

Legal Aspects of Business

Unit- 5

The Information Technology Act, 2000

Prepared by: Ms. Neha Rani
Assistant Professor
School of Business Studies
Shobhit Institute of Engineering and Technology
(Deemed to be University) Meerut

Content

- ▶ Definition, Digital Signature, Electronic Governance, Attribution, Acknowledgment and Dispatch of Electronic Records, Sense Electronic Records and Sense Digital Signatures, Regulation of Certifying Authorities, Digital Signature Certificates, Duties of Subscribers, Penalties and Offences.
- ▶ Intellectual Property Laws- Introduction, Legal Aspects of Patents, Filing of Patent Applications, Rights from Patents, Infringement of Patents, Copyright and its Ownership, Infringement of Copyright, Civil Remedies for Infringement.

Introduction

- ▶ The Information Technology Act, 2000 or ITA, 2000 or IT Act, was notified on October 17, 2000.
- ▶ It is the law that deals with cybercrime and electronic commerce in India.
- ▶ In 1996, the United Nations Commission on International Trade Law (UNCITRAL) adopted the model law on electronic commerce (e-commerce) to bring uniformity in the law in different countries.
- ▶ Further, the General Assembly of the United Nations recommended that all countries must consider this model law before making changes to their own laws. India became the 12th country to enable cyber law after it passed the Information Technology Act, 2000.

- ▶ While the first draft was created by the Ministry of Commerce, Government of India as the Ecommerce Act, 1998, it was redrafted as the ‘Information Technology Bill, 1999’, and passed in May 2000.
- ▶ Information Technology Act 2000, has 13 chapters, 94 sections and 4 schedules. –
- ▶ First 14 sections deals with some legal aspects concerning digital signature.
- ▶ Further other sections deal with certifying authorities who are licensed to issue digital signature certificate.
- ▶ Sections 43 to 47 provide for penalties and compensation.
- ▶ Sections 48 to 64 deals with Tribunals a appeal to high court.
- ▶ Section 65 to 79 of the act deals with offences.
- ▶ Section 80 to 94 deals with miscellaneous of the Act.

Objectives of the Act

- ▶ Grant legal recognition to all transactions done via electronic exchange of data or other electronic means of communication or e-commerce, in place of the earlier paper-based method of communication.
- ▶ Give legal recognition to digital signatures for the authentication of any information or matters requiring legal authentication
- ▶ Facilitate the electronic filing of documents with Government agencies and also departments
- ▶ Facilitate the electronic storage of data
- ▶ Give legal sanction and also facilitate the electronic transfer of funds between banks and financial institutions
- ▶ Grant legal recognition to bankers under the Evidence Act, 1891 and the Reserve Bank of India Act, 1934, for keeping the books of accounts in electronic form.

Features of the Information Technology Act, 2000

- ▶ All electronic contracts made through secure electronic channels are legally valid.
- ▶ Legal recognition for digital signatures.
- ▶ Security measures for electronic records and also digital signatures are in place
- ▶ A procedure for the appointment of adjudicating officers for holding inquiries under the Act is finalized
- ▶ Provision for establishing a Cyber Regulatory Appellant Tribunal under the Act. Further, this tribunal will handle all appeals made against the order of the Controller or Adjudicating Officer.
- ▶ An appeal against the order of the Cyber Appellant Tribunal is possible only in the High Court

- ▶ Provision for the appointment of the Controller of Certifying Authorities (CCA) to license and regulate the working of Certifying Authorities. The Controller to act as a repository of all digital signatures.
- ▶ The Act applies to offences or contraventions committed outside India
- ▶ Senior police officers and other officers can enter any public place and search and arrest without warrant
- ▶ Provisions for the constitution of a Cyber Regulations Advisory Committee to advise the Central Government and Controller.

Digital Signature

- ▶ A digital signature is exactly what it sounds like a modern alternative to signing documents with paper and pen.
- ▶ It uses an advanced mathematical technique to check the authenticity and integrity of digital messages and documents. It guarantees that the contents of a message are not altered in transit and helps us overcome the problem of impersonation and tampering in digital communications.
- ▶ Digital signatures also provide additional information such as the origin of the message, status, and consent by the signer.

Electronic Governance

- ▶ It is the use of electronic means, to promote good governance. It connotes the implementation of information technology in the government processes and functions so as to cause simple, moral, accountable and transparent governance. It entails the access and delivery of government services, dissemination of information, communication in a quick and efficient manner.

