International Journal of Enhanced Research in Educational Development (IJERED)
ISSN: 2320-8708, Vol. 11 Issue 4, July-August, 2023, Impact Factor: 7.326

Sentencing Policy with Special Reference to Information technology Act, 2000

Dr. Renu Saini

Assistant Professor Khalsa College of Law, ASR

ABSTRACT

The internet is one of the influential creations that offer people; endless knowledge, entertainment, communication and platform to have closer ties. Due to anonymous nature of Internet, it is possible to engage into a variety of criminal activities with impunity. People with intelligence, have been grossly misusing this aspect of internet to perpetuate criminal activities in cyberspace. The technology boom and easy internet access across the country even in rural and henceforth ignored area; cybercrime has become a phenomenon. Cybercrime is an unlawful act, wherein the computer is either a tool or a target or both. These are new class of crimes, rapidly increasing due to extensive use of internet and information technology enabled services. The increase rate of technology in computers has led to the enactment of Information Technology Act, 2000. Due to the increase in the digital technology various offences has also increased. Since new-new technology come every day, the offences has also increased therefore the ITA, 2000 need to be amended in order to include those offences which are now not included in the Act.There is grave underreporting of cybercrimes in the nation. Cyber Crime is committed every now and then, but is hardly reported. The cases of cybercrime that reaches to the Court of Law are therefore very few. There are practical difficulties in collecting, storing Digital Evidence. Sentencing is one of the difficult tasks that a judge may be facing as he has to consider number of factors while pronouncing it such as determining which actions or omissions are permissible, who is to be punished with what kind of punishment or to what extent punishment is required, role of offender in commission ofan offence, severity of an offence, availability of evidences, injury caused to the victim and many more.

Keywords*:* Sentencing, Information Technology, Cyber Crime, Cyber Offences, Digital India Act

INTRODUCTION

In a world which today notices an alarming increase in crime rates, the need to regulate the domain of criminal justice system in every country is the need of the hour. Crime and punishment have today formed a very crucial and delicate aspect of the society; it can no longer be guided by customs and precedents. A fixed regime needs to be brought into force and the subjective element needs to be reduced as much as possible. However a fact that cannot be ignored that no fixed penalties can be induced over the accused because of it being too harsh and too ignorant on the rights of the accused. The accused has the right to avail certain basic human rights which the fixed penalty regime violates. Also, giving discretion to the judges on deciding penalties will also result in violation of fundamental rights.[1]With the advancement of technology, wide range of criminal activities is being carried on but none had greater likely impact or influence than the internet and its related technology enabled services.

The internet is one of the influential creations that offer people; endless knowledge, entertainment, communication and platform to have closer ties. Due to anonymous nature of Internet, it is possible to engage into a variety of criminal activities with impunity. People with intelligence, have been grossly misusing this aspect of internet to perpetuate criminal activities in cyberspace. The technology boom and easy internet access across the country even in rural and henceforth ignored area; cybercrime has become a phenomenon. Cybercrime is an unlawful act, wherein the computer is either a tool or a target or both. These are new class of crimes, rapidly increasing due to extensive use of internet and information technology enabled services. These include hacking, phishing, credit card frauds, cyber terrorism, publishing or transmitting obscene material or material containing sexual explicit act, cyber stalking and so on. To regulate such activities that violate the rights of an Internet user, the Government of India has enacted Information Technology Act, 2000. The act provides for various forms of offences along with their punishments.

[1]Tanisha Prashant, Sentencing Policy in India, retrieved from https://blog.ipleaders.in/criminal-justice-sentencing-policy-india/, visited on August 12, 2023 at 4:48 p.m.

