Comparison between Information Technology Act, 2000 & 2008

[1] Kaushalsinh Vala, [2] Chandresh Parekh, [3] Ashish Jha
[1]Post Graduate Student, [2]Assistant Professor, [3]Advocate & Legal Advisor
[1]MTech Cyber Security,
[1]Raksha Shakti University, Ahmedabad, Gujarat, India

Abstract:
The Act to give legitimate acknowledgment to exchanges completed by methods for electronic information trade and different methods for electronic correspondence, generally alluded to as "electronic business", which include the utilization of contrasting options to paper-based techniques for correspondence and capacity of data, to nusta altering electronic recording of archives with the Government organizations and further to revise the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for issues associated therewith or coincidental thereto. Changes in the Amendment include: rethinking terms, for example, "specialized gadget" to reflect current utilize; approving electronic marks and contracts; influencing the proprietor of an offered IP to address in charge of substance got to or appropriated through it; and making enterprises in charge of executing successful information security rehearses and obligated for breaks.

Index Terms *– IT Act, Information technology act, ITAA 2008, amendments, cyberlaw, cyber security, CERT.*

I. INTRODUCTION

The Information Technology Act, 2000, an Act to give legitimate acknowledgment to exchanges did by methods for electronic information trade and different methods for electronic correspondence, generally alluded to as "web based business", which include the utilization of options in contrast to previous paper-based techniques for correspondence and capacity of data, to encourage electronic recording of archives with the Government organizations and further to change the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for issues associated therewith or coincidental thereto, was ordered in the year 2000,With the progression of time, as innovation grew, further and new strategies for perpetrating digital wrongdoing surfaced, and there was a need to correct the IT Act, 2000. With the goal that it can embed new sorts of digital offenses and fitting in different escape clauses that presented obstacles in the powerful requirement of the IT Act, 2000

This contemplated the rising of Information Technology (Amendment) Act, 2008 which was made compelling from 27 October 2009. The IT (Amendment) Act, 2008 has acquired striking changes the IT Act, 2000 from multiple points of view.

The Information Technology Amendment Act, 2008 (IT Act 2008) is a considerable expansion to India's Information Technology Act (ITA-2000). The IT Amendment Act was passed by the Indian Parliament in October 2008 and came enthusiastically a year later. It is regulated by the Indian Computer Emergency Response Team (CERT-In). This Amendment was made to address issues that the first bill neglected to cover and for its further improvement and related security.

There are also challenges posed by this amended Act that can be predicted and our country needs to be well equipped to overcome these challenges.

II. IT ACT, 2000 VS IT (AMENDMENT) ACT, 2008

(1) Electronic signatures introduced-

With the entry of the IT (Amendment) Act,2008 India has turned out to be mechanically impartial because of the selection of electronic marks as a lawfully legitimate method of executing marks. This incorporates computerized marks as one of the methods of marks and is far more extensive in ambit covering biometrics and other new types of making electronic marks. This is a constructive change as India has distinctive portions individuals and all may not be innovatively proficient to comprehend and utilize the advanced marks. It is a moving errand for the Central government to endorse conditions for considering the unwavering quality of electronic marks or electronic confirmation strategies under Section 3A (2), the technique for learning electronic mark or verification under Section 3A(3), the way in which data might be validated by electronic marks in Section 5 and the revised Act in Section 84A has enabled the Central Government to recommend modes or techniques for encryption. These parameters ought to be

set down in interview with associations, for example, NASSCOM and additionally administrative organizations that can aid the detailing of essential measures and related principles.

(2) Corporate responsibility introduced in S. 43A

The corporate responsibility for data protection is incorporated in S 43A in the amended IT Act, 2000 whereby corporate bodies handling sensitive personal information or data in a computer resource are under an obligation to ensure adoption of 'reasonable security practices' to maintain its secrecy, failing which they may be liable to pay damages. Also, there is no limit to the amount of compensation that may be awarded by virtue of this section. This section must be read with Section 85 of the IT Act,2000 whereby all persons responsible to the company for the conduct of its business shall be held guilty in case offense was committed by a company unless no knowledge or due diligence to prevent the contravention is proved.

Inclusion of this arrangement is a specific essentialness to BPO organizations that handle such touchy data in the normal course of their business. This arrangement is imperative to verify touchy information and is consequently a positive development. In any case, the test is to first, illustrate what we qualify as "sensible security rehearses". The Act in clarification to Section 43A shows these systems intended to shield such data from 'unapproved get to, harm, use, adjustment, divulgence, or disability, as might be determined in an understanding between gatherings' or as might be indicated by any law for the present in power and without both, as might be endorsed by Central Government in discussion with expert bodies/affiliations. The law clarifying the meaning of 'sensible security practices' is yet to be set down or potentially Central government is yet to outline its principles thereon.

