Course Name- B.A.LL.B 4th sem / LL.B 2nd sem
Subject- Cyber Law
Teacher- Mrs. Aakanksha
Concept- Unit III Information Technology Act 2000

-Regulation of Certifying Authorities

The Information Technology Act, 2000 has established a Certifying Authority to regulate the electronic transactions. In this article, we will look at the various aspects of the regulation of certifying authorities.

IT Act, 2000 – Regulation of Certifying Authorities:

The following sections pertain to the regulation of certifying authorities:

Section 17 – Appointment of the Controller and other officers

- The Central Government may appoint a Controller of Certifying Authorities after notifying the Official Gazette. They may also appoint Deputy Controllers and Assistant Controllers as it deems fit.
- The Controller discharges his responsibilities subject to the general control and also directions of the Central Government
- The Deputy Controllers and Assistant Controllers shall perform the functions assigned to them by the Controller under the general superintendence and also control of the Controller.
- 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.
- 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.
- There shall be a seal of the Office of the Controller.

2. Functions of Controller (Section 18)

- A Controller performs some or all of the following functions:

- Supervise the activities of the Certifying Authorities and also certify their public keys
- Lay down the standards that the Certifying Authorities follow
- Specify the following:
- qualifications and also experience requirements of the employees of all Certifying Authorities
- conditions that the Certifying Authorities must follow for conducting business
- the content of the printed, written, and also visual materials and advertisements in respect of the digital signature and the public key
- the form and content of a digital signature certificate and the key
- the form and manner in which the Certifying Authorities maintain accounts
- terms and conditions for the appointment of auditors and their remuneration
- Facilitate the Certifying Authority to establish an electronic system, either solely or jointly with other Certifying Authorities and its regulation
- Specify the manner in which the Certifying Authorities deal with the subscribers

- Resolve any conflict of interests between the Certifying Authorities and the subscribers
- Lay down the duties of the Certifying Authorities
- Maintain a database containing the disclosure record of every Certifying Authority with all the details as per regulations. Further, this database is accessible to the public.

3. Recognition of Foreign Certifying Authority (Section 19)

- A Controller has the right to recognize any foreign certifying authority as a certifying authority for the purpose of the IT Act, 2000. While this is subject to the conditions and restrictions which the regulations specify, the Controller can recognize it with the previous approval of the Central Government and notify in the Official Gazette.
- If a controller recognizes a Certifying Authority under sub-section (i), then its digital signature certificate is also valid for the purpose of the Act.
- If the controller feels that any certifying authority has contravened any conditions or restrictions of recognition under sub-section (i), then he can revoke the recognition. However, he needs to record the reason in writing and notify in the Official Gazette.

4. Controller to act as a repository (Section 20)

- The Controller will act as a repository of all digital signature certificates under this Act.
- The Controller will –
- Make use of secure hardware, software, and also procedures.
- Observe the standards that the Central Government prescribes to ensure the secrecy and also the security of the digital signatures.
- The Controller will maintain a computerized database of all public keys. Further, he must ensure that the public keys and the database are available to any member of the public.

5. License to issue Digital Signature Certificates (Section 21)

(1) Subject to the provisions of sub-section (2), any person can apply to the Controller for a license to issue digital signature certificates.

(2) A Controller can issue a license under sub-section (1) only if the applicant fulfills all the requirements. The Central Government specifies requirements with respect to qualification, expertise, manpower, financial resources, and also infrastructure facilities for the issuance of digital signature certificates.

(3) A license granted under this section is –

(a) Valid for the period that the Central Government specifies

(b) Not transferable or inheritable

(c) Subject to the terms and conditions that the regulations specify

6. Power to investigate contraventions (Section 28)

The Controller or any other Officer that he authorizes will investigate any contravention of the provisions, rules or regulations of the Act.
The Controller or any other Officer that he authorizes will also exercise the powers conferred on Income-tax authorities under Chapter XIII of the Income Tax Act, 1961. Also, the exercise of powers will be limited according to the Act.

