Christ University Law Journal
2018, Vol. 7, No. 2, 1-22
ISSN 2278-4332X | https://doi.org/10.12728/culj.13.1

A Critical Analysis of the Information Technology Act, 2000 vis-à-vis Mitigation of Child Pornography

Aishwarya Deb* and Prithwish Roy Chowdhury†

Abstract

This paper investigates the efficacy of the provisions of the Information Technology Act, 2000 dealing with child pornography which has been, more often than not, considered to be a victimless crime. The author argues that the ambiguity in the provisions of the Act has led to arbitrariness in investigations and procedures dealing with the offence of child pornography. This paper, by critically analysing the provisions of the aforementioned legislation vis-à-vis child pornography, attempts to show that the menace can be mitigated by following a victim-centred approach and also by incorporating certain procedural standards, as per the Budapest Convention, 2001. The authors also make an attempt to propose certain changes which are required in the existing legislation, in order to effectively deal with the said crime in cyber space, in a more victim or child friendly manner.

Keywords: Budapest Convention 2001, Child pornography, Cyberspace, Information Technology Act 2000, Victim-centred approach

*NALSAR University of Law, Hyderabad, India; aishwarya.deb@nalsar.ac.in

†Advocate, Calcutta High Court, India; 12bll011@nirmauni.ac.in

1. Introduction

"To no one will we sell or deny or delay right or justice"

– Magna Carta

Although India is a party to the UN Convention on the Rights of the Child, 1990, which strives to secure the rights of children, the Indian society has tried very hard to brush off the issue of child pornography. It starts from the families of children who are victims of child pornography that try to conceal the issue, due to fear of persecution, resulting in underreporting of the crime and underestimation of the gravity of the problem. The child, by reason of his/her physical and mental immaturity needs special safeguards and care, including appropriate legal protection.[1] India, having enacted a special legislation, namely the Information Technology Act, 2000, on the 9th of June, 2000, put forward a major step to combat crimes in cyberspace. However, one cannot deny the fact that there has been an increase in the publication and transmission of sexually explicit content involving children.[2] Hence, the effectiveness of the provisions dealing with child pornography under the aforementioned legislation needs to be questioned.

Earlier, various scholars had justifiably highlighted the inherent ambiguity in the provisions of the Act dealing with child pornography and had put forth the view that absence of clarity in any special legislation is indeed a ground for protest, as per the void for vagueness doctrine.[3] Also, research in this area points out that child pornography has, more often than not, been treated as a victimless offence owing to the ambiguity surrounding child pornography laws and weak connection between the victim and

[1] United Nations Convention on the Rights of the Child, Preamble, ¶10, *opened for signature* Nov.20, 1989, http://www.ohchr.org/ EN/ Professional Interest/ Pages/CRC.aspx(last visited on Mar. 10,2018).

[2] M.M. Singh et al., *An epidemiological overview of child sexual abuse*, 3(4) J Family Med Prim Care 430-435 (2014), https:// www.ncbi.nlm.nih.gov/ pmc/articles/PMC4311357/ (last visited on Mar. 10, 2018).

[3] Amlan Mohanty, *New Crimes under the Information Technology (Amendment) Act*, 7 IJLT 118, 119 (2011).

the possessor of the pornographic content, due to the dynamic nature of virtual space.[4]

However, the pertinent question that is left unanswered is whether the existing legal framework adequately administers investigations relating to child pornography. Considering the fact that a complete eradication of child pornography may not be possible, can the problem be mitigated by following a victim-centred approach? These are some critical issues which will be untangled in the course of this paper, as the author explores the contentious issue of child pornography, by critically analysing the relevant provisions of the Act.

The initial section of the article aims to address the shortcomings of the legislation in the matter of setting up a preventive mechanism to deal with the menace of child pornography, thereby highlighting the need for a modified and compact legislation. The next section analyses the legal provisions penalising the offence of child pornography and further looks into the role of intermediaries. This section also explores the investigation procedure related to the crime and proposes a model to be followed in accordance with the Convention on Cybercrime, 2001[5]. The issue of victimisation has been dealt with in the third section of the paper which proposes the need for incorporating a victim-centred approach in the legislative structure. This is followed by the section which deals with the issue of a complete ban on child pornography and discusses its possibilities. The final part of the paper suggests certain changes which can be implemented in the existing legislature to make the system more victim-friendly and curb the menace to a large extent.

---

[4] Audrey Rogers, *Child Pornography's Forgotten Victims*, 28 PACE L. REV. 847,864 (2008).

