The Information Technology Act (hereinafter IT Act) manages cybercrime and electronic trade in India. It had been enacted in the year 2000 and implemented w.e.f. 17th October 2000. This Act encourages the development & utilization of computers, the web and programming in the nation too, as to provides a lawful system to the advancement of e-commerce and e-exchanges within the country. This Act consists of 94 Sections in 13 Chapters with Four Schedules accommodates for a legal framework for the evidentiary value of electronic record and wrongdoings which are of technological nature.

- **SALIENT FEATURES OF IT ACT**

1. This application applies to the whole of India including J&K
2. Lawful acknowledgement for electronic records and digital signatures
3. Safety measures for electronic records and also digital signatures are in place
4. Licensing and instruction of Certifying authorities for issuing digital signature certificates
5. Protect the systems and data
6. Appointment of adjudicating officials for holding requests under the Act is decided
7. Arrangement for founding up a Cyber Regulatory Appellant Tribunal under the Act. This tribunal will affect all bids made against the request for the Controller or Adjudicating Officer.
8. An appeal against the request for the Cyber Appellant Tribunal is conceivable just within the High Court
9. Appointment of the Controller of Certifying Authorities (CCA) to licence and manage the working of Certifying Authorities. The Controller to go about as a source of each digital signature.
10. Provisions for the constitution of a Cyber Regulations Advisory Committee to direct the Central Government and Controller.
11. This Act to use for offences or violations committed outside India

1. BRIEF EXPLANATION OF SECTION 87(2) OF THE IT ACT

[1]Section 87 deals with the Power of the Central Government to make rules.

- *In particular, and without partiality to the generality of the preceding power, such rules may provide for all or any of the subsequent matters, namely: –*
- *the conditions for considering the reliability of electronic signature or electronic authentication technique under sub-section (2) of section 3A[1];*
- *the procedure for establishing electronic signature or authentication under sub-section (3) of section 3A;*

  (ab) the way within which any information or matter could also be authenticated through electronic signature under section 5[2];

- *the electronic form within which filing, issue, grant or payment shall be effected under sub-section (1) of section 6[3];*
- *the manner and format during which electronic records shall be filed, or issued and also the method of payment under sub-section (2) of section 6;*

  (ca) the way within which the authorised service provider may collect, retain and appropriate service charges under sub-section (2) of section 6A[4];

- *the matters regarding the type of digital signature, manner and format during which it may going to be affixed under section 10[5];*
- *the manner of storing and affixing electronic signature creation data under section 15[6];*

  (ea) the safety procedures and practices under section 16[7];

- *the qualifications, experience and terms and conditions of service of Controller, Deputy Controllers and Assistant Controllers under section 17[8];*
- *the requirements which an applicant must fulfil under sub-section (2) of section 21[9];*
- *the period of validity of licence approved under clause (a) of sub-section (3) of section 21;*
- *the form during which an application for a licence may also make under sub-section (1) of section 22[10];*

- *the sum of fees payable under clause (c) of sub-section (2) of section 22;*
- *such other documents which shall accompany a request for a licence under clause (d) of subsection (2) of section 22;*
- *the form and thus the fee for renewal of a licence and also the fee payable thereof under section 23[11];*

(ma) the procedure of application and fee for issue of Electronic Signature Certificate under section 35[12];

- *the form during which application for issue of a digital signature certificate can also be made under sub-section (1) of section 35;*
- *the fee to be paid to the Certifying Authority for the issue of a digital signature certificate under sub-section (2) of section 35;*

(oa) the duties of subscribers under section 40A[13];

(ob) the reasonable security practices and procedures and sensitive personal information or data under section 43A[14];

- *the method within which the adjudicating officer shall hold an inquiry under sub-section (1) of section 46[15];*
- *the qualification and therefore the knowledge which the adjudicating officer shall possess under sub-section (3) of section 46;*
- *the procedure within which appeal may also be filed and thus the fee thereof under sub-section (3) of section 57[16];*
- *any other power of a civil court required to be prescribed under clause (g) of sub-section (2) of section 58[17];*
- *the powers and functions of the Chairperson of the Cyber Appellate Tribunal under section 52A;*
- *the information, duration, manner and form of such information to be retained and preserved under section 67C[18];*
- *the procedures and safeguards for the interception, monitoring or decryption under sub-section (2) of section 69[19];*
- *the procedures and safeguards for blocking for access by the general public under sub-section (3) of section 69A[20];*