Benefits of E-governance

- ▶ Reduced corruption
- ▶ High transparency
- ▶ Increased convenience
- ▶ Growth in GDP
- ▶ Direct participation of constituents
- ▶ Reduction in overall cost.
- ▶ Expanded reach of government

Types of Interactions in E-Governance

G2G (Government to Government): When the exchange of information and services is within the periphery of the government, is termed as G2G interaction. This can be both horizontal, i.e. among various government entities and vertical, i.e. between national, state and local government entities and within different levels of the entity.

G2C (Government to Citizen): The interaction amidst the government and general public is G2C interaction. Here an interface is set up between government and citizens, which enables citizens to get access to wide variety of public services. The citizens has the freedom to share their views and grievances on government policies anytime, anywhere.

G2B (Government to Business): In this case, the e-governance helps the business class to interact with the government seamlessly. It aims at eliminating red-tapism, saving time, cost and establish transparency in the business environment, while interacting with government.

G2E (Government to Employees): The government of any country is the biggest employer and so it also deals with employees on a regular basis, as other employers do. ICT helps in making the interaction between government and employees fast and efficient, along with raising their level of satisfaction by providing perquisites and add-on benefits.

Attribution of electronic records (SECTION 11)

An electronic records shall be attributed to the originator

- A. If it was sent by the originator himself.
- B. By a person who had the authority to act on behalf of the originator in respect of that electronic record.
- C. by an information system programmed by or on behalf of the originator to operate automatically.

(With respect to IT At 2000, attribution of electronic records means fixing identity of sender and receiver. Here originator is a person who sends or generates any electronic record. The receiver of electronic record is termed as Addressee.

For example

- ▶ If 'X' sends an email to 'Y', then 'X' is a sender or originator and 'Y' is receiver or Addressee.
- ▶ In normal course of communication (postal communication or paper communication), it's very easy to identify originator and addressee but in electronic communication it's not the same.
- ▶ The electronic record can be sent by the originator himself or by the person who has been authorized by the originator or by an information system that the originator has authenticated.)

Acknowledgment Of Receiving Of Electronic Record (Section12)

If the originator has not specified any specific mode of acknowledgement (an act by the addressee that he/she has received the electronic record), the acknowledgement can be given by a return mail by the addressee or an automated response by the addressee or an act by addressee that shows the acknowledgement.

For example

when a person receives an email by an estate agent, for real estate properties, the person can send a thank u mail or can send an automatic reply or can show interest in the offer given by the agent by visiting him. All the three option show an acknowledgement.

- ▶ If the originator has specified a format and time period for sending the acknowledgement, then the addressee must send the acknowledgement in that format and within the given time period otherwise the originator can send a notice to the addressee stating that no acknowledgement was received.

- ▶ Where the originator has not stipulated that the electronic record shall be binding only on receipt of such acknowledgment, and the acknowledgment has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed to within a reasonable time, then the originator may give notice to the addressee stating that no acknowledgment has been received by him and specifying a reasonable time by which the acknowledgment must be received by him and if no acknowledgment is received within the aforesaid time limit he may after giving notice to the addressee, treat the electronic record as though it has never been sent.

TIME AND PLACE OF Dispatch of Electronic Record(Section 13)

1. Save as otherwise agreed to between the originator and the addressee, the dispatch of an electronic record occurs when it enters a computer resource outside the control of the originator.
2. Save as otherwise agreed between the originator and the addressee, the time of receipt of an electronic record shall be determined as follows, namely :-
 - (a) if the addressee has designated a computer resource for the purpose of receiving electronic records – receipt occurs at the time when the electronic, record enters the designated computer resource, or

- ▶ if the electronic record is sent to a computer resource of the addressee that is not the designated computer resource, receipt occurs at the time when the electronic record is retrieved by the addressee.

(b) if the addressee has not designated a computer resource along with specified timings, if any, receipt occurs when the electronic record enters the computer resource of the addressee.

3. Save as otherwise agreed to between the originator and the addressee, an electronic record is deemed to be dispatched at the place where the originator has his place of business, and is deemed to be received at the place where the addressee has his place of business.

4. The provisions of sub-section (2) shall apply notwithstanding that the place where the computer resource is located may be different from the place where the electronic record is deemed to have been received under sub-section (3).