(3) Critique on amended section 43 of IT Act

The revised Act gives the qualification among 'negation' and 'offense' by the presentation of the component of men's rea for an offense (s 43 for contradictions and s 66 of the Act for offenses). It is relevant to take note of that no roof limit for pay is endorsed under s 43 of the Amendment Act, 2008 which was one crore rupees in the IT Act. The evacuation of as far as possible can be abused or mishandled especially found in occurrences where the organization records negligible cases against its ex-representative who may have joined a contender firm without breaking its work contract.

The intention of the amended Act is to introduce the element of intention in this clause of the Section and this means rea element also finds its roots in Section 66 where a person will be sentenced if he does the same act 'dishonesty' or 'fraudulently' within the meaning of IPC i.e. with intention to defraud or cause wrongful loss. 'Intention to cause damage' in S.43(j) can be said to also include an intention to cause wrongful loss. Per se 'stealing' cannot be done without the men's rea in place and therefore this act should fall under s.66 and not 43 in case S.43 is to cover only acts done inadvertently or by negligence. This certainly cannot be the intention /objective of the amendment. Hence, a clarification on this point is necessary.

(4) Important definitions added

Two very important definitions are added to the IT Act through IT Amendment Act,2008- Section 2(a)- "Communication device and Section 2 (w) –intermediary". Although cell phones and other devices used to communicate would fall under the definition of computer in the IT Act. This amendment removes any ambiguity and brings within the ambit of the Act all communication devices, cell phones, iPods or other devices used to communicate, send or transmit any text, video, audio or image. The insertion of definition of 'intermediary' similarly clarifies the categories of service providers that come within its definition that includes telecom service providers, network service providers, internet service provider, web hosting service providers, search engines, online payment sites, online auction sites, online market places, and cyber cafes.

(5) Legal validity of electronic documents re-emphasized

Two new segments Section 7A and 10A in the corrected Act fortify the identicalness of paper-based reports to electronic archives. Area 7A in the revised Act makes the review of electronic archives additionally important wherever paper-based reports are required to be evaluated by law. Segment 10A presents lawful legitimacy and enforceability on contracts shaped through electronic methods. These arrangements are embedded to elucidate and fortify the lawful guideline in Section 4 of the IT Act,2000 that electronic archives are standard with electronic records and e-contracts are legitimately perceived and satisfactory in law. This will encourage the development of web-based business action on the web and construct netizen's certainty.

(6) Critique on Power of Controller under the amended Act

Section 28 of the Act provides that the Controller or any authorized officer shall investigate 'any contravention of the provisions of this Act, rules or regulations made thereunder'

These words ought to be supplanted with words 'any negation of the arrangements of this Chapter' in light of the way that the alteration in Section 29 for Controllers capacity to get to PCs and information has been abridged by evacuation of words " any repudiation of the arrangements of this Act, guidelines or guidelines made thereunder" for addition of words " any contradiction of the arrangements of this Chapter" . Additionally, the Controller's capacity can't intend to cover with Adjudicating officers who are approved to arbitrate on instances of negation that fall under Section 43 or the topic locale of CAT or the Police. In this manner, the intensity of Controller must be deciphered keeping in view the expectation and targets of the Act which can be elucidated.
The job of the Controller to go about as an archive of computerized marks has been revoked by the IT Amendment Act, 2008. This job has now been doled out to the Certifying Authority in Section 30 of the IT Act. This change represents a noteworthy test to guaranteeing the mystery and protection of electronic marks is kept up. The Certifying specialists will bear a more noteworthy obligation and need to fortify their security framework to guarantee its job as an archive is conveyed with adequacy. It should assign more assets and labour to routinely distribute data with respect to its practices, electronic marks authentications and distribute the present status of each testament.

(7) The Role of Adjudicating officers under the amended Act

The Adjudicating officer 's power under the amended Act in Section 46 (1A) is limited to decide claims where a claim for injury or damage does not exceed 5 crores. Beyond 5 crores the jurisdiction shall now vest with the competent court. This has introduced another forum for adjudication of cyber contraventions. The words 'competent court' also needs to be clearly defined. As per Section 46(2), the quantum of compensation that may be awarded is left to the discretion of Adjudicating officers. This leaves a wide room for subjectivity and quantum should be decided as far as possible objectively keeping in view the parameters of amount of unfair advantage gained an amount of loss caused to a person (wherever quantifiable) and repetitive nature of the default. The Information Technology (qualification and experience of adjudicating officers and manner of holding inquiry) Rules,2003 lay down the scope and manner of holding inquiry including reliance on documentary and other evidence gathered in investigations. The rules also provide for compounding of contraventions and describe factors that determine the quantum of compensation or penalty.

In the IT Act,2000 the workplace of mediating officer had the forces of the common court and all procedures before it is esteemed to be legal procedures. Another change is fused in Section 46(5)© whereby the Adjudicating officers have been met with forces of execution of requests gone by it, including the request of connection and clearance of property, capture, and confinement of blamed and arrangement for the collector. This engages the workplace of the Adjudicating officer and broadens more noteworthy enforceability and viability of its requests.

