Lecture in a Conference/meeting at Mauritius from 22nd March,2010 to 25th March,2010 on Cyber Law on invitation from Information & Communication Technologies Authority (ICTA) of Mauritius

By

Justice Rajesh Tandon,
Chairperson,
Cyber Appellate Tribunal
Ministry of Communications & Information Technology Department of Information Technology,
Jeevan Bharti (LIC) Building, Connaught Place,
New Delhi.

Subject

CYBER LAW

The Information Technology Act,2000 came into force on 17th October, 2000. This Act was amended vide notification dated 27th October,2009. The Definitions in the Amended Act are as under:

(a) "Act" means Information Technology Act,2000 (21 of 2000)

(b) "Communication" means dissemination, transmission, carriage of information or signal in some manner and include both a direct communication and an indirect communication"

(c) "Communication link" means the use of satellite, microwave, radio, terrestrial line, wire, wireless or any other communication media to inter-connect computer resource.

The Information Technology Act,2000 was introduced on 9th June,2000. Mitigation that has led to the introduction of the Information Technology Act,2000 was the model law of electronic commerce known as the United Nation Commission of International Trade Law which was introduced in the general assembly of UN by its resolution No.51 of 162 dated 30th January,1997 which has recommended that all the States should give favourable consideration to the said model law which contained equal legal treatment of user of electronic communication and paper based communication. The preamble of Act 21 of 2000 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 Banker's Books Evidence Act,1891 and the Reserve Bank of India Act,1934 and for matters connected therewith or incidental thereto;

Whereas the General Assembly of the United Nations by resolution A/RES/51/162 dated 30th January,1997 has adopted the Model Law on Electronic Commerce adopted by the United Nations Commission on International Trade law;

And whereas the said resolution recommends, inter alia, that all States give favourable consideration to the said Model Law when they enact or revise their laws, in view of the need for uniformity of the law applicable to alternatives to paper-based methods of communication and storage of information."

UNCITRAL MODEL LAW ON ELECTRONIC COMMERCE 1996, AS AMENDED 1998

PART ONE. ELECTRONIC COMMERCE IN GENERAL
CHAPTER I. GENERAL PROVISIONS

Article 1. Sphere of application*

This Law** applies to any kind of information in the form of a data message use din the context*** of commercial**** activities.

*The Commission suggests the following text for States that might wish to limit the applicability of this Law to international data messages:

"This Law applies to a data message as defined in paragraph (1) of article 2 where the data message relates to international commerce."

**This Law does not override any rule of law intended for the protection of consumers.

***The Commission suggests the following text for States that might wish to extend the applicability of this Law: "This Law applies to any kind of information in the form of a data message, except in the following situations:

**** The term 'commercial' should be given a wide interpretation so as to cover matters arising from all relationships of a commercial nature, whether contractual or not. Relationships of a commercial nature include, but are not limited to, the following

transactions: any trade transaction for the supply or exchange of goods or services; distribution agreement, commercial representation or agency; factoring; leasing; construction of works; consulting; engineering, licensing; investment; financing; banking; insurance; exploitation agreement or concession; joint venture and other forms of industrial or business cooperation; carriage of goods or passengers by air, sea, rail or road.

Article 2. Definitions

For the purposes of this Law-

(a) `Data message' means information generated, sent, received or stored by electronic, optical or similar means including, but not limited to, electronic data interchange (EDI), electronic mail, telegram, telex or telecopy.

(b) 'Electronic data interchange (EDI)' means the electronic transfer from computer to computer of information using an agreed standard to structure the information.

(c) 'Originator' of a data message means a person by whom, or on whose behalf, the data message purports to have been sent or generated prior to storage, if any, but it does not include a person acting as an intermediary with respect to that data message.

(d) 'Addressee' of a data message means a person who is intended by the originator to receive the data message, but does not include a person acting as an intermediary with respect to that data message;

(e) 'Intermediary' with respect to a particular data message, means a person who, on behalf of another person, sends, receives or stores that data message or provides other services with respect to that data message.

(f) 'Information system' means a system for generating, sending, receiving, storing or otherwise processing data messages.

Article 3. Interpretation.

(1) In the interpretation of this Law, regard is to be had to its international origin and to the need to promote uniformity in its application and the observance of good faith.

(2) Questions concerning matters governed by this Law which are not expressly settled in it are to be settled in conformity with the general principles on which this Law is based.

Article 4. Variation by agreement.

(1) As between parties involved in generating, sending, receiving, storing or otherwise processing data messages, and except as otherwise provided, the provisions of chapter III may be varied by agreement.
(2) Paragraph (1) does not affect any right that may exist to modify by agreement any rule of law referred to in chapter II.

CHAPTER II. APPLICATION OF LEGAL REQUIREMENTS TO DATA MESSAGES.

Article 5. Legal recognition of data messages.

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.

Article 5 bis. Incorporation by reference.
(as adopted by the Commission at its thirty-first session, in June,1998)

Information shall not be denied legal effect, validity or enforceability solely on the grounds that it is not contained in the data message purporting to give rise to such legal effect, but is merely referred to in that data message.

Article 6. Writing

(1) Where the law requires information to be in writing, that requirement is met by a data message if the information

contained therein is accessible so as to be usable for subsequent reference.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being in writing.

(3) The provisions of this article do not apply to the following: […]

Article 7. Signature

(1) Where the law requires a signature of a person, that requirement is met in relation to a data message if-

(a) a method is used to identify that person and to indicate that person's approval of the information contained in the data message; and

(b) that method is as reliable as was appropriate for the purpose for which the data message was generated or communicated, in the light of all the circumstances, including any relevant agreement.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the absence of a signature.

(3) The provisions of this article do not apply to the following:[…]

Article 8. Original

(1) Where the law requires information to be presented or retained in its original form, that requirement is met by a data message if:

(a) there exists a reliable assurance as to the integrity of the information from the time when it was first generated in its final form, as a data message or otherwise; and

(b) where it is required that information be presented, that information is capable of being displayed to the person to whom it is to be presented.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for the information not being presented or retained in its original form.

