INFORMATION TECHNOLOGY ACT 2000: NEED TO DETACH THE LOOPHOLES

Jagatha Sivani*

ABSTRACT

Imagine the scenario wherein the litigation, perpetrator simply escapes the liability imposed on him just by demonstrating some lacunae exist in the law and you were left with unjustness in your hands. This is an ever-heart-wrenching moment where you can do nothing just because of a few shortcomings present in the law. These lacunae have to be detached from the same to render justice to the individual. This article will have a critical analysis of the Information Technology Act of 2000 as it consists of some loopholes which may pave the way to escape the liability imposed on the perpetrator in litigation. In this article, we will analyze the privacy concerns of the individual, breach of data, jurisdictional issues of the cyber world, non-inclusion of some cyber offenses, stipulations of lesser punishments, and dearth of awareness among the people and lack of skilled personnel to deal with these offenses, in expounded version. It is the need of the hour to bring amendments to the existing law or enact a new one for effective enforcement of the same.

Keywords: Information Technology Act 2000, Loopholes, Privacy Issues, Jurisdiction, Trained Officers.

INTRODUCTION

In this aeon, technology being an exponential space has played a focal role and added a comfort factor in rank and file. From dawn to dusk, it provides a boon to our daily life pursuits like education, governance, banking, communication, sharing, and so on. It mitigates the time factor in governance wherein the traditional way the person needs to whirl around documentation and other processes. However, it is a coin with two sides. It places you in the Dutch of its dark side. Generally, rights in this virtual world are vulnerable to intrusion. This has to be regulated through effective law and order so that no one can intrude on the rights of others in the cyber world. The Indian government has enacted various technology-related legislation to resolve the violations being made in the digital space. Among them, the legislature primarily enacted the

*BA LLB, THIRD YEAR, ANDHRA UNIVERSITY.

Information Technology Act of 2000 (hereinafter referred to as IT Act 2000) to administer the application of technology in India.

INFORMATION TECHNOLOGY ACT 2000

The inception of this IT Act 2000 can be traced back to the years of 1996 when UNCITRAL (United Nations Commission on International Trade Law) made a Model law on E-commerce that accords legal recognition to E-Commerce and superintend the digital intricacies. IT Act 2000 was based on this Model Law on E-Commerce. This IT Act 2000 accords legal recognition to digital signatures and electronic records, governs E-Commerce, regulates the cyber appellate tribunals, set down the duties of the subscribers, penalizes cyber offenses, and furnishes the liabilities to the intermediaries for the breach of duty authorized to them. The Information Technology Act 2000 was condemned by many critics. It was drafted at the toddler stage of technology when there is no Artificial Intelligence, IoT, and quantum computing, and India's internet penetration stood at a very nascent stage hat is 0.5%[1]. There were no proper discussions held in the parliament while passing the bill. There is an absence of foresight in the advancement of technology and its further ramifications while drafting the IT Act 2000. This may pave the way to abscond the litigation on the nefarious offense which can be a piece of cake to the perpetrator. A better enactment is required so that it should be at par with the advent of technology and should not accord impunity to the perpetrator. Nevertheless, the IT Act 2000 was a fiasco in many aspects that can be discussed below as follows.

LACUANE IN THE IT ACT 2000

CONCERN OF PRIVACY: Dr. Pavan Duggal[2], a cyber rights activist and Supreme Court advocate said, 'albeit privacy is now a fundamental right, the IT ACT does not provide the content to regulate data protection and privacy issues'. Privacy is the most vulnerable space to get targeted in the cyber world. Lack of clarity on this privacy protection may lead to distrust of the database and some other applications used in the tech space. The Information Technology Act 2000 stipulated the provisions for the breach of privacy if it is committed by

[1]Soumik Ghosh, 'India's IT Act 2000 a toothless tiger?' (*CSO India, November 12,2019)* <*https://www.csoonline.com/article/3453078/india-s-it-act-2000-a-toothless-tiger-that-needs-immediate-amendment.html* >*accessed on 13 May 2023*

[2] Soumik Ghosh, 'India's IT Act 2000 a toothless tiger?' (*CSO India, November 12,2019)* <*https://www.csoonline.com/article/3453078/india-s-it-act-2000-a-toothless-tiger-that-needs-immediate-amendment.html* >*accessed on 13 May 2023*

any of the individuals or the intermediary and it penalizes for the same. But no provision makes the government accountable for the breach of privacy. The government justifies its action by stating that it will get access to the information only in a public emergency. But it doesn't specify the word 'public emergency'. This portrays the possibility of the government's whim. It does not stipulate any remedy to the individual for the violation of his privacy rather it provides a penalty for the same is up to five crore. This can be condemned by saying that till 2019 no penalty had exceeded 12-13 lakhs in any single case[3].