Duties Of Subscribers (Section 40 to 42)

With respect to the Electronic Signature Certificate the subscriber has to perform such duties as may be prescribed by the Act. Further every subscriber has to exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate. He has to take all steps to prevent its disclosure. In the event of the private key being compromised the subscriber has to communicate the same immediately to the Certifying Authority as specified by the Regulations. The subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

Section : 40. Generating key pair.

Where any Digital Signature Certificate, the public key of which corresponds to the private key of that subscriber which is to be listed in the Digital Signature Certificate has been accepted by a subscriber, then, the subscriber shall generate the key pair by applying the security procedure.

Section : 41. Acceptance of Digital Signature Certificate.

(1) A subscriber shall be deemed to have accepted a Digital Signature Certificate if he publishes or authorizes the publication of a Digital Signature Certificate—

(a) to one or more persons;
(b) in a repository, or otherwise demonstrates his approval of the Digital Signature Certificate in any manner.

(2) By accepting a Digital Signature Certificate the subscriber certifies to all who reasonably rely on the information contained in the Digital Signature Certificate that—

(a) the subscriber holds the private key corresponding to the public key listed in the Digital Signature Certificate and is entitled to hold the same;
(b) all representations made by the subscriber to the Certifying Authority and all material relevant to the information contained in the Digital Signature Certificate are true;
(c) all information in the Digital Signature Certificate that is within the knowledge of the subscriber is true.

Section : 42. Control of private key.

(1) Every subscriber shall exercise reasonable care to retain control of the private key corresponding to the public key listed in his Digital Signature Certificate and take all steps to prevent its disclosure to a person not authorized to affix the digital signature of the subscriber.

(2) If the private key corresponding to the public key listed in the Digital Signature Certificate has been compromised, then, the subscriber shall communicate the same without any delay to the Certifying Authority in such manner as may be specified by the regulations.

Explanation.— For the removal of doubts, it is hereby declared that the subscriber shall be liable till he has informed the Certifying Authority that the private key has been compromised.

43. PENALTY FOR DAMAGE TO COMPUTER, COMPUTER SYSTEM, ETC.

If any person without permission of the owner or any other person who is incharge of a computer, computer system or computer network –

- accesses or secures access to such computer, computer system or computer network or computer resource];
- downloads, copies or extracts any data, computer data base or information from such computer, computer system or computer network including information or data held or stored in any removable storage medium;
- introduces or causes to be introduced any computer contaminant or computer virus into any computer, computer system or computer network;
- 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;
- disrupts or causes disruption of any computer, computer system or computer network;
- denies or causes the denial of access to any person authorised to access any computer, computer system or computer network by any means;
- 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 thereunder;
- 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) destroys, deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means;steal, conceal, 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;]

2[he shall be liable to pay damages by way of compensation to the person so affected.]

Explanation.–For the purposes of this section,–

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

- 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 in a formalised manner or have been produced by a computer, computer system or computer network and are intended for use in a computer, computer system or computer network;
- computer virus‖ means any computer instruction, information, data or programme that destroys, damages, degrades or adversely affects the performance of a computer resource or attaches itself to another computer resource and operates when a programme, data or instruction is executed or some other event takes place in that computer resource;
- damage‖ means to destroy, alter, delete, add, modify or rearrange any computer resource by any means.

1[(v) ―computer source code‖ means the listing of programme, computer commands, design and layout and programme analysis of computer resource in any form.]

3[43A. COMPENSATION FOR FAILURE TO PROTECT DATA.–

Where a body corporate, possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Explanation.–For the purposes of this section,–

- body corporate‖ means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities;
- reasonable security practices and procedures‖ means security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties or as may be specified in any law for the time being in force and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit;
- sensitive personal data or information‖ means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.]

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-

- furnish any document, return or report to the Controller or ?he 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.
- file any return or furnish any information, books or other documents within the time specified therefor in the regulations fails to file return or furnish the same within the

time specified therefor in the regulations, he shall be liable to a penalty not exceeding five thousand rupees for every day during which such failure continues.