(3) For the purposes of subparagraph *(a)* of paragraph (1):

(a) the criteria for assessing integrity shall be whether the information has remained complete

and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and

(b) the standard of reliability required shall be assessed in the light of the purpose for which the information was generated and in the light of all the relevant circumstances.

(4) The provisions of this article do not apply to the following: [...].

Article 9. Admissibility and evidential weight of data messages

(1) In any legal proceedings, nothing in the application of the rules of evidence shall apply so as to deny the admissibility of a data message in evidence:

(a) on the sole ground that it is a data message; or,

(b) if it is the best evidence that the person adducing it could reasonably be expected to obtain, on the grounds that it is not in its original form.

(2)Information in the form of a data message shall be given due evidential weight. In assessing the evidential weight of a data message, regard shall be had to the reliability of the manner in which the data message was generated, stored or communicated, to the reliability of the manner in which the integrity of the information was maintained, to the manner in which its originator was identified, and to any other relevant factor

.

Article 10. Retention of data messages

(1) Where the law requires that certain documents, records or information be retained, that requirement is met by retaining data messages, provided that the following conditions are satisfied:

(a) the information contained therein is accessible so as to be usable for subsequent reference; and

(b) the data message is retained in the format in which it was generated, sent or received, or in a format which can be demonstrated to represent accurately the information generated, sent or received; and

(c) such information, if any, is retained as enables the identification of the origin and destination of a data message and the date and time when it was sent or received.

(2) An obligation to retain documents, records or information in accordance with paragraph (1) does not extend to any information the sole purpose of which is to enable the message to be sent or received.
(3) A person may satisfy the requirement referred to in paragraph (1) by using the services of any other person, provided that the conditions set forth in subparagraphs *(a)*, *(b)* and *(c)* of paragraph (1) are met.

CHAPTER III. COMMUNICATION OF DATA MESSAGES

Article 11. Formation and validity of contracts

(1) In the context of contract formation, unless otherwise agreed by the parties, an offer and the acceptance of an offer may be expressed by means of data messages. Where a data message is used in the formation of a contract, that contract shall not be denied validity or enforceability on the sole ground that a data message was used for that purpose.

(2) The provisions of this article do not apply to the following: [...].

Article 12. Recognition by parties of data messages

(1) As between the originator and the addressee of a data message, a declaration of will or other statement shall not be denied legal effect, validity or enforceability solely on the grounds that it is in the form of a data message.
(2) The provisions of this article do not apply to the following: [...].

Article 13. Attribution of data messages

(1) A data message is that of the originator if it was sent by the originator itself.
(2) As between the originator and the addressee, a data message is deemed to be that of the originator if it was sent:

(a) by a person who had the authority to act on behalf of the originator in respect of that data message; or

(b) by an information system programmed by, or on behalf of, the originator to operate automatically.

(3) As between the originator and the addressee, an addressee is

entitled to regard a data message as being that of the originator, and to act on that assumption, if:

(a) in order to ascertain whether the data message was that of the originator, the addressee properly applied a procedure previously agreed to by the originator for that purpose; or

(b) the data message as received by the addressee resulted from the actions of a person whose relationship with the originator or with any agent of the originator enabled that person to gain access to a method used by the originator to identify data messages as its own.

(4) Paragraph (3) does not apply:

(a) as of the time when the addressee has both received notice from the originator that the data message is not that of the originator, and had reasonable time to act accordingly; or

(b) in a case within paragraph (3)*(b)*, at any time when the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was not that of the originator.

(5) Where a data message is that of the originator or is deemed to be that of the originator, or the addressee is entitled to act on that assumption, then, as between the originator and the addressee, the addressee is entitled to regard the data message as received as being what the originator intended to send, and to act on that assumption. The addressee is not so entitled when it knew or should have known, had it exercised reasonable care or used any agreed procedure, that the transmission resulted in any error in the data message as received.

(6) The addressee is entitled to regard each data message received as a separate data message and to act on that assumption, except to the extent that it duplicates another data message and the addressee knew or should have known, had it exercised reasonable care or used any agreed procedure, that the data message was a duplicate.

Article 14. Acknowledgement of receipt

(1) Paragraphs (2) to (4) of this article apply where, on or before sending a data message, or by means of that data message, the originator has requested or has agreed with the addressee that receipt of the data message be acknowledged.

(2) Where the originator has not agreed with the addressee that the acknowledgement be given in a particular form or by a particular method, an acknowledgement may be given by

(a) any communication by the addressee, automated or otherwise, or

(b) any conduct of the addressee sufficient to indicate to the originator that the data message has been received.

(2) Where the originator has stated that the data message is conditional on receipt of the acknowledgement, the data message is treated as though it has never been sent, until the acknowledgement is received.

(3) Where the originator has not stated that the data message is conditional on receipt of the acknowledgement, and the acknowledgement has not been received by the originator within the time specified or agreed or, if no time has been specified or agreed, within a reasonable time, the originator:

(a) may give notice to the addressee stating that no acknowledgement has been received and specifying a reasonable time by which the acknowledgement must be received; and

(b) if the acknowledgement is not received within the time specified in subparagraph *(a)*, may, upon notice to the addressee, treat the data message as though it had never been sent, or exercise any other rights it may have.

(5) Where the originator receives the addressee's acknowledgement of receipt, it is presumed that the related data message was received by the addressee. That presumption does not imply that the data message corresponds to the message received.

(6) Where the received acknowledgement states that the related data message met technical requirements, either agreed upon or set forth in applicable standards, it is presumed that those requirements have been met.

(7) Except in so far as it relates to the sending or receipt of the data message, this article is not intended to deal with the legal consequences that may flow either from that data message or from the acknowledgement of its receipt.

***Article 15. Time and place of dispatch and receipt* of data messages**

(1) Unless otherwise agreed between the originator and the addressee, the dispatch of a data message occurs when it enters an information system outside the control of the originator or of the person who sent the data message on behalf of the originator.