[5] *Convention on Cybercrime, 2001*, November 23, 2001, ETS No. 185, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf (last visited on Feb.20, 2018)

2. Information Technology Act, 2000

2.1 Scope of the statutory provision dealing with child pornography in India

India has emerged as one of the biggest contributors and consumers of child pornography, despite a crackdown against such material on the Internet.[6] The statistics provided by the National Crime Records Bureau reveals that there were almost one hundred and thirty-two cases of child pornography pending before various Courts in India, in the year 2016.[7] This leads us to question the effectiveness of the present legislation dealing with cybercrimes in India. However, before analysing the efficacy of the legal provisions, we must understand the term 'child pornography'.

The Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography, 2002(hereinafter referred to as 'Optional Protocol') defines the term **"**as any representation, by whatever means, of a child engaged in real or simulated explicit sexual activities or any representation of the sexual parts of a child for primarily sexual purposes**"**[8]. Similarly, the Convention on Cybercrime, 2001(primarily known as the Budapest Convention) defines the term 'child pornography' to include "...pornographic material that visually depicts:

a) a minor engaged in sexually explicit conduct;

b) a person appearing to be a minor engaged in sexually explicit conduct;

---

[6] Shashank Shekhar, *Despite crackdown, India emerges as one of biggest contributors, consumers of child porn,* INDIA TODAY, (Sept. 6, 2017),http://indiatoday.intoday.in/story/child-pornography-kerala-haryana-csam/1/1041706.html (last visited on Oct.16,2017)

[7]Ministry of Home Affairs, National Crime Records Bureau, *Crime in India 2016*, 200 (October, 2017).

[8] The Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography,art.2(c), May 25, 2000, http://www.ohchr.org/ EN/Professional Interest/ Pages/ OPSCCRC.aspx (Last visited on Mar. 10, 2018)

c) realistic images representing a minor engaged in sexually explicit conduct."[9]

The Convention aims to deal with the problem of child pornography, by providing a common perception on such crime, thereby solving the jurisdictional and international cooperation issues related to it. On the contrary, the Information Technology Act, 2000 (hereinafter referred to as the Act) was framed in accordance with the United Nations Commission on International Trade Law Model Law on E-Commerce, to provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication[10], with very little focus on combating cybercrimes *per se*.

The Information Technology (Amendment) Act, 2008 brought along with it penal provisions to deal with crimes in cyberspace. The fact that the said amending legislation was passed as a reactionary measure in order to address the rise in number of cybercrimes, is discernible from the vague and ambiguous provisions of the Act, which criminalise offences without defining the scope of activity that could classify as criminal.[11] The Act attempts to penalise the offence of child pornography under Section 67B by not only punishing the act of 'publishing' or 'transmitting' of pornographic content involving children, but also its collection, online viewing, downloading, promotion, exchange and distribution. However, it leaves outside its scope, the act of viewing such content. Further, the Act has failed to provide an inclusive definition of the term 'child pornography'. Hence, the penal provision suffers from ambiguity to a certain extent. Specifically, the phrase "abusing children online" is vague as it does not provide whether such abuse should be sexual in nature or not, even though as per our understanding, pornographic content usually includes "sexually explicit content". Such vagueness and

[9] Convention on Cyber Crime, art. 9(2), *opened for signature* November 23,2001, ETS No. 185, https://rm.coe.int/1680081561(last visited on Mar. 10, 2018)

[10]The Information Technology Act, 2000, No. 21, Acts of Parliament,2000, (India) Preamble, ¶1.

[11]Mohanty, *supra*note3, at 103-105.

complexity in the provision itself has led to ineffective measures dealing with child pornography. Consequently, it becomes difficult to distinguish sexually explicit content involving children from other pornographic materials.

Although India is a signatory to the Optional Protocol, 2002, the Act does not set forth any method to independently identify pornography and places the responsibility on the regulatory authorities and Courts to identify such, on a case to case basis. Considering the fact that cyberspace, owing to its dimension, provides for certain liberties that makes it easier to contravene legal provisions, it is not advisable for the legislation to be left open to broad interpretations.[12]

Complexity in the penal provision is one of the major reasons for lower conviction rates for the offence of child pornography in India. The rise in the number of pornographic content involving children that is being uploaded from India, is a clear proof of the fact that the said statute has been ineffective in deterring people from committing the offence. Instead, it has, to a certain extent, led to the abuse of power granted to the public officials, which is quite evident from the thriving black market of pornography.[13] However, the very fact that cybercrimes can be easily learnt and executed, require fewer resources relative to the potential damage caused, can be committed in a jurisdiction without being physically present in it and are often not clearly illegal, make criminalisation of such conduct essential.[14] Although the rationale behind inserting such provisions in the Act was to punish the perpetrators for the harm inflicted upon children and protect the victims against future harm, the Act seems to have failed to fulfil the objective. What is therefore required on the part of the legislature, is to lay down parameters for implementation of the penal provisions.