Section 69(3)[4] furnishes the mandatory decryption of information to the government by any subscriber or intermediary or any person otherwise, they shall be liable to imprisonment which is up to 7 years, and also to a fine. This provision may blatantly violate the privacy of the individual by the government. Section 43A[5] talks about sensitive personal data but it doesn't specify what is sensitive personal data and it only penalizes the corporate body while deserting the liability of government agencies. To deal with these issues we need to detach these nuances in the IT Act 2000. Indian parliament needs to look up these existing lacunae while bringing up the amendment to this legislation. It is advised to specify the worded provisions so that it can avoid ambiguity in the text and need foresight to the future advancement of technology as there is a conceivability of arbitrary violation of the privacy of an individual in the cyber world and to avoid the heinous offenses related to that.

LESSER PUNISHMENTS: Greater punishment means greater prevention of crime. If the punishment provision is less, it doesn't make an impact on the perpetrator and doesn't deter the crime. The concept of a bad man and the theory of deterrence comes into the picture to reduce the crime rate by the imposition of severe punishment and by instilling fear in the mind of the individual. This will dissuade them to commit the crime. Lesser punishment may not instill any apprehension of the punishment in the mind of the perpetrator. The IT Act 2000 imposes penalties up to 5 crores but till 2019 no penalty has been beyond the 12-13 lakhs[6] to the intermediaries, whose turnover may be up to billions per annum. As a consequence, there is a probability to misuse of this lacuna in the IT Act by the intermediaries and infringes the

[3] Soumik Ghosh, 'India's IT Act 2000 a toothless tiger?' (*CSO India, November 12,2019)* <*https://www.csoonline.com/article/3453078/india-s-it-act-2000-a-toothless-tiger-that-needs-immediate-amendment.html* >*accessed on 13 May 2023*
[4] The Information Technology Act 2000, s 69
[5] The Information Technology Act 2000, s 43A
[6] Soumik Ghosh, 'India's IT Act 2000 a toothless tiger?' (*CSO India, November 12,2019)* <*https://www.csoonline.com/article/3453078/india-s-it-act-2000-a-toothless-tiger-that-needs-immediate-amendment.html* >*accessed on 13 May 2023*

provision according to their caprices. The 2008 amendment in the IT Act 2000 reduces the quantum of punishment and is made as a bailable offense, also raising the fine which replicates a toothless tiger against the perpetrator[7]. To prevent the crime the punishment should be rigorous so that could instill fright in the mind of the individual and deter them from committing the crime.

OTHER CYBER CRIMES: The IT Act 2000 addressed only a few types of cyber offenses under Chapter 11. Other cyber offenses like phishing, spamming, fintech issues like internet banking fraud, and some offenses against women like cyberbullying are not stipulated in the Act. It doesn't furnish any provision to penalize online trademark violations (relating to domain names) which are also known as cybersquatting and doesn't resolve Intellectual property-related issues like protection of copyright and patents. It is not an exhaustive Act. It doesn't have a foresight of evolving cyber offenses. Many prominent companies like the TATA company case[8], and Yahoo.com case[9] were involved in these cybersquatting cases, but even after that, no amendment was made to resolve these in the IT Act 2000. Non-inclusion of these offenses under the IT Act may en route a way to escape liability. So it is suggested to include these cyber offenses through amendments to the IT Act 2000 otherwise it could leave the capsule of impunity to the perpetrator.

CONFLICT OF JURISDICTION: According to Section 75[10] of the Information Technology Act 2000, it provides the transnational jurisdiction of the offenses committed in cyberspace. But there is a lack of international cooperation among the various countries around the world. The absence of mutual legal assistance agreements, extradition treaties, or cooperation among the nations made the application of jurisdiction futile. The obtuse interpretation of words in Section 75[11] may leave a chance to abscond liability and make it difficult for law enforcement agencies to implement the same and it will also be difficult to prosecute the perpetrator. A humongous number of service providers are located outside the territorial boundaries of India and they don't have an obligation to comply with the IT Act 2000. This increases the chances of escaping liability for violation of the Act. So, India requires a persistent and unique law that administers the jurisdiction of cyber offenses

[7] Soumik Ghosh, 'India's IT Act 2000 a toothless tiger?' (*CSO India, November 12,2019)* <*https://www.csoonline.com/article/3453078/india-s-it-act-2000-a-toothless-tiger-that-needs-immediate-amendment.html* >*accessed on 13 May 2023*
[8] *Tata Sons Ltd. and Anr. Vs Arno Palmen and Anr.* CS(OS) No. 563/2005
[9] *Yahoo!, Inc. vs Aakash Arora & Anr.* CS No. 78/1999
[10] The Information Technology Act 2000, s 75
[11] The Information Technology Act 2000, s 75

committed within its territory and outside of its territory so that it could steer clear of uncertainty in its application and render justice to victims by not demonstrating the anomalies in the existing laws. India needs to learn from cross-border studies regarding these jurisdictional aspects in other countries so that it could implement them in our country. It may be suggested to amend the IT Act 2000 and adopt online dispute resolutions for these transnational cyber offenses which may be effective in rendering justice.