(2) Unless otherwise agreed between the originator and the addressee, the time of receipt of a data message is determined as follows:

(a) if the addressee has designated an information system for the purpose of receiving data messages, receipt occurs:

(i) at the time when the data message enters the designated

information system; or
(ii) if the data message is sent to an information system of the addressee that is not the designated information system, at the time when the data message is retrieved by the addressee;
(b) if the addressee has not designated an information system, receipt occurs when the data message enters an information system of the addressee.
(3) Paragraph (2) applies notwithstanding that the place where the information system is located may be different from the place where the data message is deemed to be received under paragraph (4).
(4) Unless otherwise agreed between the originator and the addressee, a data message is deemed to be dispatched at the place where the originator has its place of business, and is deemed to be received at the place where the addressee has its place of business. For the purposes of this paragraph:
(a) if the originator or the addressee has more than one place of business, the place of business is that which has the closest relationship to the underlying transaction or, where there is no underlying transaction, the principal place of business;
(b) if the originator or the addressee does not have a place of business, reference is to be made to its habitual residence.
(5) The provisions of this article do not apply to the following: [...].

Part two. Electronic commerce in specific areas

CHAPTER I. CARRIAGE OF GOODS

Article 16. Actions related to contracts of carriage of goods

Without derogating from the provisions of part one of this Law, this chapter applies to any action in connection with, or in pursuance of, a contract of carriage of goods, including but not limited to:
(a) (i) furnishing the marks, number, quantity or weight of goods;
(ii) stating or declaring the nature or value of goods;
(iii) issuing a receipt for goods;
(iv) confirming that goods have been loaded;
(b) (i) notifying a person of terms and conditions of the contract;
(ii) giving instructions to a carrier;
(c) (i) claiming delivery of goods;
(ii) authorizing release of goods;
(iii) giving notice of loss of, or damage to, goods;
(d) giving any other notice or statement in connection with the performance of the contract;
(e) undertaking to deliver goods to a named person or a person authorized to claim delivery;

(f) granting, acquiring, renouncing, surrendering, transferring or negotiating rights in goods;
(g) acquiring or transferring rights and obligations under the contract.

Article 17. Transport documents

(1) Subject to paragraph (3), where the law requires that any action referred to in article 16 be carried out in writing or by using a paper document, that requirement is met if the action is carried out by using one or more data messages.

(2) Paragraph (1) applies whether the requirement therein is in the form of an obligation or whether the law simply provides consequences for failing either to carry out the action in writing or to use a paper document.
(3) If a right is to be granted to, or an obligation is to be acquired by, one person and no other person, and if the law requires that, in order to effect this, the right or obligation must be conveyed to that person by the transfer, or use of, a paper document, that requirement is met if the right or obligation is conveyed by using one or more data messages, provided that a reliable method is used to render such data message or messages unique.
(4) For the purposes of paragraph (3), the standard of reliability required shall be assessed in the light of the purpose for which the right or obligation was conveyed and in the light of all the circumstances, including any relevant agreement.
(5) Where one or more data messages are used to effect any action in sub paragraphs *(f)* and *(g)* of article 16, no paper document used to effect any such action is valid unless the use of data messages has been terminated and replaced by the use of paper documents. A paper document issued in these circumstances shall contain a statement of such termination. The replacement of data messages by paper documents shall not affect the rights or obligations of the parties involved.

(6) If a rule of law is compulsorily applicable to a contract of carriage of goods which is in, or is evidenced by, a paper document, that rule shall not be inapplicable to such a contract of carriage of goods which is evidenced by one or more data messages by reason of the fact that the contract is evidenced by such data message or messages instead of by a paper document.
(7) The provisions of this article do not apply to the following: [...].

Gradually the Act was amended on 5th February,2009 being the Amendment No.10 of 2009 which has introduced the world digital signature instead of electronic signature as provided under Chapter II of Section 3 of the Act. In Section 2, Clause (ha) was introduced after the word (h) which provides the Communication device. It reads as under:

"Communication device" means cell phones, personal digital assistance or combination of both or any other device used to communicate, send or transmit any text, video, audio or image;"

The Information Technology Act,2000 came into force on 17th October, 2000. It has 94 sections divided into 13 chapters. This Act was amended vide notification dated 27th October,2009.

In the Advanced Law Lexicon, the `Cyber law' deals with the computers and the Internet. Rather we can say as a computerized process.

Advanced Law Lexicon, 3rd edition 2005 has defined the same in the word of `Cyberspace". It has used a term as a `floating' in an electronic environment, which is accessible internationally. Then the Author has also defined the `Cyber theft' known as the act of using an online computer service.

In this dictionary `Cyber law' is defined as under:-

> "The field of law dealing with computers and the Internet including such issues as intellectual property rights, freedom of expression, and free access to information."

In the Advanced Law Lexicon, the `Cyber law' deals with the computers and the Internet. Rather we can say as a computerized process.

Advanced Law Lexicon, 3rd Edition 2005 has defined **`Cyber theft'** known as the act of using an online computer service.

In this dictionary **`Cyber law'** is defined as under**: -**

> "The field of law dealing with computers and the Internet, including such issues as intellectual property rights, freedom of expression, and free access to information."

The definition of the Information Technology Act provides as under:

"Computer" means any electronic, magnetic, optical or other high speed date processing device or system which performs logical, arithmetic, and memory functions by manipulations of electronic, magnetic or optical impulses, and includes all input, output, processing, storage, computer software, or communication facilities which are connected or related to the computer in a computer system or computer network;

JURISDICTION

Section 1(2) of the Information Technology Act,2000 reads as under:-

> "1(2) "It shall extend to the whole of India and, save as otherwise provide din this Act, it applies also to any offence or contravention hereunder committed outside India by any person."