---

[12] *Id*.at 119.

[13] *See* Vallishree Chandra and Gayathri Ramachandran, *The Right to Pornography in India: An analysis in light of individual liberty and public morality*, 4 NUJS L Rev 323(2011).

[14] Mohanty, s*upra* note 3, at107.

2.2 Liability of intermediaries in the circulation of sexually explicit content

Circulation of any sort of content in cyberspace is dependent on an intermediary, who on behalf of another person, receives, stores or transmits that record or provides any service with respect to that record. This includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes.[15] However, the author only intends to analyse the question regarding the immunity granted to intermediaries vis-à-vis the offence of child pornography and all other considerations with respect to the role of intermediaries is beyond the scope of this paper.

The functioning of the intermediaries comes under strict scrutiny especially in cases of obscenity and pornography, since they are the ones without whom circulation of such material would be impossible. The intermediary's liability is primarily used as a control mechanism to prevent undesirable content from being transmitted or published on the internet. Despite having such a mechanism, there has been a hundred percent increase in cases of publication or transmission of obscene material, including child pornography, using electronic means.[16] The question of intermediary liability was first raised in *Avnish Bajaj v. State(NCT of Delhi)*[17], also known as the *Bazee.com* case, where the sexually explicit content in question involved children and was required to be removed from the web immediately, but was circulating swiftly

[15]The Information Technology Act, 2000, §2(w), inserted vide The Information Technology (Amendment) Act, 2008 (w.e.f. October 27, 2009), No.09, Acts of Parliament, 2009 (India).

[16]Devesh K. Pandey, *Pornography cases up 100 percent last year,* THE HINDU (New Delhi), August 07, 2014, http:// www.thehindu.com/ news/national/pornography-cases-up-100-per-cent-last-year/ article 6288856.ece (last visited on Mar. 10, 2018); *See* Ministry of Home Affairs, National Crime Records Bureau, *Crime in India 2016*, 201-204 (October, 2017), http://ncrb.gov.in/ Stat Publications/CII/ CII2016/ pdfs/ NEWPDFs/Crime%20in%20India%20-%202016%20Complete% 20PDF%20291117.pdf (last visited on Mar. 10, 2018).

[17]Avnish Bajaj v. State(NCT of Delhi), (2008) 150 DLT 769 (India)

through mobile networks and the internet, because multiple people were sharing it.[18] It has been mooted by few cyber lawyers that keeping in view the paradigm of the internet, an area where it is practically impossible for service providers of platforms to control the act, omissions of primary/secondary/ tertiary users of such platforms, the intermediaries should not be held liable for such an act/ omission, unless they possess actual knowledge of the same.[19]A *prima facie* case under Section 292 of Indian Penal Code, 1860 and Section 67 of the Information Technology Act, 2000, was made out against the appellant in the *Avnish Bajaj* case. The judgment[20] rendered by the Hon'ble Delhi High Court in the aforementioned case, was one of the driving forces behind amendment of Chapter XII of the Act, which now exempts the liability of the intermediaries in certain cases. The intermediaries have been granted conditional immunity under Section 79 of the Act, so much so, that the intermediaries abiding by the due diligence requirements under this section, are exempt from liability.

The Information Technology (Intermediaries guidelines) Rules, 2011,[21]framed by the Central Government in exercise of the powers conferred by Section 87(2) (zg) read with Section 79(2) of the Information Technology Act, 2000 provides for the due diligence requirements to be fulfilled by the intermediaries[22] in order to be immune from the acts of third parties, of which they did not possess actual knowledge. However, on a plain reading of the provision dealing with child pornography, the act of publishing or transmitting of sexually explicit material involving children, whether knowingly or unknowingly, is a criminal offence. What follows from this interpretation is that the qualified immunity

[18]*See* ChinmayiArun, *Gatekeeper Liability and Article 19(1)(a) of the Constitution of India*, 7 NUJS L Rev 73(2014).

[19] SharatBabuDigumarti v. Govt. (NCT of Delhi), (2017) 2 SCC 18,¶ 39 (India).

[20]Avnish Bajaj v. State(NCT of Delhi), (2008) 150 DLT 769 (India)

[21]*See* The Information Technology (Intermediaries guidelines) Rules, 2011, Preamble.

[22]*Id.* at Rule 3.

provided to the intermediaries is an exception to the penal provision. However, the liability of the intermediaries has once again come under spotlight with the *Kamlesh Vaswani case*[23] and questions have been raised regarding the removal of such immunity as well.