INFORMATION TECHNOLOGY ACT, 2000

In 1996, the United Nations Commission on International Trade Law (UNCITRAL) adopted the model law on electronic commerce to bring uniformity in the law in different countries. The model was promulgated to assist countries in the framing of legislation which would enable and facilitate electronic commerce and electronic government. Further, the General Assembly of the United Nations recommended that all countries must consider this model law before making changes to their own laws. This model law –

1. establishes rules and norms that validate and recognize contracts formed through electronic means,
2. Set rules for forming contracts and governing electronic contract performance,
3. Define the characteristics of valid electronic writing and of an original document,
4. Provides for the acceptability of electronic signatures for legal and commercial purposes, and
5. Support the admission of computer evidence in courts and arbitration proceedings.

India became the 12th country to enable cyber law after it passed the Information Technology Act, 2000. While the first draft was created by the Ministry of Commerce, Government of India as the E Commerce Act, 1998, it was redrafted as the 'Information Technology Bill, 1999, and passed in May 2000.[2]The IT Bill, 1999 has been based on the UNCITRAL Model law on e-commerce and incorporated various important features of the Model Law within it. The purpose of the bill was to provide the necessary legal and business infrastructure required for enabling e- commerce in India. The bill was tabled in parliament in December, 1999. It received the President's assent on June 9, 2000 and was implemented on October 17, 2000. The Act was amended by the Information Technology (Amendment) Act, 2008 which brought in a number of important amendments, which came into effect on October 27, 2009

Objectives Of The Act

1.To provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referredto as "electronic commerce", which involve the use of alternatives to paper-based methods of communication and storage of information;
2. To facilitate electronic filing of documents with the Government agencies,
3. To amend the Indian Penal Code, 1860, the Indian Evidence Act, 1872, the Banker's Book Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected there with or incidental thereto.[3]

Cybercrimes

There is no universally accepted definition of cybercrimes. It is not officially defined in the Information Technology Act, 2000 or in any other Legislation. A report by McConnell International (2000), a global technology policy and management consulting firm, defines cybercrimes as "harmful acts committed from or against a computer or network."[4] Computer crime can involve activities that are traditional in nature, such as theft, fraud, forgery and mischief, all of which are generally subject everywhere to criminal sanctions.[5]

Dr. Debarati Halder and Dr. K. Jaishankar defines Cybercrimes as, "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modem telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS).[6]

It refers to all the activities done with criminal intent in cyberspace or using the medium of Internet. These could be either the criminal activities in the conventional sense or activities, newly evolved with the growth of the new medium. Any activity, which basically offends human sensibilities, can be included in the ambit of cybercrimes.[7] These crimes are usually committed by a broad range of persons. It may be individual, groups or state viz., students, amateur computer programmer, persons having vested interests, business rivals, terrorists and members of organized crime group.

[2]Cyber Laws, "Information Technology Act, 2000" retrieved from https://www.toppr.com/guides/business-laws-cs/cyber-laws/information-technology-act-2000/visited on Sep. 6, 2021 at 10: 00 p.m.
[3]Information Technology Act, 2000 (21 of 2000).
[4]Amita Verma, "Cyber Crimes in India", Central Law Publications, Allahabad, 2012, p.66.
[5]"United Nation Manual on the prevention and control of computer- related crime", United Nations, New York, 1994, p.4.
[6]Rashmi Saroha, "Profiling a Cyber Criminal" retrieved from https://www.ripublication.com/irph/ijict_spl/ijictv-4n3spl_06.pdf, visited on Sept.15,2021 at 7:35 p.m.
[7]Pavan Duggal, "Cyber Law 3.0", Universal Law Publishing Co. Pvt. Ltd., New Delhi, India, 2014, p.168.

CLASSIFICATION OF CYBERCRIMES

Cybercrimes can be basically divided into four major categories-
1. Cybercrimes against persons;
2. Cybercrimes against property;
3. Cybercrimes against government; and
4. Cybercrimes against society.

I. Cybercrimes against persons
Cybercrimes committed against persons include various crimes like, publishing or transmitting obscene material, material containing sexually explicit act, child pornography, cyber stalking, cyber defamation, e-mail spamming, e-mail bombing, and many more.

