ISSN NO. 2320-5407

Journal homepage: http://www.journalijar.com
Journal DOI: 10.21474/IJAR01

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH

RESEARCH ARTICLE

IN-BUILT CHALLENGES FOR INFORMATION TECHNOLOGY LAW IN INDIA

***Dr. Swapnil Sudhir Bangali[1] and Dr. Harita Swapnil Bangali[2].**

1. Faculty in Symbiosis Law School, Pune, constituent of Symbiosis International University, Pune, India.
2. Independent Practitioner and consultant and worked with Infosys as Senior Legal Attorney.

Manuscript Info

Manuscript History:

Received: 12 April 2016
Final Accepted: 19 May 2016
Published Online: June 2016

Key words:
Contraventions, Section 43, Challenges, Online Defamation, Privacy, Amendment

****Corresponding Author***

Swapnil Sudhir Bangali.

Abstract

The Information Technology Act, 2000 was a much celebrated enactment as India achieved the feet of becoming the 12th nation in the world for having exclusive enactment on Information Technology. The need was felt to enhance the remedies for the contraventions under Section 43 of The Information Technology Act, 2000 and the necessary amendment was made in 2008. Even thought the Amendment of 2008 enhanced the scope of Section 43, still there are many loopholes and gaps which need to be bridged to provide effective implementation for the victims of the contraventions. This article aims to take account of such techno-legal and procedural challenges which need to be addressed with one more amendment in The Information Technology Act, 2000.

Introduction:-

The Model Law on E-commerce was enacted by UNICITRAL in 1997. Countries around the world started the enforcement of the Model Law in their own domestic sphere. It was virtually a race of countries to become first ever country having its own Information Technology Law. India became 12th nation in the world to have enacted an exclusive legislation on Information Technology based on UNICITRAL Model Law. The Information Technology Act, 2000 was passed in India with an expectation to incorporate the provisions under UNCITRAL Model Law and the offences and contraventions, including the new technological advancement. It was expected that this law will encompass all the possible technological challenges because of the digitization and use of information communication technology in India.

Jenkins et al (1996) observed that though law cannot possibly be expected to keep pace with changes in technology, still there are few areas in the current information technology law which needs some attention. The Information Technology Act, 2000 was amended comprehensively in the year 2008. The amendment in 2008 had a major impact on the contraventions under Section 43 of The Information Technology Act, 2000. The Amendment added two sub-clauses in the form of sub-clause (i) and (j) to enhance the scope of contraventions under Section 43 and to provide more remedies for the victims of contraventions. Even the amendment was made in terms of adjudication by special court that is, Adjudicating Officer appointed under Section 46 and the jurisdiction of the Competent Court under Section 46 (1A) of The Information Technology Act, 2000.

The amendment in 2008 not only made an impact on the way the contraventions under Section 43 of The Information Technology Act, 2000 were adjudicated but also bridged the gap between contraventions and offences under the Act. Even after such a major amendment made in the law, there are few reforms which are yet to be addressed, especially, in Section 43 of The Information Technology Act, 2000 due to techno-legal challenges which arose with the advent of time and development of technology.

Challenges:-

Pavan Duggal et al (2013), an expert of Information Technology Law in India, opined that for an effective impact assessment of the said Amendment one has to take into account the historical evolution of The Information Technology Act, 2000 by analyzing original provision of Section 43 and the challenges and difficulties in implementation of the said legislation.

The Amendment in the year 2008 in The Information Technology Act, 2000 had a massive impact on Section 43. Prior to the Amendment, Section 43 contained sub-clauses (a) to (h) were providing for the penalties for the contraventions under The Information Technology Act, 2000. Two more sub-clauses were added in Section 43 in the form of sub-clause (i) and (j). The major objective for adding the penalties for the contraventions was to make the provision more comprehensive and to give more protection to the victims of the contraventions.

Even though, the purpose of the Amendment was to provide more comprehensive remedy to the victim of the contraventions, after a critical impact analysis one may opine that The Information Technology (Amendment) Act, 2008 was passed in haste and certain very important factors were not considered especially, in respect of the procedural and technological factors in the legislation. The hurry with which the Amendment was passed and how the proper impact assessment was not done prior to the policy decisions were enforced, created certain loopholes in the most important provision of Section 43 of The Information Technology Act, 2000.