5. For the purposes of this section –

- if the originator or the addressee has more than one place of business, the principal place of business, shall be the place of business.
- if the originator or the addressee does not have a place of business, his usual place of residence shall be deemed to be the place of business.
- "usual place of residence", in relation to a body corporate, means the place where it is registered.

(This section states that when a person sends an electronic record from his computer then that particular time becomes the time of dispatch.

For example

If Mr. X composes an email at 3.30 am and presses the “Send” button at 4.30 am then time of dispatch will be 4.30 am. because after pressing send button the sender cannot make any changes to the record.)

Sense Electronic Records and Sense Digital Signatures

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.

Secure digital signature.

If, by application of a security procedure agreed to by the parties concerned, it can be verified that a digital signature, at the time it was affixed, was-

- ▶ unique to the subscriber affixing it.
- ▶ capable of identifying such subscriber.
- ▶ created in a manner or using a means under the exclusive control of the subscriber and is linked to the electronic record to which it relates in such a manner that if the electronic record was altered the digital signature would be invalidated.

then such digital signature shall be deemed to be a secure digital signature.

Security procedure.

The Central Government shall for the purposes of this Act prescribe the security procedure having regard to commercial circumstances prevailing at the time when the procedure was used, including-

- ▶ the nature of the transaction.
- ▶ the level of sophistication of the parties with reference to their technological capacity.
- ▶ the volume of similar transactions engaged in by other parties.
- ▶ the availability of alternatives offered to but rejected by any party.
- ▶ the cost of alternative procedures, and
- ▶ the procedures in general use for similar types of transactions or communications.

Regulation of Certifying Authorities

APPOINTMENT OF CONTROLLER AND OTHER OFFICERS.

- (1) The Central Government may, by notification in the Official Gazette, appoint a Controller of Certifying Authorities for the purposes of this Act and may also by the same or subsequent notification appoint such number of Deputy Controllers and Assistant Controllers as it deems fit.
- (2) The Controller shall discharge his functions under this Act subject to the general control and directions of the Central Government.
- (3) The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and control of the Controller.
- (4) The qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers shall be such as may be prescribed by the Central Government.
- (5) The Head Office and Branch Office of the office of the Controller shall be at such places as the Central Government may specify, and these may be established at such places as the Central Government may think fit.
- (6) There shall be a seal of the Office of the Controller.

FUNCTIONS OF CONTROLLER

- ▶ exercising supervision over the activities of the Certifying Authorities.
- ▶ certifying public keys of the Certifying Authorities.
- ▶ laying down the standards to be maintained by the Certifying Authorities.
- ▶ specifying the qualifications and experience which employees of the Certifying Authorities should possess.
- ▶ specifying the conditions subject to which the Certifying Authorities shall conduct their business.
- ▶ specifying the contents of written, printed or visual materials and advertisements that may be distributed or used in respect of a Digital Signature Certificate and the public key.
- ▶ specifying the form and content of a Digital Signature Certificate and the key.
- ▶ specifying the form and manner in which accounts shall be maintained by the Certifying Authorities.

- ▶ specifying the terms and conditions subject to which auditors may be appointed and the remuneration to be paid to them.
- ▶ facilitating the establishment of any electronic system by a Certifying Authority either solely or jointly with other Certifying Authorities and regulation of such systems.
- ▶ specifying the manner in which the Certifying Authorities shall conduct their dealings with the subscribers.
- ▶ resolving any conflict of interests between the Certifying Authorities and the subscribers.
- ▶ laying down the duties of the Certifying Authorities.
- ▶ maintaining a data base containing the disclosure record of every Certifying Authority containing such particulars as may be specified by regulations, which shall be accessible to public.

Digital Signature Certificates

- ▶ A Digital Signature Certificate is a secure digital key that is issued by the certifying authorities for the purpose of validating and certifying the identity of the person holding this certificate. Digital Signatures make use of the public key encryptions to create the signatures.
- ▶ A digital signature certificate (DSC) contains information about the user's name, pin code, country, email address, date of issuance of certificate and name of the certifying authority.