The publication, transmission of obscene material including pornography, indecent exposure and child pornography constitutes one of the most important cybercrimes known today. The potential harm of such a crime to humanity can hardly be overemphasized. Cyber harassment is a distinct cybercrime which can be sexual, racial, religious or of any other nature. It brings to other related areas of violation of privacy of netizens. Violation of privacy of online citizens is a cybercrime of grave nature.

II. Cybercrimes against property
The second category of cybercrimes is cybercrime against all form of property which include unauthorized computer trespassing through cyberspace, transmission of harmful programs, hacking, computer vandalism, copyright infringement, unauthorized access to computerized information, destroys, delete or alters any information residing in a computer resource or diminishing its value or utility or affects it injuriously, and many more. Hacking and Cracking are amongst the gravest cybercrimes known till date. It is a dreadful feeling to know that someone has broken into your computer systems without your knowledge and consent and has tampered with precious confidential · data and information.[8]

III. Cybercrimes against government
The third category of cybercrime is cybercrime against the government. This category of cybercrime is the most serious offence and is also known as Cyber Terrorism. It includes hacking government official websites, military websites. Cyber warfare, distribution of pirated software, access of unauthorized information also covered under this category of cybercrime.

IV. Cybercrimes against society
The fourth category of cybercrime is cybercrime against society. These crimes not only affect the individual or government or any organization but the society at large. They include pornography (especially child pornography), polluting the youth through indecent exposure and trafficking etc, apart from pornography, finance related crimes, forgery, trafficking, sale of illegal articles are also covered under this category of cybercrime.

SENTENCING AND PUNISHMENT

The concept of punishment is the by-product of Social Contract Theory. The concept of social contract theory was evolved which urged the members of the society to surrender all their rights and liberties in the sovereign for the preservation of peace, life and prosperity of the subjects. The sovereign was the lawful administrator who would render protection to the individual. Through social contract a new form of social organization the state was formed to assure guarantee rights, liberties, freedom and equality.[9] It is the duty of the state to make laws regarding the protection of the rights, liberties of the people and whosoever disobey the laws will be liable to be punished Punishments are imposed with an object to prevent the crime and to protect the society.

Sentences are the statements in judgments which lay out what the punishment for a particular offence will be according to the law. When the same is put in action, is operationalized, it would be called as punishment. Thus, it can be said that sentence is the predecessor to the actual inflicting of punishments.[10]

Sentencing is that phase of criminal justice system where the real punishment is announced after the stage of conviction to the convicted person by the judge. Sentencing is one of the difficult tasks that a judge may be facing as he has to consider number of factors while pronouncing it such as determining which actions or omissions are permissible, who

[8] *Id*. at p.169.
[9] S.R. Myneni, "Jurisprudence (Legal Theory)", Asia Law House, Hyderabad, 3rd ed., 2020, p. 425.
[10] Aastha Sahay, "Sentencing and punishment policy in India" retrieved from https://www.probono-india.in/blog-detail.php?id=152 visited on August18,2021 at 3:20 p.m.

is to be punished with what kind of punishment or to what extent punishment is required, role of offender in commission ofan offence, severity of an offence, availability of evidences, injury caused to the victim and many more. In ***Paras Ram and Others vs. State of Punjab***[11], the Supreme Court observed:

"A proper sentence is the amalgam of many factors such as the nature of the offence, the circumstances- extenuating or aggravating of the offence, the prior criminal record, if any, of the offender, the age of the offender, the record of the offenders to employment, the background of the offender with reference to education, home life sobriety and social adjustment, the emotional and mental conditions of the offender, the prospects for the rehabilitation of the offender, the possibility of return of the offender to normal life in the community, the possibility of the treatment or training of the offender, the possibility that the sentence may serve as a deterrent to crime by the offender or by others and the current community need, any, for such a deterrent in respect to the particular type of offence. These factors have to be taken into account by the court in deciding upon the appropriate sentence."