And also, there are some other differences like,

(8) Composition of CAT
(9) Section 67 C to play a significant role in cybercrime prosecution
(10) Section 69- Power of the controller to intercept amended
(11) Power to block unlawful websites should be exercised with caution S.69a
(12) Section 69B added to confer Power to collect, monitor traffic data
(13) Liability of Intermediary amended

III. CONCLUSION:

The IT (Amendment) Act,2008 from a general point of view has presented momentous arrangements and revisions that will encourage the compelling authorization of cyberlaw in India. India is presently innovatively impartial with electronic marks supplanting the necessity of advanced marks. The significance of information insurance in the present data innovation age can't be undermined and it finds a spot in Section 43,43A, 66, 72 of the IT Act,2000. In this time of union, the meaning of 'specialized gadget' and 'go-between' have been appropriately embedded/returned to and legitimacy of e-contracts is strengthened by the inclusion of Section 10 A. Area 46(5)© of the IT Act is an appreciated arrangement that enables the Adjudicating officers by giving forces of execution on the workplace of Adjudicating officer at standard with a common court. The plenty of new cybercrimes has been consolidated under section XI as offenses under the revised Act to battle developing sorts of cybercrimes especially, genuine wrongdoings, for example, youngster erotic entertainment, and digital fear mongering. The Intermediaries have been set under a commitment to keep up and give access to touchy data to suitable offices to help with comprehending cybercrime cases under Section 67C, Section 69. In any case, the obligation of ISPs has been returned to and the onus will lie on the complainant to demonstrate absence of due persistence or nearness of real information by a mediator as demonstrating connivance would be troublesome. These are a portion of the difficulties that cyberlaw implementation groups will be looked with The intensity of capture attempt of traffic information and interchanges over the web should be practiced in exacting consistence of guidelines confined under separate Sections in the Act giving such powers of checking, gathering, unscrambling or interference. Power for blocking

sites ought to likewise be practiced cautiously and ought not transgress into regions that add up to outlandish oversight. A large number of the offenses added to the Act are cognizable yet bailable which improves the probability of altering of proof by cybercriminal once he is discharged on safeguard. The police must, accordingly, assume a careful job to gather and save proof in an auspicious manner. For this, the police power should be very much furnished with criminological learning and prepared in cyberlaw to adequately explore cybercrime cases. The presentation of Examiner of Electronic Evidence will likewise help in powerful investigation of computerized proof and cybercrime arraignment.

(1) educating the common man and informing them about their rights and obligations in Cyberspace. The practical reality is that most people are ignorant of the laws of the cyberspace, different kinds of cybercrimes, and forums for redressal of their grievances. There is an imperative need to impart the required legal and technical training to our law enforcement officials, including the Judiciary and the Police officials to combat the Cybercrimes and to effectively enforce cyber laws.

(2) The announcing and passageways in police office require prompt consideration. In residential region, each neighbourhood police headquarters ought to have a digital wrongdoing cell that can adequately explore cybercrime cases. Openness is one of the best hindrances in the conveyance of rapid equity.

(3) we have just a single Government perceived criminological lab in India at Hyderabad which gets ready legal reports in cybercrime cases. We need all the more such labs to effectively deal with the expanding volume of cybercrime examination cases. Prepared and well-prepared law implementation work force - at nearby, state, and worldwide dimensions can guarantee legitimate accumulation of proof, appropriate examination, participation and arraignment of digital cases.

(4) Further under Section 79 of the IT Act, 2000 no guidelines exist for ISPs to mandatorily store and preserve logs for a reasonable period to assist in tracing IP addresses in Cybercrime cases. This needs urgent attention and prompt action.

(5) The investigation of cybercrimes and prosecution of cyber criminals and the execution of court orders requires efficient international cooperation regime and procedures. Although Section 1(2) read with Section 75 of the IT Act,2000, India assumes prescriptive jurisdiction to try accused for offences committed by any person of any nationality outside India that involves a computer, computer system or network located in India, on the enforcement front, without a duly signed extradition treaty or a multilateral cooperation arrangement, trial of such offenses and conviction is a difficult proposition.

IT (Amendment) Act, 2008 is a positive development, be that as it may, there are as yet certain lacunae in the Act, (few of which were quickly called attention to in this paper) which will surface while the alterations are tried on the blacksmith's iron of time and propelling advances!

IV. REFERENCES:

[1] https://en.wikipedia.org/wiki/Information_Technology_Act,_2000.

journal of current research, ISSN-0975

[2] https://www.scribd.com/document/331319050/cyber-law

[3] https://www.meity.gov.in/writereaddata/files/it_amendment_act2008%20%281%29_0.pdf

[4] https://www.scribd.com/document/331319050/cyber-law

[5] http://www.authorstream.com/Presentation/merangamri-1577833-act/ definition added

[6] https://www.slideshare.net/akshaykhatri2010/information-technology-act-59495171

[7] https://indiankanoon.org/doc/1540152/

[8] http://cyberlaws.net/indian-cyber-law-text-2/

[9] http://www.authorstream.com/Presentation/merangamri-1577833-act/

[10] https://www.scribd.com/presentation/338889238/Unit4