CHANAKYA LAW REVIEW (CLR)

Vol. III (ISSUE 02) JULY-DEC, 2022, pp.33-39

Ensuring Compliance in Cyberspace: The Need for Robust Cyber Law Enforcement

Upasana Priya[54]

ABSTARCT

Cyberspace has become an integral facet of modern world which makes robust enforcement of cyber law, the need of the hour. An individual's privacy and security in the digital realm can only be protected by cyber law enforcement which ensures the compliance with laws, standards and regulations designed to protect them. In that context, this Article examines the lacunae in the implementation of cyber laws, the challenges faced in the enforcement agencies including cross-border cyber frauds. It aims to critically analyse the reasons for the ineffective implementation. The Landmark cases are also discussed for throwing light on it. This Article also suggests proactive measures such as creating awareness regarding cyber threats, educating about risks and strengthening the legal framework for the prosecution of cybercriminals. A secure and resilient digital world can be built for all by addressing the challenges and leveraging emerging technologies.

Keywords: Cyber Space, Privacy, Cyber Law, Cyber Fraud.

Introduction

The term Cyber Law has, per se, not been defined in any Indian statute be in Information Technology Act, 2000 or the Indian Penal Code, 1860 (These are some of the legislations governing Cyber Law in India). As a matter of fact, the wide connotations of the field of law make it nearly impossible to contain it in a single definition.

With the increasing reliance on the Internet, there arose a need to regulate the space and form stringent laws and policies to keep criminal activities at bay. In the Indian context, none the existing legislation was having the ability to incorporate these restrictions as the laws were

[54] Ph.D. Research Scholar (2022-2023) Chanakya National Law University, Patna.

formulated keeping in mind the socio-economic conditions of the past and could not fulfill the contemporary requirements. This gap in legislation, which was largely unforeseen at the time of enactment of older legislations, needed to be filled in and that was done with the help of Information Technology Act, 2000 (*hereinafter* "IT Act, 2000") and the Rules and regulations therein.[55] With the introduction of this act, a supporting legal infrastructure was aimed to be provided to the cyberspace.

Governing Legislations

The Ministry of Electronics & Information Technology is the governing body as far as the specific legislations regarding the cyberspace are concerned. The primary legislation dealing with regulation of cyberspace is the *Information Technology Act, 2000* and the subsequent amendments including Amendment Act of 2008. Various notifications regarding the IT Act, 2000 have been passed by the ministry clarifying various aspects mentioned in the Act.[56] In addition to that, various other legislations like *Indian Penal Code, 1860; Indian Evidence Act, 1872* etc. also have provisions that regulate the cyber laws in India. I shall not dwell into the intricacies of the provisions for the purpose of this paper.

In addition to the various statutes mentioned above, the ministry, from time to time, by way of press releases, office memorandum or various protocols, keeps incorporating additional aspects in the realm of cyber law. Some of the major ones are enlisted below:

In May 2011, in a press release by the Press Information Bureau, Ministry of Communications & Information Technology regarding exemption from liability for hosting third party information: diligence to be observed under Intermediary Guidelines Rules. This was regarding the Rules notified under Section 79 pertaining to liability of intermediaries under the IT Act, 2000.[57]

In 2015, '*National Encryption Policy'* was proposed to be set up to ensure secure transactions in Cyber Space for individuals, businesses and Government. A draft was prepared on a High Level Expert Committee's recommendations and put up on the website of DeitY for public comments. However, taking note of certain ambiguities, it was withdrawn.[58]

[55] Information Technology (Certifying Authorities) Rules, 2000; Information Technology (Security Procedure) Rules, 2004; Information Technology (Certifying Authority) Regulations, 2001.
[56] All major notifications available at https://www.meity.gov.in/content/notifications.
[57] Available at https://www.meity.gov.in/writereaddata/files/PressNote_25811.pdf.
[58] Available at https://www.meity.gov.in/writereaddata/files/national-encryption-policy-govt_0.pdf.

On 18th April 2017, Ministry of Electronics & Information Technology's Cyber Law and e-security division passed order regarding measures to curb Online Child Sexual Abuse Material (CSAM) to contain the spread of such material.[59]

In July 2017, the Ministry of Electronics & Information Technology issued an office memorandum regarding constitution of a committee of experts to deliberate on a data protection framework in India wherein an expert committee was sought to be formulated.[60]

The most recent of the legislations to be considered is regarding the Aarogya Setu App envisaged in the *Aarogya Setu Data Access and Knowledge Sharing Protocol, 2020*.[61] The protocol deals was passed to ensure secure collection of data by the Aarogya Setu mobile application, protection of personal data of individuals, and the efficient use and sharing of personal and non-personal data for mitigation and redressal of the COVID-19 pandemic.