CYBER OFFENCES AND PUNISHMENT UNDER THE IT ACT, 2000

Chapter IX of the act deals with the penalties, compensation and adjudication. The list of offencescommitted by person is covered under Section 43 of the act. The section states that if any person without permission of the owner or any other person who is in charge of a computer, computer system or computer network-

(a) Access or secures access to such computer, computer system or computer network or computer resource;
(b) 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;
(c) Introduces or causes to be introduced any computer contaminant or virus into any computer system or computer network;
(d) Damages or causes to be damaged any 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;
(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 there under;
(h) Charges the services availed of by a person to the account of another person 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;
(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.[12]

Section 43A of the act has been inserted by IT (Amendment) Act, 2008 which states that a body corporate shall be liable to pay damages by way of compensation to the person so affected due to their negligence in implementing and maintaining reasonable security practices and procedures to protect the data.

Sub-section (a) of section 44 of the act prescribes penalty not exceeding one lakh and fifty thousand rupees to any person for the failure to furnish any document, return or report to controller or the Certifying Authority. Sub-section (b) of section 44 of the act prescribes penalty not exceeding five thousand rupees to any person for every day during which the failure continues to file any return or furnish any information, books or other documents within the time specified in the regulation. Sub-section (c) of section 44 of the act prescribes penalty not exceeding ten thousand rupees for every day during which the failure continues to maintain books of account or records.

Section 45 provides residuary penalty which states that 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.

The following table shows the offences and punishment under chapter XI against all the mentioned sections of the ITA, 2000 with amendments as per IT Amendment Act, 2008.

[11]Paras Ram and Others vs. State of Punjab (1981) 2 SCC 508 (India).
[12]Information Technology Act, 2000 (21 of 2000).

SECTIONS	**OFFENCE**	PUNISHMENT
65	Tampering with computer source documents.	Imprisonment up to three years or fine which may extend up to two lakh rupees or with both.
66	Computer related offences mentioned under section 43.	Imprisonment for a term which may extend to three years or with fine which may extend to five lakh rupees or with both.
66B	Dishonestly receiving stolen computer resources or communication device.	Imprisonment of either description for a term which may extend to three years or with a fine which may extend to rupees one lakh or with both.
66C	Identity theft.	Imprisonment of either description for a term which may extend to three years or with a fine which may extend to rupees one lakh or with both.
66D	Cheating by personation by using computer resource.	Imprisonment of either description for a term which may extend to three years or with a fine which may extend to rupees one lakh or with both.
66E	Violation of privacy.	Imprisonment which may extend to three years or with fine not exceeding two lakh rupees or with both.
66F	Cyber terrorism.	Imprisonment which may extend to imprisonment for life.
67	Publishing or transmitting obscene material in electronic form.	Imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees on first conviction 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.
67A	Publishing or transmitting of material containing sexually explicit act, etc. in electronic form.	Imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees on first conviction 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.

67B	Publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form.	Imprisonment of either description for a term which may extend to three years and with fine which may extend to five lakh rupees on first conviction 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.
68	Noncompliance of order of controller by Certifying Authority or any employee of such authority.	Imprisonment not exceeding two years or a fine not exceeding one lakh rupees or both.
69	Failure to assist the agency referred to in sub-section (3) in regard to interception, monitoring or decryption of any information in any computer resource	Imprisonment for term which may extend to seven years and shall be liable to pay fine.
69A	Non-compliance of the intermediary with the direction issued for blocking for public access of any information through any computer resource.	Imprisonment for term which may extend to seven years and shall be liable to pay fine.
69B	Contravention of the provisions of sub-section (2) by intermediary in regard to monitoring and collect traffic data or information through any computer resource for cyber security.	Imprisonment for term which may extend to three years and shall also be liable to pay fine.
70	Illegal access or attempts to secure access to a protected system.	Imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.
70B	Failure to provide the information by any service provider, intermediaries, data centres, body corporate or person to Indian Computer Emergency response team.	Imprisonment of either description for a term which may extend to one year or with a fine which may extend to rupees one lakh or with both.
71	Misrepresentation	Imprisonment of either description for a term which may extend to two years or with a fine which may extend to five lakh rupees, or both.
72	Breach of confidentiality and privacy.	Imprisonment of either description for a term which may extend to two years or with a fine which may extend to one lakh rupees, or both.
72A	Disclosure of information in breach of lawful contract.	Imprisonment of either description for a term which may extend to three years or with a fine which may extend to five lakh rupees, or both.
73	False publishing of electronic signature certificate on certain particulars.	Imprisonment of either description for a term which may extend to two years or with a fine which may extend to one lakh rupees, or with both.