(za) the procedure and safeguards for observation and collecting traffic information or data under sub-section (3) of section 69B[21];

(zb) the info security practices and procedures for a protected system under section 70[22];

(zc) the way of performing functions and duties of the agency under sub-section (3) of section 70A[23];

(zd) the officers and employees/workers under sub-section (2) of section 70B[24];

(ze) salaries and allowances and terms and conditions of service of the Director-General and other officers and workers under sub-section (3) of section 70B;

(zf) the approach within which the functions and duties of an agency shall be performed under sub-section (5) of section 70B;

(zg) the procedures to be observed by the intermediaries under sub-section (2) of section 79[25];

(zh) the modes or ways for encryption under section 84A[26].

1. **Section 3A** deals with **Digital Signature** where (2) says any digital signature considered that the signature creation data used to link, control to the authenticator only & no other person and any data after any kind of change to the digital signature is detachable. (3) says the Central Government may prescribe the procedure of discovering whether the digital signature of the person is authenticated or not.
2. **Section 5** deals with the **Legal recognition of digital signature** which says any law provides that any information shall be authenticated by attaching the signature then that information deemed to be satisfied in such a manner which had been prescribed by the Central Government.
3. **Section 6** deals with **Use of electronic records and digital signatures in the Government and its agencies**. (1) says that the filing of any application with any agency controlled by the appropriate government and approval of any licence, sanction by whatever name must be in a prescribed manner as well by the

appropriate government. (2) The appropriate government prescribes the manner and format of electronic record filing or any method of payment charges filing.

4. **Section 6A** deals with the **Delivery of services by service provider**. (2) The appropriate government approve any service provider such as private company, partnership firm etc. to collect charges prescribed by the appropriate government.
5. **Section 10** deals with **Power to make rules by Central Government in respect of digital electronics** which says that the Central government can prescribe the type, manner and procedure in which digital signature shall be attached and simplifies identification. They also control the processes to ensure the security of electronic records or any other matter which may necessary to give lawful effect to a digital signature.
6. **Section 15** deals with **Secure digital signature** which says that if the private key of the subscriber during the time of attaching signature was under control and when the private key of the subscriber data was stored attached in such manner as may be prescribed, then a digital signature shall be deemed to be a secure digital signature.
7. **Section 16** deals with **Security procedures and practices** which says the Central Government purposes to prescribe the security to electronic record and electronic signature.
8. **Section 17** deals with the **Appointment of Controller and other officers** which says the Central Government may notify in the Official Gazette to appoint a Controller of Certifying Authorities of this act to perform the functions assigned to them, discharge his function. The qualification and experience for CCA will be prescribed by the Central Government.
9. **Section 21** deals with **Licence to issue digital signature certificates**. (2) The Central Government prescribed that no licence shall be issued unless the applicants have fulfilled the requirement of qualifications, financial resources, etc. (3) The licence under this section must be valid for such period prescribed by the Central Government, not to be transferable and according to the terms and condition specified by the regulations.
10. **Section 22** deals with the **Application for a licence**. (1) Every application for the issue of the licence must be in the form prescribed by the Central Government. (2) It shall be attended by a certification practice statement, identification of applicant by the

procedure of the statement, payment of a fee not exceeding Rs. 25,000, and other documents prescribed by the Central Government.

11. **Section 23** deals with **Renewal of licence** which says that it shall be in such form that attended by such fees which are not exceeding Rs. 5,000 and not less than 40 days before the expiry of the validity of the licence, as may be prescribed by the Central Government.

12. **Section 35** deals with **Certifying authority to issue a digital signature certificate**. (1) Any person who makes an application under this act may be in such form prescribed by the Central Government. (2) The Certifying Authority to be paid by such fee not exceeding Rs. 25,000 prescribed by the Central Government.

13. **Section 40A** deals with the **Duties of a subscriber of a digital signature certificate** which says that in respect of digital signature certificate, duties to be prescribed to the subscriber to perform.

14. **Section 43A** deals with **Compensation for failure to protect data** which says that where any company (body corporate) dealing with any personal information prescribed by the Central Government owns by company controls is negligently maintaining security procedure to protect the information causes wrongful gain or loss to any person, then that body corporate shall be liable to pay the compensation to the affected person.