It cannot be ignored that the measures taken by the intermediaries are often ineffective in regulating the content being uploaded on the web-based platforms.[24] With the sexually explicit contents circulating through the internet to multiple devices, inability on the part of the intermediaries seems to be justified on the face of it.

It is obligatory on the part of the intermediary to publish the rules and regulations, privacy policy and user agreement for accessor usage of the intermediary's computer resource by any person[25]. Yet, owing to the multifarious nature of cyberspace and user anonymity, the intermediaries have often expressed inability to remove or block the sexually explicit material. Also, several intermediaries do not have the resources or technological capacity to achieve the requisite degree or targeted blocking or filtration[26]. This has forced the internet service providers to direct the parties to approach the Court and obtain orders for the removal of such material. As a result, the pornographic content remains on the website till the direction is issued by the Court. However, removing the immunity granted to the intermediaries and criminalising their actions, cannot be a proper solution to the problem of wide circulation of pornographic content. The Hon'ble Supreme Court has already deliberated upon the scope of protection granted to the intermediaries in the case of *Shreya Singhal v. Union of India*.[27]

On a cursory reading of Section 69A of the Act, we can infer that the blocking of any pornographic content can take place only by a

---

[23]KamleshVaswani v. Union of India &Ors., (2016) 7 SCC 592 (India).

[24]*See* Tata Sky Ltd. v. Youtube LLC &Ors., 2016 SCCOnline Del 4476 (India).

[25]*Supra* at 22.

[26]Arun, *supra*note 18.

[27] Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).

reasoned order, after complying with several procedural safeguards including a hearing of the originator and intermediary[28]. In such a case, no question arises regarding the intermediary applying its own mind to whether information should or should not be blocked.[29] The Hon'ble Apex Court in *Sharat Babu Digumarti v.Government (NCT of Delhi)*[30], reversed the decision rendered in the *Avnish Bajaj* case, and refrained from striking down Section 79(3)(b) of the Act, by concurring with the dictum in the *Shreya Singhal* case. The Court emphasised on the fact that the horizon of Section 79 has been expanded to protect the intermediaries, who do not possess actual knowledge of the content, unlike the originator to whom the protection has deliberately not been accorded. Since Section 67, along with Sections 67A and 67B together form a complete code, Section 79 therefore, can be treated as an exemption provision to this holistic trinity. The Act being a special legislation, once an offence has nexus or connection with electronic record, the protection and effect of Section 79 cannot be ignored and negated, since it explicitly uses the non-obstante clauses and has an overriding effect on any other law in force.[31]

In such a scenario, the responsibility lies entirely with the Courts to take a step ahead and give preference to cases involving child pornography or petitions filed before them, seeking order for blocking websites containing sexually explicit content, and grant instant relief by way of interim orders to block or remove such material. If such a step is not taken, then approaching the Court for relief will be nothing but a futile exercise and even if a direction is given after lapse of time, it would not serve any purpose and the loss suffered would not be compensated in monetary terms.[32] However, coming back to the question of liability of the intermediary, the strict liability standard cannot be imposed on the

---

[28]SharatBabuDigumarti v. Govt. (NCT of Delhi), (2017) 2 SCC 18,¶28 (India).

[29]*Id*.

[30] (2017) 2 SCC 18 (India).

[31]SharatBabuDigumarti v. Govt. (NCT of Delhi), (2017) 2 SCC 18,¶ 32.

[32]Google v. M/s. Visaka Industries Ltd., 2016 SCC Online Hyd 393 (India).

intermediaries because they act primarily on the order of the appropriate government and at times, the Courts, too.

2.3 Need for a standard procedural code as per the Budapest Convention

Owing to the fact that India is not a signatory to the Budapest Convention 2001, the investigative processes concerning cybercrimes have faced a major setback due to lack of a standard code prescribing ways and measures to carry out such tasks. The Budapest Convention is the first of its kind, since it seeks to develop a common criminal policy aimed at protection of society from cybercrimes, by formulating domestic legislations in a manner to effectively fight against such crimes and develop mutual co-operation amongst countries. It is also one of a kind as it tries to effectively provide for a distinct definition of the term 'child pornography'.

Though our cyber legislation is modelled in a way to provide for punishment in case of publishing or transmission of sexually explicit content involving children, the terminology used is quite ambiguous, hence making it difficult to convict persons under the said provision. Also, Section 67B cannot be read alone, but has to be read with Sections 67[33] and 67A,[34] since they together form a complete code. The fact that the conviction rates are low under the said legislation is itself proof of the complexity of procedure relating to cybercrimes in India.[35] Further, the Courts have traditionally been using the same standard test to deal with cases concerning pornography and obscenity. However, all the obscene content on the internet cannot be classified as pornography.[36] The Act merely provides that the investigative agencies have the same powers as enshrined under the Code of Criminal Procedure, 1973.[37]

---

[33]The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, (India),§ 67.