74	Publication of electronic signature certificate for any fraudulent or unlawful purpose.	Imprisonment for a term which may extend to two years or with a fine which may extend to one lakh rupees, or with both.

The Hicklin Test was laid down by the Queen's Bench in ***Regina vs. Hicklin***.[13] The test of obscenity is whether the tendency of the matter charged as obscenity is to deprave and corrupt those whose minds are open to such immoral influences and into whose hands a publication of this sort may fall. On application of the Hicklin test, a publication can be judged for obscenity based on isolated passages of a work considered out of context. Works can be judged by their apparent influence on most susceptible readers, such BS children or weak-minded adults.

One of the most celebrated cases under section 67 of the IT Act,2000 has been that of ***Avinash Bajaj Vs. State (NCT) of Delhi***[14]. Avinash Bajaj, the CEO of Bazee.com was arrested under Section 67 of the IT Act for an advertisement by a user to sell the DPS MMS sex scandal video through the Bazee.com website. He applied for bail. The court noted that Mr Bajaj was nowhere involved in broadcasting of pornographic material could not be Viewed on the Bazee.com website. But Bazee.com receives a commission from the sales and earns revenue for advertisements carried on via its web pages. The Court further observed that the evidence collected indicates that the offence of cyber pornography cannot be attributed Bazee.com but to some other person. The court granted bail to Mr Bajaj subject to the furnishing of two sureties' one lakh rupees each to the satisfaction of the concerned Court or Metropolitan Magistrate or Duty Magistrate. However, the burden lies on the accused that he was merely the service provider and does not provide content; this case was a classic illustration of the online intermediary liability dilemma. The content under question was exactly the kind of material that ought to be removed from the web immediately.

In ***Aveek Sarkar & Anr. Vs. State of West Bengal and Anr***,[15] Justices K.S. Radhakrishnan and AK. Sikri upheld and ruled that if any picture or article contains lascivious material which appeals to prurient interests and tends to deprave and corrupt those likely to read, see or hear it would be deemed to obscene. The court additionally said that "A photo of a bare or semi-naked lady can't in essence be called revolting. Just those sex related materials which have a propensity of energizing indecent considerations' can be held to be revolting, yet the profanity must bemade a decision from the perspective of a normal individual, by applying contemporary network standard".

INFORMATION TECHNOLOGY (AMENDMENT) ACT, 2008

The IT Act, 2000 was amended by the Information Technology amendment Act, 2008, which bought in a number of important amendments which came into effect on October27, 2009. The punishment to pay damages by way of compensation to the person so affected under Section 43 has been substituted for he shall be liable to pay damages by way of compensation not exceeding one crore rupees to the person so affected. A new Section 43A has been inserted to protect sensitive personal data or information possessed, dealt or handled by a body corporate in a computer resource which such body corporate owns, controls or operates. If such body corporate is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, it shall be liable to pay damages by way of compensation to the person so affected. It introduced Section 66A which penalised sending "offensive messages" through communication service, etc. In view of the increasing threat of terrorism in the country, the new amendments include an amended section 69 giving authorities the power of "interception or monitoring or decryption of any information through any computer resource".