PROVISIONS RELATING TO JURISDICTION IN CYBER SPACE UNDER THE INFORMATION TECHNOLOGY ACT,2000

The most powerful invention of the 20th Century is the **information and communication technology** for the society and its application for the society development such as administration of **Information and Communication technology** in judicial system will play an integral role for the society to trust on its

judicial process, due to its inherent advantage of fast processing, Trivial retrieval, less human intervention, relatively low cost of development and in some criminal cases where physical presence is an issue this solution is the best one .

The offences under the Information Technology Act are as under:

Section 65. Tampering computer source documents.-Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy, or alter any computer source code used for a computer, computer programme, computer system or computer network, when the computer source code is required to be kept or maintained by law for the time being in force, shall be punishable with imprisonment upto three years, or with fine which may extend upto two lakh rupees, or with both.

Section 66 . Computer related offence.- If any person, dishonestly or fraudulently, does any act referred to in section 43, he shall be punishable with imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.
.

Section 66A. Punishment for sending offensive messages through communication service etc. Any person who sends, by means of a computer resource or a communication device.-

(a) any information that is grossly offensive or has menacing character; or

(b) any information which he knows to be false, but for the purpose of causing annoyance, inconvenience, danger, obstruction, insult, injury, criminal intimidation, enmity, hatred or ill will, persistently by making use of such computer resource or a communication device; or

(c) any electronic mail or electronic mail message for the purpose of causing annoyance or inconvenience or to deceive or to mislead the addressee or recipient about the origin of such messages, shall be punishable with imprisonment for a term which may extend to three years and with fine.

Section 66B. Punishment for dishonestly receiving stolen computer resource or communication device. – Whoever dishonestly received or retains any stolen computer resource or communication device knowing or having reason to believe the same to be stolen computer resource or communication device, shall be punished with imprisonment of either description for a term which may extend to three years or with fine which may extend to rupees one lakh or with both.

Section 66C:Punishment for identity theft.-Whoever, fraudulently or dishonestly make use of the electronic signature, password or any other unique identification feature of any other person, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to rupees one lakh.

Section 66D:Punishment for cheating by personation by using computer resource.-Whoever, by means for any communication device or computer resource cheats by personating, shall be punished with imprisonment of either description for a term which may extend to three years and shall also be liable to fine which may extend to one lakh rupees.

Section 66E: Punishment for violation of privacy.-Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three yeas or with fine not exceeding two lakh rupees, or with both.

Section 66F. Punishment for cyber terrorism:-

(1) Whoever,-

(A) with intent to threaten the unity, integrity, security or sovereignty of India or to strike terror in the people or any section of the people by-

(i) denying or cause the denial of access to any person authorized to access computer resource; or

(ii) attempting to penetrate or access a computer resource without authorization or exceeding authorized access; or

(iii) introducing or causing to introduce any computer contaminant; and by means of such conduct causes or is likely to cause death or injuries to persons or damage to or destruction of property or disrupts or knowing that it is likely to cause damage or disruption of supplies or services essential to the life of the community or adversely affect the critical information infrastructure specified under section 70 or

(B) knowingly or intentionally penetrates or accesses a computer resource without authorization or exceeding authorized access, and by means of such conduct obtains access to information, data or computer database that is restricted for reasons of the security of the State or foreign relations; or any restricted information, data or computer database, with reasons to believe that such information, data or computer database so obtained may be used to cause or likely to cause injury to the interests of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States, public order, decency or morality, or in relation to contempt of court, defamation or incitement to an offence, or to the advantage of any foreign nation, group of individuals or otherwise.

Commits the offence of cyber terrorism.

(2) Whoever commits or conspires to commit cyber terrorism shall be punishable with imprisonment which may extend to imprisonment for life.'

Section 67. Punishment for publishing or transmitting obscene material in electronic form.-Whoever publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it, shall be punished on first conviction with imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to five years and also with fine which may extend to ten lakh rupees.

Section 67A. Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form. Whoever publishes or transmits or causes to be published or transmitted in the electronic form any material which contains sexually explicit act or conduct shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Section 67B:Punishment for publishing or transmitting of material depicting children in sexually explicit act etc. in electronic form.-Whoever-

(a) publishes or transmits or causes to be published or transmitted material in any electronic form which depicts children engaged in sexually explicit act or conduct; or

(b) creates text or digital images, collects, seeks, browses, downloads, advertises, promotes, exchanges or distributes material in any electronic form depicting children in obscene or indecent or sexually explicit manner; or

(c) cultivates, entices or induces children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or

(d) facilitates abusing children online, or

(e) records in any electronic form own abuses or that of others pertaining to sexually explicit act with children,

shall be punished on first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to ten lakh rupees and in the event of second or subsequent conviction with imprisonment of either description for a term which may extend to seven years and also with fine which may extend to ten lakh rupees.

Provided that provisions of Section 67, Section 67A and this section does not extend to any book, pamphlet, paper, writing, drawing, painting representation or figure in electronic form.

Section 67C. Preservation and retention of information by Intermediaries. (1) Intermediary shall preserve and retain such

information as may be specified for such duration and in such manner and format as the Central Government may prescribe.
(2) Any intermediary who intentionally or knowingly contravenes the provisions of sub-section (1) shall be punished with an imprisonment for a term which may extend to three years and also be liable to fine.

Section 70. Protected system.-(1)The appropriate Government may, by notification in the Official Gazette, declare any computer resource which directly or indirectly affects the facility of Critical Information Infrastructure, to be a protected system.
(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub section (1).
(3)Any person who secures access or attempts to secure access to a protected system in contravention of the provisions of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.
(4) The Central Government shall prescribe the information security practices and procedures for such protected system.

Section 71.Penalty for misrepresentation.—Whoever makes any misrepresentation to, or suppresses any material fact from the Controller or the Certifying Authority for obtaining any licence or (Electronic Signature) Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 72. Breach of Confidentiality and Privacy.- Save as otherwise provided in this Act or any other law for the time being in force, if any person who, in pursuance of any of the powers conferred under this Act, rules or regulations made thereunder, has secured access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Section 72A Punishment for disclosure of information in breach of lawful contract.—Save as otherwise provided in this Act or any other law for the time being in force, any person

including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person, shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both.

