, 2004'*** for the purpose of prescribe the manner and format of the electronic records and the method of payment of fee. Rule 3 of the said Rules deals with filing of any form, application or any other document. Rule 4 of the said Rules deals with issue or grant of any license, permit, sanction or approval. Rule 5 of the said Rules deals with receipt or payment of money ***(Rule 5 provides that payment or receipt may be made by a cheque in the electronic form)***.

Section 81A - Application of the Act to Electronic cheque and Truncated cheque

(1) The provisions of this Act, for the time being in force, ***shall apply to***, or in relation to, ***electronic cheques and the truncated cheques*** subject to such modifications and amendments as may be necessary for carrying out the purposes of the Negotiable Instruments Act, 1881 (26 of 1881) by the Central Government, in consultation with the Reserve Bank of India, by notification in the Official Gazette.

(2) Every notification made by the Central Government under subsection (1) shall be laid, as soon as may be after it is made, before each House of Parliament, while it is in session, for a total period of thirty days which may be comprised in one session or in two or more successive sessions, and if, before the expiry of the session immediately following the session or the successive sessions aforesaid, both houses agree in making any modification in the notification or both houses agree that the notification should not be made, the notification shall thereafter have effect only in such modified form or be of no effect, as the case may be; so, however, that any such modification or annulment shall be without prejudice to the validity of anything previously done under the notification.

Explanation : For the purpose of this Act, the expression "electronic cheque" and "truncated cheque" shall have the same meaning as assigned to them in section 6 of the Negotiable Instruments Act 1881 (26 of 1881).

The provision of this Act shall apply to the electronic cheques or truncated cheque subject to such modifications as the Central Government may notify, after consultation with RBI. Such notification must be placed in both the house of Parliament for 30 days. If both the houses agree for modification in the notification, in such a case the modified notification will be applicable

Think Through

According to Section 1(4) of this Act, the negotiable instrument (other than a cheque) shall not be applicable to this Act.

Section 7 - Retention of Electronic Records

(1) Where any law provides that documents, records or information shall be retained for any specific period, then, that requirement ***shall be deemed to have been satisfied if*** such documents, records or information are ***retained in the electronic form***, -
(a) the information contained therein ***remains accessible*** *so as to be usable for a subsequent reference*;
(b) the electronic record is retained in the ***format*** *in which it was originally generated, sent or received* or in a format which can be *demonstrated* to represent accurately the information originally generated, sent or received;
(c) the details which will ***facilitate the identification of the origin, destination, date and time of dispatch or receipt*** of such electronic record are available in the electronic record:

However, this clause does not apply to any information which is automatically generated solely for the purpose of enabling an electronic record to be dispatched or received.

(2) ***Nothing in this section shall apply to any law that expressly provides for the retention of documents***, records or information in the form of electronic records, publication of rules, regulation, etc. in Electronic Gazette

This section deals with the retention or storing of electronic records. When any electronic records are created, its utility can be realized if it can be stored for future reference for a long period of time.

Certain laws such as Companies Act, Income Tax Act, and Evidence Act require record or documents prepared to be retained for a specific period of time. Such requirement shall be deemed to be satisfied if such documents etc are retained in an electronic form. For this purpose, sub-section (1) lays down the following conditions –

Conditions prescribed for retention of documents in electronic form

Proviso -

Generally, a computer automatically generates a backup file of every document or record saved in it. The same would not come under the category of the retained electronic record.

Section 7A - Audit of Documents etc. in Electronic form

Where in any law for the time being in force, there is a provision for ***audit*** of documents, records or information, that provision ***shall also be applicable for audit*** of documents, records or information processed and maintained ***in electronic form***.

Section 8 - Publication of rules, regulation, etc., in Electronic Gazette

Where any law provides that any ***rule, regulation, order, bye-law, notification or any other matter*** shall be ***published*** in the ***Official Gazette***, then, such requirement ***shall be deemed to have been satisfied if*** such rule, regulation, order, bye-law, notification or any other matter is published in the Official Gazette or ***Electronic Gazette***:

Provided that where any rule, regulation, order, bye-law, notification or any other matters published in the Official Gazette or Electronic Gazette, ***the date of publication shall be deemed to be the date of the Gazette which was first published in any form***.

Section 8 provides for the publication of rules, regulations and notifications in the ***Electronic Gazette***. It provides that where any law requires the publication of any rule, regulation, order, bye-law, notification or any other matter in the Official Gazette, then such requirement shall be deemed to be satisfied if the same is ***published in an electronic form***. It also provides where the Official Gazette is ***published both in the printed as well as in the electronic form, the date of publication shall be the date of publication of the Official Gazette which was first published in any form***.

Section 9 - Sections 6, 7 and 8 Not to Confer Right to insist document should be accepted in electronic form

Nothing contained in sections 6, 7 and 8 shall confer a right upon any person to insist that any Ministry or Department of the Central Government or the State Government or any authority or body established by or under any law or controlled or funded by the Central or State Government should ***accept, issue, create, retain and preserve any document in the form of electronic records or effect any monetary transaction in the electronic form.***

This section has ***permitted the use of traditional*** records, retention of the traditional records and the publication of the Official Gazette and has also simultaneously allowed the electronic record to be used

in the Government and its agencies. Therefore, it has been declared that sections 6, 7 and 8 shall not confer any right upon any person to insist that the Government or its agencies should accept, create and preserve any document in the form of electronic record or effect any monetary transaction in the electronic form.

Section 10 - Power to make rules by Central Government in respect of Electronic Signature

The Central Government may, for the purposes of this Act, by rules, prescribe -
(a) the ***type*** of Electronic Signature;
(b) the ***manner and format*** in which the Electronic Signature ***shall be affixed***;
(c) the ***manner or procedure*** which ***facilitates identification*** of the person affixing the Electronic Signature;
(d) ***control processes and procedures*** to ensure adequate integrity, security and confidentiality of electronic records or payments; and
(e) any other matter which is necessary ***to give legal effect to*** Electronic Signature.

Section 10A - Validity of contracts formed through electronic means

Where in a ***contract formation***, the communication of proposals, the acceptance of proposals, the revocation of proposals and acceptances, as the case may be, 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***.

Analysis

The Contract Act was enacted in the year 1872. At that time, there were no provisions in the Act for the formation of contract through electronic means. Therefore, by amending the IT Act 2000, Section 10A was inserted which made a deemed provision for formation of contract in electronic form. Section 10A provides that, information or matter in an electronic form shall ***"not be deemed to be unenforceable"*** (which means the requirement of formation of contract in writing shall be deemed to have been fulfilled) and ***it shall not be unenforceable solely on the ground that such electronic form or means was used for that purpose***.

The basic structure of the contract has not been changed. The Contract Act is still applicable. Only the form of signed writing and manner of formation of contract has been newly added.