[34]*Id.* at § 67A.

[35]*Supra* note 7,at 196.

[36]*See*MaqboolFida v. Rajkumar Pandey, (2008) Cri LJ 4107 (India).

[37]The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, (India), § 80.

Considering the fact that cyberspace has its own unique characteristics, the procedures used for carrying out investigations in real world are ineffective when it comes to dealing with cybercrimes. Child pornography investigations are most of the times initiated due to a complaint made by a third party, who discovers what he or she believes to be pornographic content involving children on any electronic media, to a law enforcement agency. The investigative agencies may face various issues while carrying out an investigation pertaining to a case of child pornography. For instance, there might be jurisdictional issues when the required evidence has to be retrieved from some other country which eventually leads to the question of geographical determinacy.

The Budapest Convention provides for certain standards regulating the intrusive surveillance and interception of communication, which are major components of cybercrime investigation. For instance, the Convention makes it obligatory for the State parties to empower its competent authorities, to order a person in its territory to submit specified computer data in that person's possession or control. Also, a service provider is expected to submit subscriber information relating to such services in that service provider's possession or control.[38]

Since India is not a signatory to this Convention, it cannot avail this provision for smooth functioning of the investigation process, in cases involving pornographic content. Apart from this, the Convention also obligates the contracting parties to co-operate with each other through the application of international instruments on international co-operation, in criminal matters. This extends to arrangements agreed on the basis of uniform or reciprocal legislation and domestic laws, to the widest extent possible for the purposes of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.[39] It also

[38]Convention on Cyber Crime, art. 18, *opened for signature* November 23, 2001, ETS No. 185, https://rm.coe.int/1680081561 (last visited on Mar. 10, 2018).

[39]*Id.*atart.23.

provides for the scope of mutual assistance amongst State parties as far as possible, for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.[40] Even though the Act has provided for extraterritorial operation under Section 1 and Section 75, the investigative agencies often face breach of privacy issues in cybercrime investigation since India does not have any reciprocal arrangements with other states concerning cybercrime jurisdiction. It becomes difficult for them to get hold of evidences and obtain access to data held on systems located in foreign jurisdictions. The procedural methods provided under Sections 166A and 166B of the Code of Criminal Procedure, 1973 (hereinafter referred to as 'Code') are far from being effective owing to its cumbersome nature, which ultimately delays the whole investigation proceeding, usually leading to the destruction of evidence. Had India been a signatory to the Budapest Convention, which provides for special procedure for the search and seizure of stored computer data[41], it would have been much easier for the investigative agencies to get hold of the violating content.

Since cyber space is a virtual medium, the techniques used to sort and figure out evidences in 'real world' crimes seem to be quite inappropriate in dealing with crimes committed on a virtual medium. Also, Section 188 of the Code which lays down the procedure to be followed for offences committed outside India fails to incorporate any special measures that need to be taken in case of offences committed in cyberspace.

On the contrary, the Budapest Convention makes it possible for state parties which do not have an extradition treaty with some countries, to extradite offenders responsible for committing virtual criminal offences, by considering the Convention as the legal basis of such extradition.[42] As it is already known to us that India has

[40] *Id.*atart.25.

[41] *Id.*atart.19.

[42] *Id.* at art.24.

extradition treaties with only forty two countries[43], it might face hindrances where the alleged offender is from some country with which it does not have an extradition treaty. Another drawback which India faces as a result of the same is that, other countries are not obligated to forward any information obtained within the framework of its own investigations, when it considers that the disclosure of such information might assist India in initiating or carrying out investigations or proceedings concerning criminal offences in virtual space.[44] The existing procedural law which primary deals with real world crimes, thus, needs to undergo a massive change in its content if it has to accommodate the nuances of cybercrime investigations. Even though crimes like child pornography affect the body and mind of a human being, the fact that the wrong has been committed over a virtual medium through internet is what creates all the difference. The investigation procedures used to solve other crimes concerning bodily injury will fail to solve an issue of child pornography, especially because of the anonymity of the perpetrator of the crime and also at times, lack of identification of the victim.