INFORMATION TECHNOLOGY (INTERMEDIARIES GUIDELINES AND DIGITAL MEDIAETHICS CODE) RULES, 2021

The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules of 2021 (hereinafter referred to as 'the Rules') has been enacted by the Central Government under the powers conferred to it by Section 69A(2), 79(2)(c) and 87 of the Information Technology Act, with thorough coordination with the Ministry of Electronics and Information Technology and the Ministry of Information and Broadcasting. The formulation of these Rules is in response to the growing criticism against the government, while it recognizes the right to criticize and disagree as an essential element of democracy. It aims to provide a robust complaint mechanism for social media and OTT platform users to address their grievances, a mechanism earlier inexistent.

The proposed framework has been quoted to be progressive, liberal and contemporaneous, as it lays a special emphasis on the protection of women against the progression of sexual offences on social media. It emphasizes on the need of social media intermediaries and online content providers, whether for entertainment or informative purposes, to strictly

[13]Regina vs. Hicklin (1868) 3 QB 360.
[14]Avnish Bajaj v. State (NCT) of Delhi 2008 **105 DRJ 721** (India).
[15]Aveek Sarkar &Anr. vs State of West Bengal and Anr. (2014) 4 SSC 257 (India).

comply with the Constitution and domestic laws of India. It extends its approach to instill a sense of accountability against misuse and abuse by social media users and is the first of its kind to bring social media use under the regulatory framework of the Information Technology Act.

These rules have been in light of the recent run-down on the OTT platforms by the government, which have been actively, rather vehemently, lobbying for stronger and more stringent regulations in place. However, contrary to such a view, as per the PIB, the Rules have been formulated keeping in mind the importance of free speech and journalistic and creative freedoms. Regardless of the political connotations, the enactment of these Rules puts India at par with international regimes on digital media regulation, providing a more comprehensive and holistic protection to its users.[16]

INFORMATION TECHNOLOGY (AMENDMENT) BILL, 2022

A bill amended the Information Technology Act, 2000. It was enacted by the Parliament in the seventy- third year of the Republic of India. A new Section 66G has been inserted which deals with the punishment for threatening a woman to express her opinion etc. Sub section (1) of this section states that the following acts shall be considered punishable offences, when committed against a woman, with the intention to intimidate or discredit her or force her to express a certain view, opinion or observation, or to force her to state any view, opinion or observation or to force her to refrain from expressing a certain view, opinion or observation: —

(a) threat of physical violence against a woman, her family or her property;
(b) threat of sexual assault;
(c) threat to reveal personal information including, but not limited to, her location, place of work and any other relevant detail which may be used to harm her physically or mentally;
(d) threat to spread false information about her;
(e) threat to question a person's citizenship or imputation of disloyalty to India;
(f) threat of false prosecution; and
(g) abuse based on religion, caste or sexuality.

Sub- section (2) of the Act states that the offences referred to in section 66G (1) shall be cognizable and non-bailable and shall be punishable in the following manner:—

(i) For the first offence, the person shall be punishable with a maximum punishment of three years or with a fine of up to fifty thousand rupees.
(ii) For the second offence, the person shall be punishable with a maximum punishment of seven years and with a fine of up to four lakh rupees.
(iii) For the third and subsequent offences, the person shall be punishable with a maximum punishment of ten years and with a fine of up to ten lakh rupees:

Provided that the offence under section 66G shall be compoundable at the discretion of the victim.
Sub- section (3) of the Act states that if any threat punishable under section 66G is carried out by the person making such threat or any other person incited by such person, the punishment shall be ten years imprisonment and with a fine of up to ten lakh rupees.

Sub- section (4) of the Act states that any amount imposed as fine under this section shall be paid to the victim as compensation.