On 25th February, 2021, the *Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021* were passed by Ministry of Electronics and Information Technology (MeitY) in order to ensure an Open, Safe & Trusted Internet and accountability of intermediaries including the social media intermediaries to users. These Rules prescribe the due diligence to be followed by all intermediaries as well as the additional due diligence to be followed by significant social media intermediaries. The Rules also provide guidelines to be followed by publishers of news & current affairs and also online curated content providers. The Rules have two segments:

1. Intermediary Guidelines administered by MeitY.
2. Digital Media Ethics Code administered by the Ministry of Information & Broadcasting (MIB) in line with the distribution of subjects under the Government of India (Allocation of Business Rules), 1961.

Landmark Precedents

One of the oldest cases regarding cyber law in the history of world was the infamous case of *R.* v. *Thompson*[62] wherein the perpetrators in the US Air force and NASA were convicted of

[59] Available at https://www.meity.gov.in/writereaddata/files/Order%20regarding%20online%20CSAM.pdf.
[60] Available at https://www.meity.gov.in/writereaddata/files/MeitY_constitution_Expert_Committee_31.07.2017.pdf.
[61] Available at https://www.meity.gov.in/writereaddata/files/Aarogya_Setu_data_access_knowledge_Protocol.pdf.
[62] (1984) 79 Cr App R 191.

cyber-crime and fraud. This cyber theft involved stealing of sensitive information and even embezzlement of money from some Kuwait bank accounts to their own English bank accounts.

India's first case dealing with cyber-crimes came only in 1999 with the case of *Yahoo, Inc.* v. *Akash Arora.*[63] In this case, Yahoo! demanded a permanent injunction against the respondents who were using the website "yahooindia.com". The court, while upholding the intellectual property rights of Yahoo, held that such a use creates deception among the customers and the party was held liable. This judgment was reiterated in the case of *Rediff Communications Ltd.* v. *Cyberbooth.*[64] In Yahoo!, in another case regarding posting of defamatory, offensive and threatening messages on a group, the court convicted the accused under Section 67 of the IT Act, 2000.[65]

The Case of *Syed Asifuddin and Ors.* v. *The State of AP & Ors.*[66] was regarding the manipulation and stealing of programming code of cell phone digital handset of Reliance Infocomm. The devices were specifically programmed by TATA Indicom for Reliance. Misusing the same, certain individuals altered the code and manipulated the same with the crux of providing better deal to the customers which would have caused losses to both companies. In technical terms, ESN of the code was altered and that amounted to a strict hit on Section 65 of the IT Act, 2000 and they were held liable.

In *State of Tamil Nadu* v. *Suhas Katti,*[67] a divorcee woman was assaulted by way of obscene and inappropriate messages on yahoo message groups and false e-mails were sent impersonating her. In one of its first convictions in the country, the accused was held liable under Section 67 of the IT Act, 2000.

With regarding to publishing of obscene material online punishable under Section 67 of the IT Act, 2000, the definition was also extended to considering transmission as also a part of publication in a manner. This was established by a case where in a private MMS was put on sale by the website "Baazee.com" and was bought by several consumers before it was put

[63] (1999) 19 PTC 229 (Delhi).
[64] AIR 2000 Bom 27.
[65] Tamil Nadu v. Suhas Katti, (2004) Cr. Comp 4680.
[66] 2005 Cri LJ 4314.
[67] C No. 4680 of 2004.

down. Even though there was no direct publication, Section 67 of the IT Act, 2000 was attracted.[68]

The issue of impersonation, as mentioned in a prior case as well, is also one of the most problematic issue as far as cyber-crimes are concerned. In an instance, a woman's personal contact details were disclosed on the public forum by the defendant while impersonating her. After receiving threatening and inappropriate calls, she filed in a complaint. The defendant was booked under Section 509 of the Indian Penal Code, 1860.[69]

The most well-known and landmark judgment in the realm of cyber law is undeniably the case of *Shreya Singhal* v. *Union of India*,[70] wherein the Hon'ble Supreme Court held Section 66A of the IT Act, 2000 as unconstitutional. It was held as violative of Article 19 of the Constitution and not falling under reasonable restrictions as specified in Article 19(2) as it was overly broad and vague.