A proper definition would have solved the problems of the investigative agencies to a certain extent, since they could easily cross-check whether the content of the images or the evidence, meet the statutory definition of 'child pornography'. Since the definition is lacking, the discretion is left in the hands of the regulatory authorities and the judges of each case dealing with the following issue. Further, the evidences collected and submitted will also be in accordance with their understanding of what constitutes porn. Since search and seizure also forms an integral part of the investigation process in cybercrime like child pornography, a standard procedure is also required to be followed. However, the provisions of the Code which deal with search and seizure have been particularly made applicable to cybercrimes also. The

[43]Government of India, *Countries with which India has Extradition Treaties/Arrangements, MINISTRY* OF EXTERNAL AFFAIRS, (May 11, 2017), http://www.mea.gov.in/leta.htm (last visited on Feb. 20, 2018)

[44]Convention on Cyber Crime, art. 26, *opened for signature* November 23, 2001, ETS No. 185, https://rm.coe.int/1680081561 (last visited on Mar. 10, 2018).

important question is regarding the relevance and applicability of these provisions with regard to the unique features of the crime of child pornography. It is doubtful that a normal search warrant might be of any help in this case considering the fact that it will be difficult to specify the scope of data or material that need to be searched.

With the enactment of the said Act, the Indian Evidence Act, 1872 was also amended to include the concept of electronic evidence to aid in the process of cyber investigation.[45] However, such evidence can only be admissible when accompanied by a certificate provided by the person, who actually occupies a responsible position in relation to the operation or management of the device or relevant activities, which are to be taken as evidence.[46]As per the decision of the Apex Court in *Anvar P.V. v. P.K.Basheer*[47], an electronic record shall only be admissible as evidence if it complies with the requisites of the sections of the Indian Evidence Act, 1872.The examiner of electronic evidence also provides expert opinion on such electronic evidence, to ensure its credibility,[48] when presented before a Court of law. The issue which repeatedly crops up is that the credibility of the electronic evidence is subject to the opinion of the examiner, and in the absence of a fixed definition as to what actually constitutes 'pornography', the sexually explicit content which has to be admitted as evidence, is entirely defined by the perception of the examiner. He uses his own understanding and identifies whether such material actually is pornographic material involving children or not. Thus, need for a uniform standard to classify pornography arises again.

[45] The Indian Evidence Act, 1872, §§ 65A & 65B.

[46]*Id.*at§ 65B (4)(c).

[47](2014) 10 SCC 473 (India)

[48]The Information Technology Act, 2000, No. 21, Acts of Parliament, 2000, (India),§ 79A.

3. A victim-centred approach towards combating child pornography

Since India is a signatory to the United Nations Convention on the Rights of the Child, 1990, it is under obligation to take appropriate measures in order to prevent the exploitative use of children in pornographic materials.[49] As discussed above, the statutory provision under the Act only provides for punishment for the offence of publishing or transmission of sexually explicit content involving children, but nowhere does it provide for any preventive mechanism which can help in combating the crime. Hence, it is observed that the penal provisions have failed to act as a deterrent to the crime.

One of the major reasons behind it can be the pre-conceived notion that child pornography is a 'victimless crime'. The drafters of the statute seem to be oblivious of the fact that the child who is being depicted in the sexually explicit content is victimised not only during the sexual abuse, but also by the mere knowledge that the pornographic content is being viewed by others, victimises them time and again. Such victimization lasts forever considering the fact that the pornographic content can resurface anytime in the virtual space through the internet.

Further, judicial treatment of those alleged of the offence of child pornography reveals a perception by some Courts, that it is a victimless crime. For instance, in the *Bazee.com* case, where the video of a girl with her boyfriend in sexually explicit conditions was circulated, the Court mainly deliberated upon the question of intermediary liability. However, the questions regarding the protection of the children who were depicted in such sexually explicit content were not raised. Following the obligation provided under the Convention, legal institutions while rendering decisions, should give primary consideration to the best interests of the child[50]. However, in cases concerning child pornography, the

[49]United Nations Convention on the Rights of the Child, art. 34, *opened for signature*Nov. 20,1989, http:// www.ohchr.org/ EN/ Professional Interest/ Pages/CRC.aspx (last visited on Mar. 10,2018).

[50]*Id.* at art. 3.

judiciary seems to have failed to fulfil this obligation. Another pertinent issue that can be deciphered from the aforementioned case is that the video was filmed and uploaded by the boyfriend, who was himself a minor.

This raises another question - does the penal provision, provided under the Act, apply to such cases as well, where a child himself/herself uploads such pornographic content? Should the minor be treated as a "child in conflict with law"?[51] There have been no deliberations upon these questions yet, because most often the investigative agencies are unable to find the person who is directly affected by the offence. This has led to the development of the notion that it is a victimless crime. Involvement of children in such pornographic activities can be traced back to the development of technology and cyberspace itself, which encourages this kind of outrageous behaviour. It is usually the possessors of such sexually explicit content who use it to seduce children by desensitizing them or forcing them to get involved into such activities themselves. Ultimately, it is the child who is the victim, irrespective of whether he/she is the one who uploaded it or not.