Benefits of a digital signature certificate

- ▶ Digital Signature Certificates are helpful in authenticating the personal information details of the individual holder when conducting business online.
- ▶ **Reduced cost and time:** Instead of signing the hard copy documents physically and scanning them to send them via e-mail, you can digitally sign the PDF files and send them much more quickly.
- ▶ The Digital Signature certificate holder does not have to be physically present to conduct or authorize a business
- ▶ **Data integrity:** Documents that are signed digitally cannot be altered or edited after signing, which makes the data safe and secure.
- ▶ The government agencies often ask for these certificates to cross-check and verify the business transaction
- ▶ **Authenticity of documents:** Digitally signed documents give confidence to the receiver to be assured of the signer's authenticity. They can take action on the basis of such documents without getting worried about the documents being forged.

Penalties under it act 2000

- ▶ **Section 43:** Where a person without the permission of owner or any other person-in-charge damage the Computer, or Computer System, or Computer Network, the he shall be liable for Penalty and Compensation to such person so affected.
- ▶ **Section 44:** Where a person fails to furnish any document, return, report to the controller, or certifying authority, then he shall be liable to pay penalty upto **Rs.1,50,000/-** per failure. Further where a person fails to furnish any information, books or other documents within time specified, then he shall be liable to pay penalty upto **Rs.5,000/-** per day. Further provided that where a person fails to maintain books of accounts or other records, then he shall be liable to pay penalty upto **Rs.10,000/-** per day.

- ▶ **Section 66D:** Any person dishonestly, or fraudulently by means of any communication device or computer resource cheats by personating, then he shall be liable to pay penalty upto **Rs.1,00,000/-**, or Imprisonment upto **3 years**, or both.
- ▶ **Section 66E:** Any person intentionally captures, publishes, or transmits image of private area of any person without consent, then he shall be liable to pay penalty upto **Rs.2,00,000/-**, or Imprisonment upto **3 years**, or both.
- ▶ **Section 66F:** Any person does any act electronically, or with use of computer with intent to threaten unity, integrity, security, or sovereignty of India, then he shall be punishable with **Imprisonment for Life**.

Offences under Information Technology Act, 2000

- ▶ **Section 65:** Any person tamper, conceal, destroy, or alter any computer source document intentionally, then he shall be liable to pay penalty upto **Rs.2,00,000/-**, or Imprisonment upto **3 years**, or both.
- ▶ **Section 66:** Any person dishonestly, or fraudulently does any act as referred in **Section 43**, then he shall be liable to pay penalty upto **Rs.5,00,000/-**, or Imprisonment upto **3 years**, or both.
- ▶ **Section 66B:** Any person dishonestly, or fraudulently receives or retains any stolen computer resource or communication device, then he shall be liable to pay penalty upto **Rs.1,00,000/-**, or Imprisonment upto **3 years**, or both.
- ▶ **Section 66C:** Any person dishonestly, or fraudulently make use of Electronic Signature, Password or any other Unique Identification Feature of any other person, then he shall be liable to pay penalty upto **Rs.1,00,000/-**, or Imprisonment upto **3 years**, or both.

Intellectual Property Law

- ▶ **Intellectual Property Rights (IPR)** are an essential but often overlooked set of rights. The creative rights over an original piece of work, invention or even an idea behind a business can come under the purview of Intellectual Property Rights.
- ▶ With the emergence of the digital age, instances of plagiarism and copyright infringements have increased manifold. Strict laws to prevent theft of intellectual property have become absolutely necessary to create an atmosphere of trust and to encourage innovation.

Legal Aspects of Patents

Patent law is a component of the broader framework regarded as intellectual property. Legal aspects include protecting your intellectual property rights, including trademarking, copyrighting and protecting trade secrets.

While trying to patent an invention, the inventor must ensure that their design meets three basic requirements.

- ▶ **Novelty:** For an invention to be considered a novelty, it has to be new.
- ▶ **Usefulness:** For an invention to be considered useful it should be able to perform what it intends to while serving a useful purpose
- ▶ **Inventive or lacking obviousness:** An Inventive patent is provided when a series of original steps are taken in the creation of an idea or product.

Patent definition

- ▶ Latin term *paterere*, "to lay open" (i.e., to make available for public inspection), In English term letters patent, royal decree granting exclusive rights to a person. Patents in the modern sense originated in 1474, in the Republic of Venice
- ▶ A patent is a form of intellectual property. It consists of a set of exclusive rights granted by a government to a true and first inventor or their assignee for a limited period of time in exchange for the public disclosure of an invention. Patent is an exclusive right granted to a person who has invented a new and useful article or an improvement over an existing article.