Section 73. Penalty for Publishing (Electronic Signature) Certificate false in certain particulars.- (1) No person shall publish a (Electronic Signature) Certificate or otherwise make it available to any other person with the knowledge that-

(a) the Certifying Authority listed in the certificate has not issued it, or
(b) the subscriber listed in the certificate has not accepted it, or
(c) the certificate has been revoked or suspended.,

unless such publication is for the purpose of verifying a (electronic signature) created prior to such suspension or revocation.

(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

.

Section 78 of I.T. Act empowers Inspector of Police to investigate cases under the Act.

JURISDICTION UNDER THE INDIAN PENAL CODE IN RELATION TO CYBER OFFENCES

(i)	Sending threatening messages by email	Section 503 IPC
(ii)	Sending defamatory messages by email	Section 499 IPC
(iii)	Forgery of electronic records	Section 463 IPC
(iv)	Bogus websites, cyber frauds	Section 420 IPC
(v)	Email spoofing	Section 463 IPC
(vi)	Web-jacking	Section 383 IPC

(vii)	E-Mail Abuse	Section 500 IPC
(viii)	Online sale of Drugs	NDPS Act
(ix)	Online sale of Arms	Arms Act

For adjudicating of the dispute under the Information Technology Act, Section 46 was enacted which has given the power for adjudication of the crimes. The power has been given to the Secretary, Information Technology and he has power to adjudge the quantum of compensation under Sections 46 and 47 of the Act.

Sections 46 and 47 are quoted below:

46. **Power to adjudicate.-**

(1) For the purpose of adjudging under this Chapter whether any person has committed a contravention of any of the provisions of this Act or of any rule, regulation, direction or order made hereunder the Central Government shall, subject to the provisions of Sub-section (3), appoint any officer not below the rank of a Director to the Government of India or an equivalent officer of a State Government to be an adjudicating officer or holding an inquiry in the manner prescribed by the Central Government.

(2) The adjudicating officer shall, after giving the person referred to in Sub-section (1) a reasonable opportunity for making representation in the matter and if, on such inquiry, he is satisfied that the person that the person has committed the contravention, he may impose such penalty or award such compensation as he thinks fit in accordance with the provisions of that section.

(3)No person shall be appointed as an adjudicating officer unless he possesses such experience in the field of Information Technology and legal or judicial experience as may be prescribed by the Central Government.

(4)Where more than one adjudicating officer are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.

(5)Every adjudicating officer shall have the powers of a civil court which are conferred on the Cyber Appellate Tribunal under Sub-Section (2) of Section 58, and-

(a)All proceedings before it shall be deemed to be judicial proceedings within the meaning of Sections 193 and 228 of the Indian Penal Code (45 of 1860)

(b)Shall be deemed to be a civil court for the purposes of Sections 345 and 346 of the Code of Criminal Procedure, 1973 (2 of 1974)
(c) shall be deemed to be a civil court for purposes of Order XXI of the Civil Procedure Code,1908 (5 of 1908)

47. Factors to be taken into account by the adjudicating officer. -

While adjudging the quantum of compensation under this Chapter, the adjudicating officer shall have due regard to the following factors, namely-

(a)The amount of gain of unfair advantage, wherever quantifiable, made as a result of the default.

(b)The amount of loss caused to any person as a result of the default;

(c) The repetitive nature of the default.

Sections 43 and 44 of the Information Technology Act,2000 provides penalties and their Adjudication. It reads as under:

Penalties and Adjudication

43. Penalty for damage to computer to com0puter, computer system etc.- If the person without permission of the owner or any other person who is in charge of a computer, computer system or computer network-
   (a) Accesses or secures access to such computer, computer system or computer network;
   (b) Downloads, copies or extracts any data, computer date-base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
   (c) Introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;

(d) damages or causes to be damaged any computer, computer system or computer network, data computer data base or any other programmes residing in such computer, computer system or computer network;

(e) Disrupts or causes disruption of any computer, computer system or computer network;

(f) denies or causes the denial of access to any person authorized to access any computer, computer system or computer network by any means;

(g) provides any assistance to any person to facilitate access to a computer, computer system or computer network in contravention of the provisions of this Act. Rules or Regulations made hereunder;

(h) charges the services availed of by a person to the account of another person by tampering with or manipulating any computer, computer system or computer network.

(i) destroy, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;

(j) steal, conceals, destroys or alters or causes any person to steal, conceal, destroy or alter any computer source code used for a computer resource with an intention to cause damage;

He shall be liable to pay damages by way of compensation to the person so affected.

Explanation.-For the purposes of this section-

(i)"computer contaminant" means any set of computer instructions that are designed-
(a)to modify, destroy, record, transmit data or programme residing within a computer system or computer network;
(b) by any means to usurp the normal operation of the computer, computer system or computer network;

(ii) "computer data-base" means a representation of information knowledge, facts, concepts or instructions in text, image, audio, \ video that are being prepared or have been prepared or have been prepared in a formalized manner or have been produced by a computer, computer system or system or computer network and are intended for use in a computer, computer system or computer network.

(iii) "Computer virus" means any computer instruction; information, data or programme that destroys, damages degrades or adversely affects the performance of a computer.

(iv) "damage" means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

(v) "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

44. **Penalty for failure to furnish information, return, etc**.- If any person who is required under this Act or any rules or regulations made thereunder to-

(a) furnish any document, return or report to the Controller of the Certifying Authority fails to furnish the same, he shall be liable to a penalty not exceeding one lakh and fifty thousand rupees for each such failure;

(b) file any return or furnish any information, books or other documents within the time specified therefore in the regulations fails to file return or furnish the same within the time specified therefore in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues;

(c) maintain books of account or records fails to maintain the same, he shall be liable to a penalty not exceeding ten thousand rupees for every day during which the failure continues.