- 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.

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, 1[direction or order made thereunder which renders him liable to pay penalty or compensation,] 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 for holding an inquiry in the manner prescribed by the Central Government.

2[(1A) The adjudicating officer appointed under sub-section (1) shall exercise jurisdiction to adjudicate matters in which the claim for injury or damage does not exceed rupees five crore:

Provided that the jurisdiction in respect of the claim for injury or damage exceeding rupees five crores shall vest with the competent court.]

- 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 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.
- 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.
- Where more than one adjudicating officers are appointed, the Central Government shall specify by order the matters and places with respect to which such officers shall exercise their jurisdiction.
- Every adjudicating officer shall have the powers of a civil court which are conferred on the―Appellate Tribunal‖ under sub-section (2) of section 58, and–
- 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);
- 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);

1[(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:–

- the amount of gain of unfair advantage, wherever quantifiable, made as a result of the default;
- the amount of loss caused to any person as a result of the default;
- the repetitive nature of the default.

OFFENCES UNDER THE ACT

The increased rate of technology in computers has led to the enactment of Information Technology Act 2000. The converting of the paperwork into electronic records, the storage of the electronic data, has tremendously changed the scenario of the country.

Offenses: Cyber offenses are the unlawful acts which are carried in a very sophisticated manner in which either the computer is the tool or target or both. Cybercrime usually includes:
(a) Unauthorized access of the computers (b) Data diddling (c) Virus/worms attack (d) Theft of computer system (e) Hacking (f) Denial of attacks (g) Logic bombs (h) Trojan attacks (i) Internet time theft (j) Web jacking (k) Email bombing (l) Salami attacks (m) Physically damaging computer system.

The offenses included in the IT Act 2000 are as follows:

1. Tampering with the computer source documents.
2. Hacking with computer system.
3. Publishing of information which is obscene in electronic form.
4. Power of Controller to give directions
5. Directions of Controller to a subscriber to extend facilities to decrypt information
6. Protected system
7. Penalty for misrepresentation
8. Penalty for breach of confidentiality and privacy
9. Penalty for publishing Digital Signature Certificate false in certain particulars
10. Publication for fraudulent purpose
11. Act to apply for offense or contravention committed outside India
12. Confiscation
13. Penalties or confiscation not to interfere with other punishments.
14. Power to investigate offenses.

Offenses UNDER THE IT ACT, 2000

1.Tampering with computer source documents:

Section 65 of this Act provides that 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 being time in force, shall be punishable with imprisonment up to three year, or with fine which may extend up to two lakh rupees, or with both.

Explanation:
For the purpose of this section "computer source code" means the listing of programmes, computer commands, design and layout and programme analysis of computer resource in any form.

Object:
The object of the section is to protect the "intellectual property" invested in the computer. It is an attempt to protect the computer source documents (codes) beyond what is available under the Copyright Law.

This section extends towards the Copyright Act and helps the companies to protect the source code of their programmes.

Section 65 is tried by any magistrate. This is cognizable and non- bailable offense.

Imprisonment up to 3 years and or Fine up to Two lakh rupees.

CASE LAWS
Frios v. State of Kerela:
Facts: In this case, it was declared that the FRIENDS application software as a protected system. The author of the application challenged the notification and the constitutional validity of software under Section 70. The court upheld the validity of both.
It included tampering with source code. Computer source code the electronic form, it can be printed on paper.

Held: The court held that Tampering with Source code is punishable with three years jail and or two lakh rupees fine of rupees two lakh rupees for altering, concealing and destroying the source code.

Syed Asifuddin case:

Facts: In this case, the Tata Indicom employees were arrested for manipulation of the electronic 32- bit number (ESN) programmed into cell phones theft were exclusively franchised to Reliance Infocom.
Held: Court held that Tampering with source code invokes Section 65 of the Information Technology Act.