Another Section 67BA has been inserted which deals with the grant of injunctions under section 66E, 66G, 67, 67A and 67B. Sub- section (1) section 67BA states thatany person who is the victim of any offence under sections 66E, 66G, 67, 67A or 67B of this Act or a police officer investigating the same, shall have the right to approach the jurisdictional Magistrate for grant of an injunction against the accused, or any other person, company, organisation or entity for deletion of the offensive text, image, audio, video or other format and for prohibition from storing, retransmitting or repeating the offensive text, image, audio, video or other format, as the case may be. Sub- section (2) states that the Magistrate shall grant the injunction without notice to the accused if he is satisfied that prima facie, a case of an offence under sections 66E, 66G, 67, 67A and 67B of this Act exists. Sub- section (3) states that the order of the Magistrate under sub-section (2) shall also be served upon any person, company, organisation or entity in conformity with the provisions of this Act and the rules made thereunder for compliance. Sub- section (4) states that any application under sub-section (1) shall be decided on the same day: Provided that for reasons to be recorded, the Magistrate may dispose

[16]Vijay Pal Dalmia,India: A Brief into The Information Technology (Guidelines for Intermediaries and Digital Media Ethics Code) Rules, 2021, retrieved fromhttps://www.mondaq.com/india/social-media/1266276/a-brief-into-the-information-technology-guidelines-for-intermediaries-and-digital-media-ethics-code-rules-2021, visited on August 13, 2023 at 5:35 p.m.

of the application within seven days. Sub- section (5) states that the injunction under sub-section (2) may be granted at the instance of the victim or of the investigating officer. Sub- section (6) states that any order passed under this section shall be subject to revision in accordance with section 397 of the Code of Criminal Procedure, 1973.[17]

DIGITAL INDIA ACT SET TO REPLACE INFORMATION TECHNOLOGY ACT OF 2022

The government has introduced a new act, the Digital India Act (DIA), aimed at preventing market power concentration and gatekeeping by big tech companies. The DIA will replace the Information Technology Act of 2022 and is expected to ensure choice, competition, fair market access, and ease of doing business in the digital space.Under the DIA, the government will revisit the need for safe harbour protection granted to intermediaries, which is currently under the Information Technology Act's safe harbour provision. The DIA seeks to ensure essential access to government and public utilities in digital governance.The act will regulate various aspects of the digital industry, including social media companies, e-commerce platforms, search engines, gaming, telecom providers, over-the-top (OTT) platforms, and artificial intelligence.

The DIA also includes provisions to protect minors from addictive technology, the right to be forgotten, and regulations for moderating fake news on social media platforms. The act will also define and regulate AI and wearable's, and ensure accountability and transparency of algorithms.In addition, the DIA will require amendments to the Competition Act, and an adjudicator and appellate mechanism will be established to hold big tech companies accountable for any breaches.The government's move to regulate the digital industry comes amid concerns over big tech companies' dominance and their alleged manipulation of the system. The DIA is expected to level the playing field and provide a fair environment for all players in the digital space.[18]

OBJECTIVES OF GLOBAL STANDARD CYBER LAWS

1. Ensure Indian Internet is Open, Safe & Trusted and Accountable
2. Accelerate the growth of innovation and technology ecosystem
3. Manage the complexities of internet and rapid expansion of the types of intermediaries
4. Create a framework for accelerating digitalization of Government and to strengthen democracy and governance (G2C)
5. Protect citizens' rights
6. Address emerging technologies and risks
7. Being Future-proof and Future-ready[19]

GOALS OF DIA

The new law should evolve through rules that can be updated, and address the tenets of Digital India

- Open Internet o Online Safety and Trust
- Accountability and Quality of Service
- Adjudicatory mechanism
- New Technologies[20]

LIMITATIONS OF IT ACT 2000

The current IT Act has following limitations, among others:

i. Lack of comprehensive provisions on user rights, trust & safety;
ii. Limited recognition of harms and new forms of cybercrimes, without any institutional mechanism for awareness creation;
iii. Lack of distinct regulatory approaches for harmful and illegal content;
iv. Absence of adequate regulations to address the regulatory requirements of emerging technology, technology, assessments of high risk automated automated-decision decision making systems modern,digital businesses including monopolies and duopolies;
v. Lack of adequate principles for data or privacy protection;
vi. Lack of a converged, coordinated & harmonized institutional regulatory body; a dedicated & efficacious investigatory/ enforceability and a swift adjudicatory mechanism;
vii. Lack of coordinated cyber security incident response mechanism[21]

[17]Information Technology (Amendment) Bill, 2022.