15. **Section 46** deals with the **Power to adjudicate**. (1) Whether any person has committed a breach of any of the provision of this act, then he will pay the penalty or compensation, and the Central Government appoint to any officer, not below the rank of a Director of GoI[2] or an equivalent office of a State Government to be an adjudicating officer in such manner prescribed by the Central Government. (3) Not any person will be appointed as an adjudicating officer unless he has some experience in the IT field and judicial, prescribed by the Central Government.

16. **Section 57** deals with **Appeal to Cyber Appellate Tribunal** which says that any aggrieved person order made by an adjudicating officer under this act may appeal to CAT under the jurisdiction of the matter and any appeal to the tribunal by the officer must be made with the consent of the parties. (3) Every appeal shall be filed within 40 days from the date when the order made by the officer and then according to it such fee can be prescribed.

17. **Section 58** deals with the **Procedure and power of the Appellate Tribunal**. (2) This tribunal discharge the function with the similar power conferred in a Civil Court of CPC, 1908 while having a suit in respect to other matter may be prescribed.

18. **Section 67C** deals with **Preservation and retention of information by intermediaries** which say that intermediary shall preserve such information for a specific duration in such manner and format as prescribed by the Central Government and any intermediary who intentionally violates the provision shall be punished with imprisonment extending up to 3 years and liable to a fine as well.

19. **Section 69** deals with **Power to issue directions monitoring or decryption of any information through any computer resource**. (2) The procedure of decryption when the Central Government or State Government satisfied that it is necessary to do for the country or state, then it may be carried out and direct the appropriate government to decrypt in a prescribed manner.

20. **Section 69A** deals with **Power to issue directions for blocking for public access of any information through any computer resource**. (3) Intermediary who fails to obey the direction (the Central Government or State Government satisfied that it is necessary to do for the country or state, then it may be carried out and direct the appropriate government to block the access by the public in a prescribed manner) shall be punished with imprisonment extend up to 7 years and liable to fine as well.

21. **Section 69B** deals with **Power to authorise to monitor and collect traffic information through any computer resource for cybersecurity**. (3) The procedure for collecting the traffic information carried out in a prescribed manner when the Central Government increase cybersecurity for prevention and identification of computer toxin in the country, then by the notice in the Official Gazette sanction agency of government to collect the data.

22. **Section 70** deals with **Protected system** which says that the appropriate government declare by the notification in the Official Gazette that computer resources which affect the capability of CII (Critical Information Infrastructure means any computer resource which has a devastating impact on national security, public health, safety etc.) by order in writing to be a protected system. The Central government prescribe the procedure for a protected system and if any person who access the protected system and in violation of the

provision shall be punished with imprisonment may extend up to 10 years and liable to a fine as well.

23. **Section 70A** deals with the **National nodal agency** which says the Central Government by notification elects any organisation of the government as the national nodal agency in reverence of CII protection. (3) The function and duties of the agency may be prescribed a manner.

24. **Section 70B** deals with the **Indian Computer Emergency Response Team to serve as the national agency for an incident response** which says that the Central Government by notification appoints an agency of government to be called the Indian Computer Emergency Response Team (ICERT). (2) The agency referred with the Director-General and other officers and workers, (3) the salary and allowances will also be provided to the Director-General, and (5) functions and duties of D-G in a prescribed manner.

25. **Section 79** deals with **Exemption from liability of intermediary in certain cases** which says that (2) the function of the intermediary is inadequate to provide access to a communication system with info available by third parties is temporary or so, then intermediary shall not be liable in this case. The Intermediary shall not initiate the transmission, select the receiver and modify the info in the transmission. Intermediary witnesses' due diligence when discharging his duties and observes other guidelines on his behalf will be prescribed by the Central Government.

26. **Section 84A** deals with **Modes or methods for encryption** which says that the Central government may use an electronic medium, for the promotion of e-governance and e-commerce.

1. GOVERNMENT NEW IT RULES, 2021

The Government of India through the Ministry of Electronics and Information Technology (MEITY) by practising its force under Section 87(2) of the IT Act, 2000, told the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("Intermediary Rules, 2021") on 25th February 2021. The Intermediary Rules, 2021 is a supersession of the earlier IT (Intermediaries Guidelines) Rules, 2011.

Rationale behind the Intermediate guidelines, 2021 to touch upon inter alia numerous problems together with fake news, deep fakes, online

intellectual belongings infringement, over-the-top (OTT) platform content material regulation, and so forth. Throughout the pandemic triggered lockdown, India registered a reported 60% growth in paid OTT subscribers. The blessings of OTT are several in that the audience has got admission to a much wider variety of customer-managed content which they can watch from the comfort in their houses at a much decrease fee. However, content streamed on OTT structures has been less regulated than its offline counterparts like cinema and tv.