Parliament Attack Case:
Facts: In this case, several terrorists attacked Parliament House on 13 December 2001. In this Case, the Digital evidence played an important role during their prosecution. The accused argued that computers and evidence can easily be tampered and hence, should not be relied.
In Parliament case, several smart device storage disks and devices, a Laptop was recovered from the truck intercepted at Srinagar pursuant to information given by two suspects. The laptop included the evidence of fake identity cards, video files containing clips of the political leaders with the background of Parliament in the background shot from T.V news channels. In this case design of Ministry of Home Affairs car sticker, there was game "wolf pack" with user name of 'Ashiq', there was the name in one of the fake identity cards used by the terrorist. No back up was taken. Therefore, it was challenged in the Court.

Held: Challenges to the accuracy of computer evidence should be established by the challenger. Mere theoretical and generic doubts cannot be cast on the evidence.

2. Hacking with the computer system:

Section 66 provides that- (1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Explanation: The section tells about the hacking activity.

Punishment: Imprisoned up to three years and fine which may extend up to two lakh rupees Or with both.

CASE LAWS
R v. Gold & Schifreen:
In this case, it is observed that the accused gained access to the British telecom Prestl Gold computers networks file amount to dishonest trick and not a criminal offense.

R v. Whiteley:
In this case, the accused gained unauthorized access to the Joint Academic Network (JANET) and deleted, added files and changed the passwords to deny access to the authorized users.
The perspective of the section does not merely protect the information but to protect the integrity and security of computer resources from attacks by unauthorized person seeking to enter such resource, whatever may be the intention or motive.

Cases Reported In India:
Official website of Maharastra government hacked. The official website of the government of Maharashtra was hacked by Hackers Cool Al- Jazeera, and claimed them they were from Saudi Arabia.

3. Publishing of obscene information in electronic form:

Section 67 of this Act provides that Whoever publishes or transmits or causes to be published 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 circumstance, 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 five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

CASE LAWS:
The State of Tamil Nadu v. Suhas Katti.
Facts: This case is about posting obscene, defamatory and annoying message about a divorcee woman in the Yahoo message group. E-mails were forwarded to the victim for information by the accused through a false e-mail account opened by him in the name of the victim. These postings resulted in annoying phone calls to the lady. Based on the complaint police nabbed the accused. He was a known family friend of the victim and was interested in marrying her. She married to another person, but that marriage ended in divorce and the accused started contacting her once again. And her reluctance to marry him he started harassing her through the internet.

Held: The accused is found guilty of offenses under section 469, 509 IPC and 67 of the IT Act 2000 and the accused is convicted and is sentenced for the offense to undergo RI for 2 years under 469 IPC and to pay fine of Rs.500/-and for the offense u/s 509 IPC sentenced to undergo 1 year Simple imprisonment and to pay fine of Rs.500/- and for the offense u/s 67 of IT Act 2000 to undergo RI for 2 years and to pay fine of Rs.4000/- All sentences to run concurrently.”

The accused paid fine amount and he was lodged at Central Prison, Chennai. This is considered the first case convicted under section 67 of Information Technology Act 2000 in India.

In a recent case, a groom’s family received numerous emails containing defamatory information about the prospective bride. Fortunately, they did not believe the emails and chose to take the matter to the police. The sender of the emails turned out to be the girl’s step-father, who did not want the girl to get married, as he would have lost control over her property, of which he was the legal guardian.

Avnish Bajaj (CEO of bazzee.com – now a part of the eBay group of companies) case.

Facts: There were three accused first is the Delhi schoolboy and IIT Kharagpur Ravi Raj and the service provider Avnish Bajaj.

The law on the subject is very clear. The sections slapped on the three accused were Section 292 (sale, distribution, public exhibition, etc., of an obscene object) and Section 294 (obscene acts, songs, etc., in a public place) of the Indian Penal Code (IPC), and Section 67 (publishing information which is obscene in electronic form) of the Information Technology Act 2000. In addition, the schoolboy faces a charge under Section 201 of the IPC (destruction of evidence), for there is apprehension that he had destroyed the mobile phone that he used in the episode.

These offenses invite a stiff penalty, namely, imprisonment ranging from two to five years, in the case of a first-time conviction, and/or fines.