There is no doubt that the legislature has added more sub-clauses in the Section 43 of The Information Technology Act, 2000 through Amendment in the year 2008 for giving more remedies to the victim of the contraventions. But whether it has solved the purpose of additional and comprehensive remedies to the victim? For answering this question, one needs to assess the scope of Section 43 of The Information Technology Act, 2000.

Scope of Section 43 of The Information Technology Act, 2000:-

Vakul Sharma et al (2014) observed that, indeed, the scope of Section 43 of The Information Technology Act, 2000 is wide, but does it really create a comprehensive code? Furthermore, it is obligatory to note that Section 43 is the 'heart of the matter' of this Act. One must be creative to interpret this section vis-à-vis various cyber contraventions. The first and major issue which arises in the light of the amendment in 2008 is relating to the scope of Section 43 of The Information Technology Act, 2000.

Once the scope of Section 43 of The Information Technology Act, 2000 is analyzed, it is necessary to study the techno-legal challenges posed for the effective implementation of the provision. Information technology is an ever changing and volatile. It is necessary to legislate on such a volatile subject matter, taking into account the developments and the changes in the field of technology. All the time depending on the judiciary to interpret law liberally is not the long lasting solution to any legal problem.

Legal Challenges:-

The major lacunae that stood in the effective implementation of the Information Technology Act, 2000 is that certain important contraventions and offences as well as the technological aspects are not covered under The Information Technology (Amendment) Act, 2008.

For instance, the liability in case of Online Defamation is not discussed anywhere under The Information Technology Act, 2000. Graham J. H. Smith et al (2007) opined that, publication and dissemination of any information on the internet requires the involvement of many different entities including hosts, network providers and access providers. As these will often have deeper pockets than the author, the extent of their liability for defamatory content handled by them is of great significance.

Few may argue that the provision under Section 66A of The Information Technology Act, 2000 provides for the offence of sending offensive communication. The said offence did not use the term 'defamation' at all. Moreover, the provision under Section 66A provided for a remedy in the form of imprisonment to the offender as a punishment. It was limiting the scope and the purpose of the legislation in the context of the Amendment made in the year 2008. The rule of interpretation says that any criminal law cannot be interpreted liberally. Dr. T. Bhattacharya et al (2001) is of the opinion that, unless the words of the statute clearly make an act criminal, it shall

not be construed criminal. J. Langan et al. (1969) is of the opinion that, strict interpretation can be construed in the interpretation of the penal statute in expressing the essentials of an offence.

On 23rd March, 2015, The Supreme Court of India struck down Section 66A of The Information Technology Act, 2000 in *Shreya Singhal v. Union of India (AIR 2015 SC 1523)* on account of section 66A being voilative of Fundamental Right of freedom of speech and expression.

Another very important issue in the information technology law in India is that of content liability of the social networking websites, which is not just a legal but a technological challenge. The analysis and assessment of the content liability of the Social Networking Websites shall be assessed with fixed and determined criteria which will define the liability and the ingredients of the offence or the liability. The liability of the service provider is always limited and this situation is always exploited by the service providers in the modern disputes on content liability. Louwers and Prins et al (2004) are of the opinion that; to limit the scope of exclusive and blanket protection to service provider, a strict criteria shall be laid down to negate the liability of the social networking sites for content and in rest of the situations they shall be held liable.

Further, David Bender et al (2005) expressed his views that, The Information Technology (Intermediaries Guidelines) Rules, 2011 were issued to deal with the liabilities of the intermediaries. The major limitation of these guidelines is that, it defines the due diligence to be followed by the intermediaries, but it does not define the different types of the content liability of the intermediaries as is the case with the Directives on Electronic Commerce, 2002 in Europe.

Technological Challenges:-

Similarly, the issue of privacy has been shown as a great concern in the constitutional domain but the fact is that, in reality, this issue has not reached at a satisfying level in the form of a full proof provision of any other enactment and also in the field of data privacy or electronic privacy. At the time of enacting The Information Technology Act, 2000, the legislature seemed to have largely neglected the issue of privacy of personally identifiable information. Nandan Kamath et al (2015) opined that, there is a single provision dealing with this under Section 72 of The Information Technology Act, 2000 which is a provision with very limited in its scope to deal with every aspect of privacy in digital world.