Considering the fact that crime committed in a virtual medium has a different dimension altogether, the loss suffered by the victim, i.e. the child who is either depicted in the pornographic content or is lured into publishing such content himself/herself, cannot be completely compensated in monetary ways. There is a need for formulating a special victim compensation scheme, apart from the one provided in the Code under Section 357A, which will cater to the needs of the victims of child pornography and provide for counselling sessions to help the victims recover from distress. It is also pertinent to note that in our criminal law system, considering the heinous nature of the crimes, special provisions for victim compensation has been made for the victims of rape and acid attacks, along with the one provided under the code[52].

[51]Juvenile Justice (Care and Protection of Children) Act, 2015, No.2, Acts of Parliament, 2016 (India),§2(13).

[52] The Code of Criminal Procedure, 1973, No.2, Acts of Parliament, 1974, (India),§357B.

Sexual or physical abuse inflicted on the child can itself have serious long term negative psychological consequences for its victims. However, the degree of psychic trauma is dependent on the way the child victim is treated after disclosure, than at the time of the offence itself. What is therefore required, is minimizing the impact of the investigation and the trauma of testifying. The aforesaid legislation has no provision for witness protection and in such a case, the child who is the victim, may not feel confident enough to divulge the true facts in fear of the perpetrator of the crime, which thereby results in acquittal of the alleged offender. Thus, the drafters of the Act, have failed to consider the gravity of child pornography, where the child is not only sexually abused, but also vulnerable to circulation of such pornographic content in cyberspace. The Act has failed to make any special arrangements for the fine levied under the penal provision, to be provided to the victim. It is for this sole reason that the Parliament enacted the Protection of Children from Sexual Offence Act, 2012 (POCSO Act) to specifically cater to the needs of the victimised children. The POCSO Act, 2012 defines the term sexual harassment to include the act of enticing a child for pornographic purposes[53] and also penalises such act with imprisonment for either of the above acts, for a period of three years and an imposition of fine.[54] Apart from that, it distinctively punishes the act of using a child for pornographic purposes[55] with an imprisonment of either description, for a term not less than seven years or which might extend up to life imprisonment and also with fine.[56] The POCSO Act, 2012 has also incorporated certain provisions for providing optimum protection of children during trials[57] and ensuring proper

[53] The Protection of Children from Sexual Offences Act, 2012, No.32, Acts of Parliament, 2012, (India), §11.

[54]*Id.*at §12; *See* Rajesh Mulchand Jain v. State of Maharashtra, 2016 SCC OnLine Bom 8577(India), *See also* Babu Ram v. State, 2017 SCC OnLine Del 9336 (India).

[55]The Protection of Children from Sexual Offences Act, 2012, No.32, Acts of Parliament, 2012, (India),§13.

[56]*Id.* at §14.

[57]*Id.* at§35, §36 & §37.

legal aid[58] for them. The POCSO Act, 2012 thereby makes an attempt to fill in the lacunae created by the existing provisions in our cyber legislation.

4. Complete ban on child pornography: Analysis and possibility of implementation

With the recent communication of Ministry of Electronics and Information to the Home Ministry, based on the information received from National Centre for Missing and Exploited Children, which states that a large number of illegal imagery related to child pornography has been uploaded from Indian territory[59], the actions taken by the government and the intermediaries to restrict or block sexually explicit content involving children, seems to have failed to a large extent. One of the major reason behind this can be the fact that the special legislation dealing with child pornography in India does not provide for any pre-emptive measures to mitigate the crime. The issue has given rise to a debate on whether pornography should be banned entirely or not and has been voiced out in the *Kamlesh Vaswani* case,[60] which has sought for a complete ban on pornography, by ensuring that no online pornography is visible in India. It has been argued that since the manufacturing and viewing of pornography is the medium of expression of one's sexuality, it must fall within the ambit of right to privacy, provided, it is manufactured and viewed privately by consenting adults and thereby not causing harm to others.[61] While the *Vaswani* petition echoes certain valid concerns regarding the portrayal of women and children in pornography[62], his demand of criminalising the act

[58]*Id.* at §40.