Held: In this case, the Service provider Avnish Bajaj was later acquitted and the Delhi schoolboy was granted bail by Juvenile Justice Board and was taken into police charge and detained into Observation Home for two days.

4. Power of Controller to give directions:

Section 68 of this Act provides that (1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder.

(2) Any person who fails to comply with any order under sub-section (1) shall be guilty of an offense and shall be liable on conviction to imprisonment for a term not exceeding three years or to a fine not exceeding two lakh rupees or to both.

Explanation: Any person who fails to comply with any order under subsection (1) of the above section, shall be guilty of an offense and shall be convicted for a term not less than three years or to a fine exceeding two lakh rupees or to both.

The offense under this section is non-bailable & cognizable.

Punishment: Imprisonment up to a term not exceeding three years or fine not exceeding two lakh rupees.

5. Directions of Controller to a subscriber to extend facilities to decrypt information:

Section 69 provides that- (1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offense; for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.

(2) The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.

(3) The subscriber or any person who fails to assist the agency referred to in subsection shall be punished with imprisonment for a term which may extend to seven years.
Punishment: Imprisonment for a term which may extend to seven years. The offense is cognizable and non- bailable.

6. Protected System:

Section 70 of this Act provides that –

(1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network 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 provision 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.

Explanation: This section grants the power to the appropriate government to declare any computer, computer system or computer network, to be a protected system. Only authorized person has the right to access to protected system.

Punishment: The imprisonment which may extend to ten years and fine.

7. Penalty for misrepresentation:
Section 71 provides that- (1) Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or which fine which may extend to one lakh rupees, or with both.

Punishment: Imprisonment which may extend to two years or fine may extend to one lakh rupees or with both.

8. Penalty for breach of confidentiality and privacy:

Section 72 provides that- Save as otherwise provide in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulation made thereunder, has secured assess to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such 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.

Explanation: This section relates to any person who in pursuance of any of the powers conferred by the Act or it allied rules and regulations have secured access to any: Electronic record, books, register, correspondence, information, document, or other material.

If such a person discloses such information, he will be punished. It would not apply to disclosure of personal information of a person by a website, by his email service provider.

Punishment: Term which may extend to two years or fine up to one lakh rupees or with both.

9. Penalty for publishing Digital Signature Certificate false in certain particulars:

Section 73 provides that – (1) No person shall publish a Digital 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 digital 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.

Explanation: The Certifying Authority listed in the certificate has not issued it or, The subscriber listed in the certificate has not accepted it or the certificate has been revoked or suspended.

The Certifying authority may also suspend the Digital Signature Certificate if it is of the opinion that the digital signature certificate should be suspended in public interest.

A digital signature may not be revoked unless the subscriber has been given opportunity of being heard in the matter. On revocation, the Certifying Authority need to communicate the same with the subscriber. Such publication is not an offense it is the purpose of verifying a digital signature created prior to such suspension or revocation.

Punishment: Imprisonment of a term of which may extend to two Years or fine may extend to 1 lakh rupees or with both.

CASE LAWS:
Bennett Coleman & Co. v. Union of India
In this case, the publication has been stated that ‘publication means dissemination and circulation’. In the context of the digital medium, the term publication includes and transmission of information or data in electronic form.

10. Publication for fraudulent purpose:

Section 74 provides that- Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose shall be punished with imprisonment for a term which may extend to two years, or with fine which extends to one lakh rupees, or with both.

Explanation: This section prescribes punishment for the following acts:

Knowingly creating a digital signature certificate for any

1. fraudulent purpose or,
2. unlawful purpose.

Knowingly publishing a digital signature certificate for any

1. fraudulent purpose or
2. unlawful purpose

Knowingly making available a digital signature certificate for any

1. fraudulent purpose or
2. unlawful purpose.

Punishment: Imprisonment for a term up to two years or fine up to one lakh or both.

11. Act to apply for offense or contravention committed outside India:

Section 75 provides that- (1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offense or contravention committed outside India by any person irrespective of his nationality.