Other than the absence or incompleteness of the issues mentioned above; The Information Technology Act, 2000 does not take into account certain common technological aspects which are necessary in case of investigations or for evidence, especially, in case of breach of privacy. One such phenomenon is Internet Protocol (IP) Address. As per the Survey Report of the Privacy Rights Clearing House et al (2013), when the user visits a website, the server of the website records the IP Address of the user. The geographical location from where the website has been accessed can be located on the server. Whenever a person browses, visits a website, sends an email or chats online, one leaves his/her distinctive IP Address behind. It is a digital footprint of the user. Vakul Sharma et al (2014) expressed that, it is possible either by searching IP registration databases or by conducting a trace route, to determine an approximate physical location of an IP address. There is no mandate as to how long the internet service providers are expected to store IP Addresses. There is no specific provision in India regarding the data retention policy to be followed by the internet service providers. The Information Technology Act, 2000 is silent on this issue since its inception.

The Survey Report of Privacy Rights Clearing House et al (2013) mentioned that, the web server may also use the cookies to customize the display, it sends to the user or it may keep track of the different pages within the site the user accesses. This results in number of customized advertisements which includes junk e-mails.

Similarly, certain techniques such as Global Unique Identifiers (GUIDs), Web bugs, Emails and Document bugs, spy wares, online digital profiling, spoofed emails and messages are also largely used for breaching the online or off line digital privacy of the person. Unfortunately, all these techniques are not covered under The Information Technology Act, 2000 in India.

Procedural Challenges:-

Another striking limitation of The Information Technology Act, 2000 is that it does not provide for clarity in certain offences and one has to rely on the other legislations such as Indian Penal Code, 1860, for example, cheating by

personation by using computer resource. If one compares the two provisions, Section 416 of the Indian Penal Code, 1860 and Section 66D of The Information Technology Act, 2000, one significant difference arises. Section 66D of the Information Technology Act, 2000 does not have an element of *mens rea* to constitute the offence of Cheating by personating by using computer means. Whereas, as per Ratanlal and Dheerajlal et al (2011), Section 416 of the Indian Penal Code, 1860 the personating itself is not an offence, and K.D. Gaur et al (2003) also mentioned that the subsequent cheating after personating needs to be committed with fraudulent and dishonest intention.

As per the Report of Working group of RBI on Electronic Banking et al (2011), Section 66D of the amended Information Technology Act, 2000 could be said to cover broadly the offence of cheating by personation by using computer resource, but unfortunately, the major lacuna is that the attempt to commit act of phishing is not made punishable under the said Act.

Another most significant offence of internet fraud is not included in The Information Technology Act, 2000 in its provisions in any manner. As per Jonathan Rusch et al (1999), the types of Internet Fraud schemes that law enforcement authorities are identifying extend well beyond securities-based transactions to many other situations, such as spurious investment and business opportunities, online auctions, sale of computer and internet related products and services, and credit card issuing.

Similarly, Robert Scheinfield and Parker Bagley et al (1996) observed that the opportunity to legislate on the Domain Name Disputes is also lost by the legislature under The Information Technology Act, 2000. Certain technical contraventions or offences like Cyber Squatting and Robert Cumbow et al (1998) observed the same thing regarding Typo Squatting which was not included in the legislation. As per Scheinfield and Bagley, the biggest challenge which The Information Technology Act, 2000 will face, especially with the inclusion of provisions like Section 66 with two fold remedies is that of requirement of proof of intention in highly technical crimes like Hacking.

Any crime, essentially consists of two elements, *actus reus* and *mens rea.* The word '*actus'* connotes physical result of human conduct. As per Smith and Hogan et al (1988), a well known definition of *'actus reus'* is "such result of human conduct as the law seeks to prevent". As per Turner et al (1962), another essential for the crime is *mens rea,* which may comprise a number of different mental attitudes including intention, recklessness and negligence.

Another fundamental requisite of the determining *mens rea* in hacking is that the offender must have been aware at the time of causing the computer to perform the function that the access intended to be secured was unauthorized or illegal. There must be, on the part of the hacker, intention to secure access, though the intention can be directed at any computer and not a particular computer. Thus, the hacker needs not be aware of which computer exactly he or she is attacking or hacking. In such a situation, proving the intention is the most difficult task for the prosecution. Clive Gringras et al (1997) opined that further, the intention to secure access also need not be directed at any particular programme or data. It is enough that the hacker intended to secure access to programmes or data *per se*.

Another issue in relation to contraventions under Section 43 of The Information Technology Act, 2000 which is of great significance is that of legal challenges due to ancillary provisions to Section 43 of The Information Technology Act, 2000.