[18] Ashmit Kumar,Digital India act set to replace Information Technology Act of 2022,retrieved from https://www.cnbctv18.com/technology/digital-india-act-set-to-replace-information-technology-act-of-2022-16140271.htm, visited on August 14, 2023 at 11:35 a.m.

[19] Proposed Digital India Act, 2023, Digital India Dialogues 09.03.2023 Bengaluru, Karnataka retrieved from https://www.meity.gov.in/writereaddata/files/DIA_Presentation%2009.03.2023%20Final.pdf visited on August 14, 2023 at 11:40 p.m. p.8.

[20]Id. p. 20.

[21] Id. p. 29

ACCOUNTABLE INTERNET

- Adjudicatory and Appellate Mechanisms for accountable and responsive digital operators; updated intermediary framework; Obligations on significant digital operators through classification/ mandates; Algorithmic transparency and periodic risk assessments by digital entities
- Accountability for upholding Constitutional rights of the citizens, esp. Article 14,19 & 21; Ethical use of AI based tools to protect rights or choices of users; Provision of deterrent, effective, proportionate and dissuasive penalties, etc. 23
- Whole-of-Government Response for a unified, coordinated, efficient and responsive governance architecture including an effective appropriate government structure, a dedicated inquiry agency and a specialized Dispute resolution/adjudication framework.
- Disclosure Norms for data collected by Data Intermediaries, collecting data above a certain threshold.
- Standards for ownership of anonymized personal data collected by Data Intermediaries.[22]

ADJUDICATION MECHANISM

Urgent need for a specialized and dedicated adjudicatory mechanismforonline civil and criminal offences. The adjudicatory mechanism should

- be easily accessible
- deliver timely remedies to citizens
- resolve cyber disputes
- develop a unified cyber jurisprudence
- enforce the rule of law online[23]

CONCLUSION

Even though the ITA penalised cyber-crimes with a broad brush through sections 43, 66 and 67,it was only in 2008 that the ITA was amended and provisions were made for specific cyber-crimes such as sending offensive messages through communication servers, dishonestly receiving a stolen computer resource or communication device, identity theft, violation ofprivacy, cyber terrorism etc. through sections 66A to 66F and sections 67 A to 67C. Theseamendments stick out like an unwieldy appendage.Due to the increase in the digital technology various offences has also increased. Since new-newtechnology come every day, the offences has also increased therefore the ITA, 2000 need to beamended in order to include those offences which are now not included in the Act.There is grave underreporting of cybercrimes in the nation. Cyber Crime is committed everynow and then, but is hardly reported. The cases of cybercrime that reaches to the Court of Laware therefore very few. There are practical difficulties in collecting, storing and appreciatingDigital Evidence. Thus the Act has miles to go and promises to keep of the victim of cybercrimes.In 2021, India recorded 50,035 cases of cybercrime in 2020, with 11.8% surge in suchoffences over the previous year. The rate of cybercrime (incidents per lakh population) alsoincreased from 3.3% in 2019 to 3.7% in 2020 in the country, according to the National CrimeRecords Bureau (NCRB) data.Indian Judiciary has come of age and deserves appropriate sentencing policy. Individualization, non- uniform or random sentencing status in India needs to give way for certainty and logicality in the award of sentence. Having sentencing guidelines in place will enable the courts respond to the daily cry for justice and the yearnings of the community. The judges should be able to award appropriate punishment proportionate to crime committed.

[22]Id. p.23
[23]Id. p.12