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

Explanation: This section has a broader perspective including cyber crime, committed by cyber criminals, of any nationality, any territoriality.

CASE LAW:

R v. Governor of Brixton prison and another
Facts: In this case the Citibank faced the wrath of a hacker on its cash management system, resulting in illegal transfer of funds from customers account into the accounts of the hacker, later identified as Valdimer Levin and his accomplices. After Levin was arrested he was extradited to the United States. One of the most important issues was the jurisdictional issue, the 'place of origin' of cyber crime.

Held: The Court held that the real-time nature of the communication link between Levin and Citibank computer meant that Levin's keystrokes were actually occurring on the Citibank computer. It is thus important that in order to resolve the disputes related to jurisdiction, the issue of territoriality and nationality must be placed by much broader criteria embracing principles of reasonableness and fairness to accommodate overlapping or conflicting interests of states, in spirit of universal jurisdiction.

12. Confiscation:

Section 76 provides that- Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provisions of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation:

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

Explanation: The aforesaid section highlights that all devices whether computer, computer system, floppies, compact disks, tape drives or any other storage, communication, input or output device which helped in the contravention of any provision of this Act, rules, orders, or regulations made under there under liable to be confiscated.

13. Penalties or confiscation not to interfere with other punishments:

Section 77 provides that – No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

Explanation: The aforesaid section lays down a mandatory condition, which states the Penalties or confiscation not to interfere with other punishments to which the person affected thereby is liable under any other law for the time being in force.

Power to investigate offenses:

Section 78 provides that – Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Deputy Superintendent of Police shall investigate any offense under this Act.

CONCLUSION

Due to the increase in digital technology, various offenses are increasing day by day. Therefore, the IT Act 2000 need to be amended in order to include those offenses which are now not included in the Act. In India, cybercrime is not of high rate. Therefore, we have time in order to tighten the cyber laws and include the offenses which are now not included in the IT Act 2000.

Since the beginning of civilization, man has always been motivated by the need to make progress and better the existing technologies. This has led to tremendous development and progress which has been a launching pad for further developments. Of all the significant advances made by mankind from the beginning to date, probably the most important of them is the development of the Internet.

However, the rapid evolution of the Internet has also raised numerous legal issues and questions. As the scenario continues to be still not clear, countries throughout the world are resorting to different approaches towards controlling, regulating and facilitating electronic communication and commerce.

MAKING OF RULES AND REGULATION

89. Power of Controller to make regulations. –

(1) The Controller may, after consultation with the Cyber Regulations Advisory Committee and with the previous approval of the Central Government, by notification in the Official Gazette, make regulations consistent with this Act and the rules made thereunder to carry out the purposes of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such regulations may provide for all or any of the following matters, namely:-

(a) the particulars relating to maintenance of data-base containing the disclosure record of every Certifying Authority under clause (m) of section 18;

(b) the conditions and restrictions subject to which the Controller may recognize any foreign Certifying Authority under sub-section (1) of section 19;

(c) the terms and conditions subject to which a license may be granted under clause © of sub-section (3) of section 21;

(d) other standards to be observed by a Certifying Authority under clause (d) of section 30;

(e) the manner in which the Certifying shall disclose the matters specified in sub-section (1) of section 34;

(f) the particulars of statement which shall accompany an application under sub-section (3) of section 35.

(g) the manner by which the subscriber communicate the compromise of private key to the Certifying Authority under sub-section (2) of section 42.

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

90. Power of State Government to make rules.–

(1) The State Government may, by notification in the Official Gazette, make rules to carry out the provisions of this Act.

(2) In particular, and without prejudice to the generality of the foregoing power, such rules may provide for all or any of the following matters, namely:–
(a) the electronic form in which filing, issue, grant, receipt or payment shall be effected under sub-section (1) of section 6;
(b) for matters specified in sub-section (2) of section 6;

(3) Every rule made by the State Government under this section shall be laid, as soon as may be after it is made, before each House of the State Legislature where it consists of two Houses, or where such Legislature consists of one House, before that House.