45. **Residuary penalty**.- Whoever contravenes any rules or regulations made under this Act, for the contravention of which no penalty has been separately provided, shall be liable to pay a compensation not exceeding twenty five thousand rupees to the person affected by such contravention or a penalty not exceeding twenty five thousand rupees.

After the decision of the Adjudicating Officer, the appeal lies to the Appellate Tribunal under Section 48 of the Information Technology Act,2000. It reads as under:

"48.Establishment of Cyber appellate Tribunal.- (1) The Central Government shall, by notification, establishes one or more

appellate tribunals to be known as the Cyber Regulation Appellate Tribunal.

(2) The Central Government shall also specify, in the notification referred to in Sub-section (1), the matters and places in relation to which the Cyber Appellate Tribunal may exercise jurisdiction."

He exercises the powers contained under Section 58 of the Information Technology Act, which reads as under:-

58. Procedure and powers of the Cyber Appellate Tribunal.-

(1) The Cyber Appellate Tribunal shall not be bound by the procedure laid down by the Code of Civil Procedure, 1908 but shall be guided by the principles of natural justice and, subject to the other provisions of this Act and of any rules, the Cyber Appellate Tribunal shall have powers to regulate its own procedure including the place at which it shall have its sittings.

(2)The Cyber Appellate Tribunal shall have, for the purposes of discharging its functions under this Act, the same powers as are vested in a civil court under the Code of Civil Procedure, 1908, while trying a suit, in respect of the following matters, namely-

(a)Summoning and enforcing the attendance of any person and examining him on oath;

(b)Requiring the discovery and production of documents or other electronic records;

(c)Receiving evidence on affidavits;

(d) Issuing commissions for the examination of witnesses or documents;

(e) Reviewing its decisions

(f) dismissing an application for default or deciding its ex parte;

(g) any other matter which may be prescribed.

(3)Every proceeding before the Cyber Appellate Tribunal shall be deemed to be a judicial proceeding within the meaning of Sections

193 and 228, and for the purposes of Section 196 of the Indian Penal Code and the Cyber Appellate Tribunal shall be deemed to be a civil court for the purposes of Section 195 and Chapter XXVI of the Code of Criminal Procedure.

According to its preamble, the IT Act basically seeks to:

Provide legal recognition for electronic commerce.

Section 1(2) of the Information Technology Act, 2000 reads as under:-

> 1(2) "It shall extent to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention hereunder committed outside India by any person."

The aforesaid definition covers the offences or contravention even committed outside India by any person.

SECURITY PROCEDURE

The role of intellectuals in curbing terrorism also has been given a shape from other Acts also like Information Technology Act where Section 16 has been incorporated for the security measures in order to avoid terrorism. Said section is quoted below:-

16. 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-

(a) the nature of the transaction;
(b) the level of sophistication of the parties with reference to their technological capacity;
(c) the volume of similar transactions engaged in by other parties;
(d) the availability of alternatives offered to but rejected by any party;

(e) the cost of alternative procedures; and
(f) the procedures in general use for similar types of transactions or communications.

In order to curb the terrorism, apart from the intellectuals, judiciary also plays an important role, being guardian of the creation of our Constitution.

So far as Information Technology Act is concerned, Section 1(2) and Section 75 provides as under:-

1. **Short title, extent, commencement and application**.-
(1)……..

(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 there under committed outside India by any person.

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.

If we come to the universal declaration of human rights, 1948, it contains 29 Articles. It contains the frame of equal dignity and the rights. The form of human rights also contains in the judgment of the Apex Court in Kapila Hingdorani Vs. State of Bihar 2003 (7) AIC 18 (SC) 194, which provides that the right to food is an essential part of the human rights. It reads as under:-

Paragraph- 50: The term 'life' used in Article 21 of the Constitution of India has a wide and far-reaching concept. It includes livelihood and so many other facets thereof. `Life' as observed by Field, J.in Munn V.Illinois 11877(94)US 11311 means something more than mere animal existence and the inhibition against the deprivation of life extends to all those limits and facilities by which life is enjoyed. (See Board of Trustees of the Port of Bombay Vs. Dilipkumar Raghvendranath Nadkarni and others 1983 (1) SCC 124 and Olga Tellis and others Vs. Bombay Municipal Corporation and others 1985(3) SCC 545.

The Constitution envisages the establishment of a welfare State at the federal level as well as at the State level. In a welfare State the primary duty of the Government is to secure the welfare of the people Providing adequate medical facilities for the people is an essential part of the obligations undertaken by the Government in a welfare State.

In Kharak Singh Vs. State of U.P.AIR 1963 SC 1295, the Supreme Court acknowledged that the term "life" means something more than mere animal existence. The inhabitation against its deprivation extended to all those limbs and faculties by which the life is enjoyed. It equally prohibited the mutilation of the body by the amputation of an arm or leg, or putting out of an eye, or the destruction of any other organ by the body through which the soul communicates with the outer world. It postulates to be free from restrictions on the enjoyment of a decent, respectable and healthy life. Right of life under Article 21 of the Constitution is a right of a person to be free from restrictions or encroachment. Where imposed directly or directly brought about by calculated measures.

National Human Rights Courts.- For the purpose of providing speedy trial offences arising out of violation of human rights, the State Government may, with the concurrence of the Chief Justice of the High Court, by notification, specify for each district a Court of Session to be a Human Rights Court to try the said offences;

Provided that nothing in this section shall apply if

(a) A court of Session is already specified as a Special Court; or
(b) A Special Court is already constituted, for such offences under any other law for the time being in force.

These are the courts, which are being shared by the Intellectuals.

Although the Human Rights courts have been established but in various States, the courts are lacking. There are no courts of Human Rights. If the courts of Human Rights are established at every place, we can pursue the wrong doers for a remedy from the Human Rights courts.