Types of Patents

- ▶ **Utility Patents:** Patents that cover inventions resulting in usefulness. However, India does not have system of Utility patents.
- ▶ **Design Patents:** Patents that cover the shape or surface of a physical object
- ▶ **Plant Patents:** Patents that cover asexually reproducing plants

Filing of Patent Applications

- ▶ **National applications** : National applications are generally filed at a national patent office, such as the United Kingdom Patent Office, to obtain a patent in the country of that office. The application may either be filed directly at that office, or may result from a regional application or from an international application under the Patent Cooperation Treaty (PCT), once it enters the national phase.
- ▶ **Regional applications** : A regional patent application is one which may have effect in a range of countries. The European Patent Office (EPO) is an example of a Regional patent office. The EPO grants patents which can take effect in some or all countries contracting to the European Patent Convention (EPC), following a single application process.

- ▶ International applications : (under the Patent Cooperation Treaty)
The Patent Cooperation Treaty (PCT) is operated by World Intellectual Property Organization (WIPO) and provides a centralized application process, but patents are not granted under the treaty. The PCT system enables an applicant to file a single patent application in a single language. The application, called an international application, can, at a later date, lead to the grant of a patent in any of the states contracting to the PCT. WIPO, or more precisely the International Bureau of WIPO, performs many of the formalities of a patent application in a centralized manner, therefore avoiding the need to repeat the steps in all countries in which a patent may ultimately be granted. The main advantage of proceeding via the PCT route is that the option of obtaining patents in a wide range of countries is retained

Types of application

1 . Standard application : A standard patent application is a patent application containing all of the necessary parts (e.g. a written description of the invention and claims) that are required for the grant of a patent. A standard patent may or may not result in the grant of a patent depending upon the outcome of an examination by the patent office it is filed in. In the U.S., a standard patent application is referred to as a "non-provisional" application.

2 . Provisional application : Provisional patent applications can be filed at many patent offices, such as the USPTO in the U.S. A provisional application provides an opportunity to place an application on file to obtain a filing date (thereby securing a priority date), but without the expense and complexity of a standard patent application. The disclosure in a provisional application may, within a limited time (one year in the U.S.), be incorporated into a standard patent application if a patent is to be pursued. Otherwise, the provisional application expires. No enforceable rights can be obtained solely through the filing of a provisional application.

3. Continuation application : In certain offices a patent application can be filed as a continuation of a previous application. Such an application is a convenient method of including material from a previous application in a new application when the priority year has expired and further refinement is needed. Various types of continuation application are possible, such as continuation and continuation-in-part

4 .Divisional application : A divisional application is one which has been "divided" from an existing application. A divisional application can only contain subject matter in the application from which it is divided (its parent), but retains the filing and priority date of that parent. A divisional application is useful if a unity of invention objection is issued, in which case the second (and third, fourth, etc.) inventions can be protected in divisional applications

Rights and obligations of a patent owner

Rights of an applicant

The applicant or the owner of the invention has the following rights: -

1. to be granted the patent, where the relevant requirements are fulfilled;
2. after the grant of the patent and within the limits defined below to preclude any person from exploiting the patented invention in the manner referred to in section 53; and
3. to conclude license contracts as provided for in the Act.

Obligations

The applicant or the owner of the invention has the following obligations -

1. to disclose the invention in a clear and complete manner, and in particular to indicate at least one mode for carrying out the invention, in accordance with the requirements, and subject to the sanctions, applicable under the Act;
2. to give information concerning corresponding foreign applications and grants;
3. to pay fees to the Managing Director, as prescribed in the Act and the regulations, subject to the sanctions provided for therein; and
4. in connection with license contracts and contracts assigning patents or patent applications, to refrain from making undesirable provisions referred to in section 69.

Rights of owner of a patent

The owner of the patent has the right to preclude any person from exploiting the protected invention by any of the following acts -

1. when the patent has been granted in respect of a product -
 1. making, importing, offering for sale, selling and using the product; or
 2. stocking such product for the purposes of offering it for sale, selling or using the product;
2. when the patent has been granted in respect of a process -
 1. using the process, or doing any of the acts referred to in paragraph (1), in respect of a product obtained directly by means of the process.

Infringement of Patents

- ▶ Patent infringement means the violation of the exclusive rights of the patent holder. As discussed earlier, patent rights are the exclusive rights granted by the Government to an inventor over his invention for a limited period of time. In other words, if any person exercises the exclusive rights of the patent holder without the patent owner's authorization then that person is liable for patent infringement. Sections 104-114 of the Patents Act, 1970 provide guidelines relating to patent infringement.