Law cannot be read in isolation. Section 43 has many dimensions and as it is providing for the remedy in the form of unliquidated damages to the victim of contraventions under the Information Technology Act, 2000, it is dependent on some other provisions and procedures. The Information Technology Act, 2000 also provides for the additional remedy in the form of punishment to the accused, such as Section 66 which provides for the remedy in the form of punishment by way of imprisonment in case the intention of the offender is proved, Section 77 which provides for inclusive clause for the application of remedy under any other law for the time being in force in India together with the provisions under The Information Technology Act, 2000, Section 46, 46A and 47 for the Adjudication of contraventions under Section 43 of The Information Technology Act, 2000, Section 48 of The Information Technology Act, 2000 which establishes Cyber Appellate Tribunal, Section 49 which provides for the composition of the Cyber Appellate Tribunal, Section 61 of The Information Technology Act, 2000 which expressly bars the jurisdiction of civil courts, Section 62 of The Information Technology Act, 2000 which provides for the appellate jurisdiction of high courts from the orders passed by the Cyber Appellate Tribunal and the provisions under Section 1(2) and 75 which encompasses the territorial jurisdiction of The Information Technology Act, 2000.

The ancillary provisions also include the offence under Section 66 of The Information Technology Act, 2000, which exists if the accused commits any contravention under Section 43 with *mens rea*. The biggest challenge in case of technology based offences is that of proving an intention. As per Vakul Sharma et al (2014), the computer related offence involves mental act with destructive animus.

Another challenge before the adjudication of the contraventions under Section 43 of The Information Technology Act, 2000 is the nature of quasi judicial authority which is conferred upon the Adjudicating Officer and Cyber Appellate Tribunal. Vakul Sharma et al (2014) is of the opinion that, the lack of judicial work before the Adjudicating Officers probably did not inspire earlier setting up of the Tribunal.

Another important factor that needs more attention in relation to Section 43 is the remedies provided for victim for the contraventions under Section 43 and other provisions under The Information Technology Act, 2000. The Information Technology (Amendment) Act, 2008 inserted Section 66 which provided for an additional remedy for the contraventions committed under Section 43 in the form of imprisonment, if the contraventions are committed with *mens rea.*

Initially, when The Information Technology Act, 2000 was passed, the contraventions were provided as technical wrongs and special court in the form of Adjudicating Officer was appointed for the adjudication of the contraventions. After the Amendment in 2008, these contraventions can be read as an offence if committed with a *malafide* intention under Section 66. Even though the contraventions are separately tried by Adjudicating Officer, it may become an offence if intention is proved. The lacunae of the provision is that under The Information Technology Act, 2000 there is a special court for trial but there is no special agency for the investigation of the contraventions, even though the contraventions are significantly technical in nature.

Another limitation under The Information Technology Act, 2000 is that, it has not expressly provided for the remedy in the form of injunction for the contraventions under Section 43. Vakul Sharma et al (2014) also opined that, the Adjudicating Officer is a quasi judicial authority who has been conferred with the powers of the civil court. The Adjudicating Officer possesses all attributes of the court.

But The Information Technology Act, 2000 does not provide for any provision for the power of granting injunction in case of contraventions. An expert of civil procedure, Vinay Kumar Gupta et al (2003) expressed that, even if we presume, that the powers of civil courts are conferred on the Adjudicating Officer, one cannot go beyond interpreting the inherent powers of the courts mentioned under Section 151 of The Code of Civil Procedure, 1908. It does not confer any power, but merely indicates that the court possesses such inherent powers. It does not enable the court to do that which is prohibited by the Code. It cannot also be exercised when there are specific provisions in the Code.

Also Mallik et al (2005) expressed that, the injunction is a remedy granted especially in case of specific relief and it is at the discretion of the court. Injunction is granted when there is a danger of waste, damage, obstruction or wrongful sale of property in suit, in execution of a decree, to which the plaintiff has a *prima facie* legal claim, or a threatened breach of contract.

The injunctions are granted by the courts under specific circumstances and only if the requirements under Order 39 of The Civil Procedure Code, 1908 are met. Most of the requirements may or may not be met in case of the contraventions under Section 43 of The Information Technology Act, 2000.