SALIENT FEATURES OF THIS RULE

- Virtually identifies content/ facts that are offending e.g., which breaches copyright, is defamatory or obscene, copies every other etc.
- The lengthy listing of due diligence to be observed with the aid of all Intermediaries whilst discharging their obligations are notified below Rule 3 of the Intermediary Rules, 2021. If such due diligence is not determined, and generally for non-observance of Intermediary Rules, as applicable, safe harbour provisions under section 79, IT Act shall no longer be to be had.
- All Intermediaries are required to employ Grievance Officers to address complaints made via users. The names and call information of such complaint officials have to be prominently displayed on the website or mobiles of such intermediary. Proceedings ought to be reported within 24 hours and resolved within 15 days by the Grievance Officers.
- Creation of a content rating system, similar to that imposed upon conventional media our bodies such as U (universal), U/A 7+, A (adult) and so on. The content will be classified in keeping with the context, subject, target audience etc. They will also display content descriptors obviously for users to see earlier than getting access to the content material. They are additionally expected to permit get admission to control mechanisms, consisting of parental locks, for content for the ones over 13 years and installed place a reliable age mechanism law.
- The Rules introduce a three-tier grievance redressal mechanism for the regulation of online content.
- Level-I: Self-regulation by the publishers means the publisher employs a grievance officer to decides the grievance within 15 days.

- Level-II: Self-regulatory Body which means it may have one or more bodies of publishers, such shall be head by the retired judge of SC, a HC and not more than 6 members. This will address the grievances when level-1 has not been resolved within 15 days.
- Level-III: Oversight mechanism which means MIB[3] create oversight mechanisms which shall issue a charter for self-regulating bodies including Codes of Practices and for hearing the grievances it shall establish the Inter-Department Committee.

1. SUPREME COURT AND THE IT ACT

Since the introduction of the IT Act in 2000, it has proved to be an extremely debatable piece of law. In its all these unusual years of operation, the Act has controlled to attract significant complaint from the legal community and most of the people. It's imagined to include a whole spectrum of flaws, shortcomings and pitfalls starting from being inefficient in tackling cybercrimes to setting unfair curbs on the civil liberties of residents.

The IT Rules, 2021 are allegedly made under section 87(1) of the IT Act, more specifically section 87(2)(z) & (zg) which respectively allow guidelines to be framed on: – "the method and safeguards for blocking for access by the general public under section 69A(2)" and "guidelines to be discovered by using the intermediaries under section 79(2)". Therefore, section 87(2)(zg) isn't always applicable to virtual information media as they may be now not intermediaries either as per the Act or as according to the IT Rules, 2021. Rules sourced to section 87(2)(z), certainly, cannot travel beyond section 69A, which is constrained to 'intermediaries' or 'agency of the authorities' and that too on grounds regarding security pursuits of the state.

In the case of ***Shreya Singhal v. Union of India,***[4] Section 66A of the IT Act is hit down in its entirety being violative of Article 19(1)(a)[5] of the Indian Constitution and not saved under Article 19(2)[6] of the Indian Constitution. Section 69A of IT Act and IT (Procedure & Safeguards for Blocking for Access of Information by Public) Rules 2009 are constitutionally valid. The IT Rules, 2021 bring back a few factors of phase 66-A and pass far beyond it, by the manner of prescription, to be administered, adjudicated upon and supervised through the government. They not only surpass the IT Act, but also contravene the very best SC's ruling in this case, and consequently will now not be saved through any trendy rule-making power under section

87(1) that is restrained to sporting out the provisions of the IT Act. Numerous laws have been historically challenged and held to be unconstitutional by using the courts in India for being outrightly vague and loosely drafted making room for numerous interpretations in this landmark judgment case.

1. CONCLUSION

The digital India programme has now turn out to be a movement that's empowering commonplace Indians with the strength of technology. The big unfold of mobile telephones, the internet and so on has also enabled many social media structures to amplify their footprints in India. The creation of the policies has ensured that there is comity in content being streamed across all platforms and that the primary criticism redressal mechanism is dealt with by way of the writer or an enterprise association or institution of publishers. those regulations and the efforts with the aid of the Indian authorities are worthy and make sure that technological improvements cross hand in hand with felony tendencies thereby growing a level playing field for all carrier companies and also protecting citizens of the country.