In view of the aforesaid, the nut shell is that the responsibilities of Intellectuals in order to curb the terrorism has been conferred not only on the statutory protection given by the Prevention of Terrorism Act,2002 but also by the International Law through the process of International Court of Justice and United Nations organization, National Human Rights Commission and now by the Information Technology Act which contains a special enactment for the security in order to get rid of the Terrorist Act. After the enforcement of Information Technology Act, 2000, the entire terrorism has now shifted to the process of Internet device and for that purpose Forensic Labs have been established in Kolkata, Allahabad, Hyderabad and New Delhi. Time has come when the Government is to take steps to establish the Forensic Labs in every State in order to curb the terrorism. The time has also come where in the shape of International Court of Justice namely Human Rights Commission and International Treaty concerning Cyber law are also required to be established covering the cyber space which dealt with the cyber crimes with no geographical back ground.

Intellectual property (IP) refers to creations of the mind:inventions, literary and artistic works and symbols, names, images and designs used in comerce.

Intellectual property is divided into two categories: Industrial propety, which includes inventions (patents), trademarks, Industrial designs, and geographic indications of source; and Copyright which includes literary and artistic works such as novels, poems and plays, films, musical works, artistic works such as drawings, paintings, photographs and sculptures and archtectual designs. Rights related to copyright include those of performing artists in their performances, producers of phonograms in their recordings, and those of broadcasters in their radio and television programs.

Intellectual Property is the most important part of the modern business. Intellectual property which is a combination of copyright, trademark, design, geographical indication, patent, industrial design, integrated circuit, is valuable assets of any Company.

In the year 1999 the word `Intellectual property organization drafted for resolving the disputes over domain name. Those standards became the basis for the Uniform disputes Resolution Policy on which the Internet administration body has based its own draft rules.

Intellectual property (**IP**) is a term referring to a number of distinct types of legal monopolies over creations of the mind, both artistic and commercial, and the corresponding fields of law.[1] Under intellectual property law, owners are granted certain exclusive rights to a variety of intangible assets, such as musical, literary, and artistic works; discoveries and inventions; and words, phrases, symbols, and designs. Common types of intellectual

property include copyrights, trademarks, patents, industrial design rights and trade secrets in some jurisdictions.

Although many of the legal principles governing intellectual property have evolved over centuries, it was not until the 19th century that the term *intellectual property* began to be used, and not until the late 20th century that it became commonplace in the United States. The British Statute of Anne 1710 and the Statute of Monopolies 1623 are now seen as the origin of copyright and patent law respectively.

Enforcement of intellectual property rights

The enforcement provisions are contained in Part – III of the Agreement of Trade Related Aspects of Intellectual Property Rights (TRIPS Agreement). On 15.12.1993, the negotiations under the Uruguay Round in the framework of the General Agreement on Tariffs and Trade (GATT) were concluded. One of the many areas of negotiations was intellectual property, which had not before been under the GATT regime. The result of the negotiations is contained in the TRIPS Agreement was formally signed at Marrakech, Morocco on 15.04.1994 and entered into force on 1.1.1995. The new organization set up under the Uruguay Round, the World Trade Organization (WTO) started its work on 1.1.1995.

The TRIPs Agreement contains a special regime for intellectual property which is partly self-contained, partly based on the contents of the conventions administered by WIPO primarily the Paris, Berne, Rome Conventions and also the Washington Treaty on Integrated Circuits.

There are three principal features of the TRIPs Agreement. The first is "adequate norms and minimum standards for the protection of intellectual property" second "effective enforcement of these norms and standards, both domestic and at the boarder" and third availability of an effective dispute settlement mechanism to ensure the obligations to provide adequate norms and standards and their effective enforcement are complied with by members.

In the case of Exphar Sa v. Eupharma Laboratories Ltd. (2004) 3 SCC 688 the Supreme court has held as follows: (p.693, paras 12-13)

> "12. We would like to emphasize the word 'include'. This shows that the jurisdiction for the purposes of Section 62 is wider than that of the court as prescribed under the Code of civil Procedure, 1908. The relevant extract for the report of the Joint Committee published in the Gazette of India dated 23.11.1956 which proceeded and laid the foundation for Section 62(2) said:
> "In the opinion of the Committee many authors are deterred from institution infringement proceedings because the court in which such proceedings are to be instituted is situated at a considerable distance from the place of their ordinary residence. The Committee feels that this impediment should be removed and the new – section (2) accordingly provides that infringement proceedings may be instituted in the in the District Court within the local limits of whose jurisdiction the person instituting the proceedings ordinarily resides, carries on business, etc.'
>
> 13. It is, therefore, clear that the object and reason for the introduction of sub-section (2) of Section 62 was not to restrict the owners of the copyright to exercise their rights but to remove any impediment from their doing so. Section 62(2) cannot be read as limiting the jurisdiction of the district Court only to cases where the person instituting the suit or other proceeding, or where there are more than one such persons, any of them actually and voluntarily resides or carries on business or presently works for gain. It prescribes an additional ground for attracting the jurisdiction of a court over and above the 'normal' grounds as laid down in Section 20 of the Code."

In the case of Indian Performing Right Society Ltd. v. Eastern Indian Motion Pictures Assn. (1977) 2 SCC 820 Krishna Iyer, J. has held as under: (SCC pp. 833-34, paras 22 and 24).

"22. The creative intelligence of man is displayed in multiform ways of aesthetic expression but it often happens that economic systems so operate that the priceless divinity which we call artistic or literary creativity in man is expounded and masters, whose works are invaluable, are victims of piffling payments. World opinion in defence of the human right to intellectual property led to international conventions and municipal laws, commissions, codes and organizations, calculated to protect works of art. India responded to this universal need by enacting the copyright Act, 1957.

The Supreme Court has further defined intellectual property in Tata Consultancy Services v. state of A.P. (2001) 4 SCC 629 it has been held as under: (SCC p. 631, para 2).