Problems in Effective and Efficient enforcement

Like any other newly formed legislation, there is a major problem in proper implementation and subsequent enforcement of the laws due to the lack of awareness or issues regarding acceptance in the society to name a few. In the case of cyber laws, the problem becomes multifarious due to the involvement of technicalities that the justice system of the country from the investigative agencies to the judges are not well versed with at the instance. Some of the issues regarding enforcement are listed below-

1. **Jurisdictional Issue**: Since the realm of cyberspace is not restricted to a particular territory, there arises a major and foremost issue as to jurisdiction. Different countries in the world have varied laws and treatment as far as cyber law is concerned depending on how developed the country is, what kind of resources it possesses and the like, and there is not much standardization.
2. **Lack of Awareness:** A major issue as far as cyberspace is concerned is the issue of lack of awareness regarding the same in general public. The realm is a relatively new aspect of law, and that becomes an impediment in the enforcement. A lack of awareness results in less reporting of cases and ultimately reduced redressal.

[68] Avnish Bajaj vs. State (N.C.T.) of Delhi, (2005) 3 CompLJ 364 Del.
[69] Manish Kathuria v. Ritu Kohli (2001)
[70] (2015) 5 SCC 1.

3. **Lack of proper technical proficiency of the implementing authorities** – Due to the dynamic nature of cyberspace, there is a problem of technical know-how among the investigating agencies and also the adjudicatory bodies. The courts are not fully equipped and even in specialized tribunals; there is a dearth of specialized knowledge.
4. **Complicated and Expensive** – Building on to the previous point, the complicacy in the area makes it very difficult and even expensive to enforce due to the need for specialized technical understanding of complex aspects. A separate infrastructure and expert witnesses are required which complicates things and can be pricey.
5. **Gaps in legislation** – Due to various gaps in legislation, there are many loopholes in the legislations that are very easy to misuse. This problem is not confined to cyber law but almost every newly made statute suffers from this difficulty and can only be cured by way of incessant efforts by the authorities.

Way Forward and Suggestive Analysis

As far as the preventive measures are concerned, following are some of the measures that can prove to be effective in proper enforcement –

1. **Consumer Education**: Cyber law is by far one of the more ill-informed areas of law due to multifarious reasons such as lack of awareness and know how among the older generation and also due to the fact that it is a very recent concept that took shape only a few years back. Hence, the most important tool for its mitigation also commences at consumer awareness. There is a dire and urgent need to make the public aware of the modes and new ways of digital frauds. This can help mitigate the problem at the root level and prevent it from expanding.
2. **Protection by corporate :** Another basic, yet effective method is the adoption of preventive measures by the organizations themselves in the form of warnings, ensuring proper authentications and many more tools. Having huge resources and technical know-how, the corporate organizations can easily warn the consumer of the risks involved. Some of these are very common and experienced by almost every consumer. Some examples being-
    - Sending regular messages about the mode of asking for OTPs.
    - Warning phrases before the start of a consumer complaint call.
    - An effective e-security framework of an organization can go a very long way in the combat of problem effectively and efficiently.

3. Data storage and protection measures: Building up to that, it is also imperative that the user data be a restricted access data and only the essential personnel be allowed to access the data. Additionally, as far as possible, the data ought to be encrypted before any processing or before it falling into the hands of any employee or a third party organization for processing.

4. Non-technical information to consumer: In line with the previous point, it is an important aspect that the information presented to the affected party should be in clear, unambiguous terms. The realm of cyberspace is fairly technical there is a need to simplify the rights of the consumers and stakeholders. For instance, the Terms and Conditions, Employee contracts, briefings etc. on this aspect should be made uncomplicated.

5. Fast and effective redressal mechanism: In this fast moving world, crime is multiplying at a swift pace and redressal mechanisms ought to move at a much faster rate. Also, especially in terms of cyber-crimes, the only way to beat it is to be ahead of it. Cyber security modules must update themselves in order to keep pace with the new methods of attack technology.

Conclusion

With the advent of a digital culture in India and the world, there is a need to make requisite amendments to the laws relating to the field of law. To put simply, crime has found a new interface. As the dependence on technology increases, an increase in cyber-crimes is an innate consequence. Here, the essential question that arises is that how much we are willing to put ourselves at risk for the sake of convenience and ease. After a careful research and understanding of the existing legal provisions with regard to cyber law, it is more than clear that the legislation is insufficient, at best. There are multitudes of gaps that need to be fixed by way of expert and technical law making. However, an important aspect that is to be kept in mind is that due to the nature of cyberspace, it is highly dicey that there can ever be a fool proof method or legislation to completely rule out any such act. The important thing is that law needs to keep evolving as an equal rate as the increment in the intensity and magnitude of the crime.

****