Conclusion:-

In conclusion, the legislative intent to provide comprehensive remedy to the victim of the contravention under Section 43 of The Information Technology Act, 2000 is clearly visible. It shows the broad and wide scope of Section 43 with certain prominent limitations. Sometimes such broad and wide scope raises certain legal challenges to encompass the objectives of the granting remedies to the victims. Through the writings of Jenkins, Vakul Sharma and Adv. Pavan Duggal, one can sense the need for reforms in the existing legal framework as well. Such a reform may also encompass the challenges which are posed due to the technological advancements and the need for reforms in the procedural and ancillary provisions to Section 43 of The Information Technology Act, 2000, such as, too much of hierarchy and set up of appellate courts in the information technology law in India. One must also look into

the additional set of remedies in the form of injunctions which are absolutely neglected in the Information Technology Law. Even though, a comprehensive provision has been created for contraventions in the form of Section 43 of The Information Technology Act, 2000, there is a need to bridge certain gaps which were left out when the amendment of 2008 was passed; hence this study.

After reading the above mentioned literature, one can fact comes to the lights that most of the commentators and authors in India have interpreted and wrote commentaries on The Information Technology Act, 2000, including that of Vakul Sharma and Nandan Kamath, but they have not written any specific commentary on the short comings and limitations of Section 43 of The Information Technology Act, 2000.

The above analysis of literature and the issues express the major in-built challenges for The Information Technology Act, 2000 in India. The scope of development of any law depends on the role of all the three limbs of the state. The legislators initially play an important role through encompassing their vision and realizing the needs of society while enacting legislation. The executives have to implement the existing law through their actions by striking the balance between letter and spirit of the law and larger interest of the society and finally the judiciary which has to interpret the law for the larger good.

It is argued mostly in India that the development of information technology law will take time as the technology will have more pace than that of law. But if the pace of law has to be increased, it is necessary that the critical analysis and impact assessment shall be done of the existing provisions of law. This will encourage the techno-legal minds to think of the possible changes that could be brought up before the legislature which will contribute to the speed of necessity of progressive legislation in the field of information technology.

Most of the commentators and authors in India also have an approach of introducing the lacunae but not critically evaluating the existing legal framework with the lacunae which they have introduced. This has lead to mere discussions on the lacunae and not promoting it up to the level of intent to recommend changes in the existing legislation or a specific provision of the legislation.

As the provision is comparatively very recently affected by way of an Amendment in 2008, there are not many judgments and interpretations available from the higher courts, which limit the development of scope of the provision. This is primary reason for the gaps in literature.

It is high time that the legislature critically evaluates all possible lacunas in The Information Technology Act, 2000 and especially, relating to Section 43 dealing with the contraventions for the larger good of the victims of contraventions.

References:-

1. **Glenn P Jenkins, (1996),** Information Technology and Innovation in Tax Administration, 1st ed., 2
2. **Adv. Pavan Duggal (2013),** IT Amendment Act Perspectives, http://www.cyberlaws.net/new/pd_on_ITAmendments.php
3. **Vakul Sharma, (2014),** Information Technology Law and Practice, 3rd ed., 117-125
4. **Graham J. H. Smith, (2007),** Internet Law and Regulation**,** 4th ed., 312-314
5. **Dr. T. Bhattacharya, (2001),** Interpretation of Statutes, 4th ed., 81
6. **P. St. J. Langan, (1969),** Maxwell on Interpretation of Statutes, 12th ed., 239-240
7. **Louwers and Prins, (2004),** International Computer Law, 22-66
8. **David Bender, (2005),** Computer Law, 3.1.2
9. **Nandan Kamath, (2015),** Law Relating to Computers, Internet and E-Commerce**,** 5th ed. 312-315
10. **Ratanlal and Dheerajlal, (2011),** The Indian Penal Code, 1860, 32nd ed., 915-918
11. **K.D. Gaur, (2003),** A Textbook on The Indian Penal Code, 2nd ed., 575-578
12. **Robert Scheinfield and Parker Bagley, (1996),** Long Arm Juridiction, Cyber Squatting, NYLJ, 123
13. **Robert Cumbow, (1998),** Typosquatters Pose Threat to Trademark Owners on the Web, Misspell a Domain Name, Wind up at a Rival Site, NYLJ, 60
14. **Smith and Hogan, (1988),** Criminal Law, 6th ed., 36
15. **Clive Gringras, (1997),** The Laws of the Internet, 221
16. **Vinay Kumar Gupta, (2003),** Mulla's The Key to Indian Practice, 8th ed., 176-177
17. **Mallik, (2005),** Ganguly's Civil Courts Practice and Procedure, 13th ed., 957