DEARTH OF AWARENESS AND TRAINED OFFICERS: Humongous number of cases were unreported due to a lack of awareness of the law and sometimes it may be a social stigma. Police and judiciary need to equip themselves with the laws relating to technology, networking, and communication technologies to crack the cases of cybercrimes and for speedy disposal of the cases. A report has shown that 450% rise in cyber offenses in the last 5 years[12]. According to the National Crime Record Bureau India reported 12317 cyber cases in 2016 and these were shot up to 44546 in 2019[13]. But Computer Emergency Response Team-In sets out different data regarding these incidents as 208456 in 2018, 394499 in 2019, 1158208 in 2020, 1402809 in 2021, and 212485 in the first two months of 2022[14]. These are the ramifications of a lack of knowledge of technology and its related laws among the people. So it is advised to conduct legal awareness among the people on these cyber offenses and about the existing laws that regulate these offenses. It may be suggested to assemble some group of police officers and get trained by IT experts and get expertise in law so that could help them to opt for speedy disposal of cases.

OTHER CONCEPTS: The IT Act 2000 doesn't comprise the legal framework for the regulation of E-Commerce. Whereas there are some guidelines to follow in regulating E-Commerce but it has no legal binding over them. Lack of consumer protection and online sale of fake products were the ramifications of this unregulated E-Commerce. Lack of infrastructure, resources, worded provisions in the law, and awareness among the people are the causes of limited enforcement of the law and providing impunity to the perpetrators.

[12] 'Cops and lawyers get training to handle cyber crimes' (Times of India, February 16, 2021) < https://timesofindia.indiatimes.com/city/jodhpur/cops-lawyers-get-training-to-handle-cybercrime-cases/articleshow/80934857.cms > accessed on 14th May, 2023

[13] Cops and lawyers get training to handle cyber crimes' (Times of India, February 16, 2021) < https://timesofindia.indiatimes.com/city/jodhpur/cops-lawyers-get-training-to-handle-cybercrime-cases/articleshow/80934857.cms > accessed on 14th May, 2023

[14] 'Two months of 2022 saw more cyber crimes than entire 2018: why e-fraud is tracking time bomb' (Cyber CERT) < https://cybercert.in/two-months-of-2022-saw-more-cyber-crimes-than-entire-2018-why-e-fraud-is-a-ticking-time-bomb/#:~:text=India%20reported%202%2C08%2C456%20incidents,first%20two%20months%20of%202022 >accessed on 14th May 2023

However, the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021 furnishes guidelines for intermediaries and digital content but this lacks in providing explicit power for the Grievance Appellate Committee for enforcing its orders. This may pose a conflict of decisions if the petitioner approaches both the courts and Grievance Appellate Committee parallelly[15]. Lack of regulation over digital content may lead to pirated versions of any copyright, or intellectual property.

CONCLUSION

Protecting and securing the data is the obligation of the state. To secure that state, i.e....., parliament to enact the law that ensures the effective enforcement of the same. If the same law has nuances or shortcomings exists then it will be an abuse of justice. Cyberspace evolving with a greater pace and is the most vulnerable to getting attacked. No doubt that this Act protects us from many computer-related offenses and provides the adjudication, adjudicating officers, controllers, and certifying authorities for the same. But even after providing the tree, the fruits need to be sweet. The enforcement should be effective in such a way by not providing impunity to the perpetrator. The Act should be amended in a way so that it could address all the offenses being done in the cyber world and provides justice for the same. These loopholes not only affect the security of India or the individuals present there but also affect the economy of the country too. These can be detached by enacting new laws or amending the existing laws. There is a need for the effective enforcement of the IT Act 2000 and there should be international cooperation through mutual legal assistant agreements, extradition treaties, and agreements among the various nation around the world to resolve cyber offenses. By filling these gaps is the only way to protect and secure the data of our country and our citizens and to regulate the offenses committed in the virtual world.

[15] 'Explained| the amendments to the IT Rules 2021' (*The Hindu, November 6,2022)* < https://www.thehindu.com/sci-tech/technology/explained-the-amendments-to-the-it-rules-2021/article66079214.ece > accessed on 14 th may 2023