[59]Press Trust of India, *US-based private body helping India curb child porn: Centre to Supreme Court,* July 16, 2017, HINDUSTAN TIMES, http://www.hindustantimes.com/india-news/us-based-private-body-helping-india-curb-child-porn-centre-to-supreme-court/story-4vDZCOFLphtYH62IykRfCI.html (last visited on Oct. 16, 2017)

[60] KamleshVaswani v. Union of India &Ors., (2016) 7 SCC 592 (India).

[61]Chandra &Ramachandran, *supra* note13.

[62]*See* GeethaHariharan, *Our unchained sexual selves: A case for the liberty to enjoy pornography privately*, (2014) 7 NUJS L Rev 89.

of private viewing of pornography cannot be held to be justified. As the issue of privacy dealt with, in this petition is beyond the scope of this paper, it will be pertinent to state that the involvement of children in pornographic content should remain outside the scope of privacy regime. As a result, it can be argued that, there is a need for absolute prohibition of child pornography, as children cannot be made prey to these kinds of excruciating circumstances and a country cannot afford to undertake any sort of experimentation with the lives of children, in the name of liberty and freedom of speech and expression.[63] With the Apex Court recently holding the right to privacy as a fundamental right[64], it is quite obvious that pornography cannot be banned in totality. As for the case of child pornography, the lack of proper enforcement standards and ineffectiveness on the part of the intermediaries to restrict such explicit content makes the possibility of complete ban on child pornography a distant thought.

5. Suggestions and Conclusion

Acting upon the recommendation of the Ajay Kumar Committee[65], the Supreme Court has recently, in an order, directed the intermediaries like Whatsapp, Facebook, Google, Microsoft etc. to take down and remove videos of child pornography from the internet[66]. The attitude of the judiciary shows that, as the current legislation is ineffective in mitigating the crime, the sole responsibility is being placed on the intermediaries to block such pornographic content from being circulated among the common people, through the virtual medium. However, in order to effectively deal with the issue, the aforementioned guidelines dealing with the role of intermediaries needs to be revised without imposing any sort of criminal liability on them, but making provision for the common people or any public-spirited citizen to approach them in case they want to complain about any such

[63]Shreya Singhal v. Union of India, (2015) 5 SCC 1 (India).

[64]*See* Justice K.S. Puttaswamy v. Union of India &Ors., 2017 SCC OnLine SC 762 (India).

[65]*See*In re, Prajwala, SMW (Crl.) No (s).3/2015, 7- 15 (October 23, 2017)

[66]*Id.* at 16.

pornographic content. In the above context, it would be pertinent to note that despite the Apex Court's direction to the Centre to introduce a portal for making complaints by citizens, with regard to issues pertaining to child sexual abuse and child pornography before January 10, 2018[67], the portal has not yet become fully operational[68].Therefore, implementation of the recommendations as suggested by the Committee is necessarily a precursor to any amendment that might be introduced in the near future. The existing legislation should be amended, primarily, by providing a precise and unambiguous definition of child pornography and by incorporating proper investigation procedures pertaining to crimes committed in cyberspace. The object of such an amendment should be to take strict preventive measures to avert access to child pornographic content and also strengthen protective measures to support the victims of the crime. An Act to combat the problem of child pornography should follow both a pre-emptive and reactive approach. Apart from this, in order to follow a victim-centred approach, the legislation should also provide certain facilities like witness protection to the child who has been victimised, so that he/she shall feel comfortable in divulging details about the perpetrator of the crime. A victim-centred approach thereby requires filling the human resource gaps wherever required, sensitizing police investigation units towards crimes against children, training of investigation officers, especially women holding such posts, and establishment of separate courts for children, with Special Judges and Special Public Prosecutors who do not have additional responsibilities.

The law may provide justice to these victims in the Court of law, but if they are not provided with proper care and treatment in their homes by their parents or guardians, injustice will continue to prevail.[69] In order to protect children from any sort of abuse, it is

[67]*See* In re, Prajwala, SMW (Crl.) No (s).3/2015, (December 11, 2017).

[68]*See*In re, Prajwala. SMW (Crl.) No (s).3/2015, (January 08, 2018); *See also*Vijaita Singh, *Centre to launch portal to redress online abuse, fraud,* THE HINDU (January 08, 2018), http:// www.thehindu.com/ news/ national/ centre-to-launch-portal-to-redress-online-abuse-fraud/article22398484.ece (last visited Feb. 28, 2018).

[69] *See* Bachpan Bachao Andolan v. Union of India, (2011) 5 SCC 1 (India).

important to make them aware of the crime and its consequences, so that they can refrain from participating in any such activity and also understand the gravity of the crime. Therefore, just enacting a beneficial legislation cannot solve this pertinent problem, unless there is social acceptance of the child-victim and promotion of the true spirit behind the enactment.