- ▶ Unlike the Design law, the Patents law does not specify as to what would constitute infringement of a patented product or process. However, the following acts when committed without the consent of the patentee shall amount to infringement:
 - making, using, offering for sale, selling, importing the patented product;
 - using the patented process, or using, offering for sale, selling or importing the product directly obtained by that process

Types of Infringement

- ▶ Direct patent infringement is the most obvious and the most common form of patent infringement. Basically, direct patent infringement occurs when a product that is substantially close to a patented product or invention is marketed, sold, or used commercially without permission from the owner of the patented product or invention.
- ▶ Indirect patent infringement suggests that there was some amount of deceit or accidental patent infringement in the incident. For instance, A holds a patent for a device and B manufactures a device which is substantially similar to the A's device. B is supplied with a product from another person C to facilitate manufacturing of the B's device. If the device so manufactured by B infringes upon A's patent, then the person C indirectly infringes A's patent. Further, if such a product is knowingly sold or supplied, it may lead to "contributory infringement". In the above example, if the person C knowingly supplies the product to B then the infringement is construed as contributory infringement.

Copyright

What is Copyright ?



copyright

all rights reserved

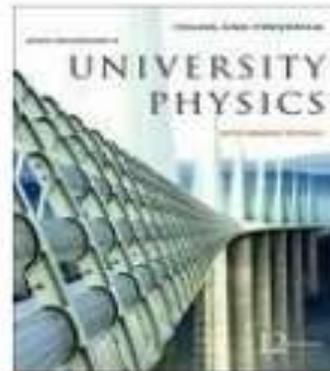
“The exclusive right given by law for a certain term of years to an author, composer etc. (or his assignee) to print, publish and sell copies of his original work”

(Oxford English Dictionary)

What can be Protected ?

4

- literary or dramatic work
- a musical work
- an artistic work
- a cinematograph film
- a sound recording
- a photograph
- a computer generated work



Whose Rights are protected ?

5

- Copyright protects the right of **Author**, i.e. creator of Intellectual Properties.
 - ▣ He/She is also called the First Owner of Copyright.

- However, in course of employment, the employer is the first owner of these rights.

Work	Creator of work
Literary or dramatic work	Author
Musical work	Composer
Cinematograph	Producer
Sound recording	Producer
Photograph	Photographer

Economic rights

- ▶ to produce copies or reproductions of the work and to sell those copies (including, typically, electronic copies)
- ▶ to import or export the work
- ▶ to create derivative works (works that adapt the original work)
- ▶ to perform or display the work publicly
- ▶ to sell or assign these rights to others
- ▶ to transmit or display by radio or video

Moral rights

Right of paternity: to claim authorship of work and to prevent all others from claiming authorship of his work.

Right of integrity: to prevent distortion, mutilation or other alterations of his work, or any other action in relation to said work, which would be prejudicial to his honor or reputation.

Copyright Symbol ©

14

- ❑ Use of the "©" symbol
- ❑ Anyone who claims copyrights can use it
- ❑ not necessary to have a registration to use the designations
- ❑ highly advisable to incorporate a copyright notice
- ❑ Example:

Copyright © 2009 Microsoft Corporation

Infringement of Copyright

Owners develop new work and get copyright protection to ensure that they can get profit from their efforts. Owner has sole authority either to sell his work or to license it to the third party who can make use of his work but if someone duplicates or reproduces the work of copyright holder without the latter's permission, then this can lead to copyright infringement, in which owner can take legal action against the infringer.

Exception to Infringement under Sec.52 of The Copyright Act, 1957

- ▶ Private or personal use, including research
- ▶ Criticism or review, whether of that work or any other work
- ▶ The reporting of current events and current affairs, including the reporting of a lecture delivered in public.

Remedies for Infringement of Copyright

- ▶ **Civil remedy:** According to Section 55 of The Copyright Act, 1957, where copyright in any work has been infringed upon, the owner of the copyright shall be entitled to all such remedies by way of injunction, damages, & accounts.
- ▶ **Criminal remedy:** According to Section 63 of The Copyright Act, 1957, the copyright holder can take criminal proceedings against the infringer, in which there is a provision of at least six-month imprisonment, which may be extended to 3 years and with a fine of Rs. 50,000, which may extend to 2 lakhs.