"2. The case advanced on behalf of the appellants is that the branded software which is an intellectual property being the product of thought, creativity and intellectual efforts cannot be 'goods' for the purpose of the Act; that it is an intangible intellectual property and, therefore, cannot be 'goods'; that software is an essentially classic form of intellectual property; that the value of the tapes on which it is sold is much less than value of the software programm itself; that the software program is always transferred on to the hardware and then the tapes are useless; that, therefore, the licensee/prayer is paying for the program and not for the tapes or discs; these discs are different from music cassettes and videotapes, music reels, etc. because the program on the discs is of music cassettes, etc. though they may be separable and can be transferred to another cassette or tape this is not generally done and the music or movie remains on the tangible property on which it was stored when sold; that there are other methods by which a software programme can be installed, like, the program directly keying in the program through the console keyboard; that what is transferred in the right to use the programme (which is a set of instructions) and not the tape on which it is stored;"

In **Gramaphone Co. of India Ltd. v. Mars Recording (P) Ltd. (2002) 2 SCC 103** the Supreme Court has interpreted Section 52 of

the Copyright Act in respect of the record. The Supreme Court has held: (SCC p. 108, para8)

"Thus the use of words 'records embodying the record on the same 'record embodying the same record' clearly mean that it is only when the same signal has been kept, would there be a violation. If another signal is created, such as in the case of version recording, it is not an infringing copy within the meaning of Section 2(m). On this basis, it was submitted that Respondent 1 had satisfied the requirement of Section 52(1)(j) of the Act which is a defence to infringement of copyright."

The role of the judiciary, therefore, in the matter of intellectual property rights, its development and adjudication has been to take very drastic measures and the judiciary from time to time has interpreted various provisions of the infringement of copyright. In Eastern Book Co. v. Navin J. Desai (2002) 25 PTC 641 (Del) (DB) the Delhi High Court has defined when the copyright work shall be deemed to be infringed. Section 51 of the Copyright Act provides:

"51. When copyright infringed. – Copyright in a work shall be deemed to be infringed when any person without a licence granted by the owner of the copyright or the Registrar of copyrights under this Act or in contravention of the conditions of a licence so granted or of any condition imposed by a competent authority under this Act does anything, the exclusive right to do which is by this Act conferred upon the owner of the copyright, or permits for profit, any place to be used for the communication of the work to the public where such communication constitutes an infringement of the copyright in the work, unless he was not aware and had no reasonable ground for believing that such communication to the public would be an infringement of copyright; or when any person-makes for sale or hire, or sells or lets for hire, or by way of trade displays or offers for sale or hire, or distributes either for the purpose of trade or to such an extent as to affect prejudicially the owner of the copyright…."

Objectives

Financial incentive

These exclusive rights allow owners of intellectual property to reap monopoly profits. These monopoly profits provide a financial incentive for the creation of intellectual property, and, in case of patents, pay associated research and development costs. Some commentators, such as David Levine and Michele Boldrin, dispute this justification.

Economic growth

The legal monopoly granted by IP laws are credited with significant contributions toward economic growth. Economists estimate that two-thirds of the value of large businesses in the U.S. can be traced to intangible assets. "IP-intensive industries" are estimated to generate 72 percent more value added (price minus material cost) per employee than "non-IP-intensive industries".]

A joint research project of the WIPO and the United Nations University measuring the impact of IP systems on six Asian countries found "a positive correlation between the strengthening of the IP system and subsequent economic growth." [7] However, correlation does not necessarily mean causation: given that the patent holders can freely relocate, the Nash equilibrium predicts they will obviously prefer operating in countries with strong IP laws. is disputed] In some of the cases, the economic growth that comes with a stronger IP system is due to increase in stock capital from direct foreign investment, as was shown for Taiwan after the 1986 reform.

Economics

Intellectual property rights are temporary state-enforced monopolies regarding use and expression of ideas and information.

Intellectual property rights are usually limited to non-rival goods, that is, goods which can be used or enjoyed by many people simultaneously—the use by one person does not exclude use by another. This is compared to rival goods, such as clothing, which may only be used by one person at a time. For example, any number of people may make use of a mathematical formula simultaneously. Some objections to the term *intellectual property* are based on the argument that *property* can only properly be applied to rival goods (or that one cannot own "property" of this sort).

Since a non-rival good may be simultaneously used (copied, for example) by many people (produced with minimal marginal cost), monopolies over distribution and use of works are meant to give producers incentive to create further works. The establishment of intellectual property rights, therefore, represents a trade-off, to balance the interest of society in the creation of non-rival goods (by encouraging their production) with the problems of monopoly power. Since the trade-off and the relevant benefits and costs to society will depend on many factors that may be specific to each product and society, the optimum period of time during which the temporary monopoly rights should exist is unclear.

Jurisprudentially, Cyber law covers the whole of the world. World being one Unit treaties agreements made under the Intellectual Property Rights i.e. Trade Related Aspects known as Trips and General agreement on Tariff and Trade known as GATT

and World Trade Organization known as W.T.O are required to be entered.

The Central Forensic Science laboratory, Kolkata is a premier Science and Technology Institution which was established in the year 1957 with basic four disciplines of forensic science viz. Ballistics, Biology, Chemistry and Physics divisions under Union Ministry of Home. Later on laboratory was placed in the year 1971 under administrative control of a newly carved out department-BPR&D. In the year 2003, a separate Directorate of Forensic Science was created consisting of three Central Forensic Science Laboratories located at Kolkata, Hyderabad, Shimla, Chandigarh and Allahabad.

The Central Forensic Science Laboratory (CBI) New Delhi was established in the year 1968. The Laboratory at New Delhi is one of the most comprehensive Laboratories in the country.

As per report, during the year 2007, the Laboratory scientists gave expert testimony in 261 courts in Delhi and other parts of India and examined 82 Scene(s) of crime at Delhi and outside for scientific investigation of crimes. The services of this forensic science were also provided to Delhi Police, CBI and Judicial courts. Forensic assistance was also provided to Directorate of Revenue Intelligence, Banks, Cabinet Secretariat Board and other public undertakings on regular basis.

Section 61 of the Information Technology Act, 2000 also debars the civil court in respect of the matters which are being tried by the Cyber Tribunal and directly the appeal goes to the High Court against the judgment of the Cyber Appellate Tribunal.