11

CYBER LAW

*Deepa Kharb**

I INTRODUCTION

CYBER LAW is a fast developing area that cuts across the traditional legal disciplines. The scenario of cyber law litigation is undergoing a transformation since 2014. The survey presents a critical analysis of judicial pronouncements delivered by the apex court and high courts in the year 2017 that have either laid down new principles or propounded debatable prepositions in order to elucidate the scope and extent of cyber law.

II INTERMEDIARY LIABILITY

The concept of intermediary liability, governing the responsibility of online platforms in respect of user/third party generated/posted content has been a subject matter of litigation for past few years. The legal infrastructure available under the Information Technology Act, 2000 (the Act hereinafter) has created safe harbour protections into the intermediary liability, which is not available to traditional publishing or broadcasting media, allowing the internet businesses to grow at an astonishing rate. The first version of section 79 of the Act gave immunity to the intermediary as long as they had no knowledge of illegality of third party content uploaded on its platform or exercised due diligence.

The 2004 MMS scandal followed by the arrest of Baazee.com CEO highlighted the deficiencies of the Act and led to the setting up of a committee to recommend appropriate amendments to the Act, especially with regards to the liability of an intermediary. The committee recommended that intermediaries be offered immunity under section79 of the Act in respect of any content uploaded/posted by their users unless there was sufficient evidence to prove 'abetment' or 'conspiracy' on the part of intermediaries or if they had received actual knowledge or a government notification about illegal content.

* Assistant Professor, The Indian Law Institute, New Delhi.

However, in the final report, the requirement of complying with the due diligence standards prescribed by the government from time to time was again added along with a notice and take down mechanism. The intermediary was also required to place a privacy policy and user agreements before allowing anyone to use its platform to disseminate information to get immunity from liability. All this was done without actually defining the word 'due diligence', leading to further confusion. The clarification came with the Information Technology (Intermediary Guidelines) Rules in 2011 only.

The intermediaries were put under an obligation by central government to take down unlawful content hosted/ uploaded within 36 hours of receiving 'actual knowledge'. In *Shreya Singhal,*[1] however, the court read down "actual knowledge" under section 79(3)(b) to mean receipt of a court order/notification directing intermediaries to remove or disable access to content expeditiously. This provided some respite to the intermediaries, who were caught between the issuer of the notice and their users to whom they were bound by the terms of use of their portals.[2]

In yet another case,[3] the High Court of Delhi held that the intermediaries could be held liable only when they fail to take steps to have an infringing content removed from their website after having actual or specific knowledge, and not mere awareness or constructive knowledge regarding of the content. The court observed that since the intermediaries only serve the purpose of being a conduit/ channel/medium/platform for exchange of information amongst the users, the cannot be expected/ equipped or obligated to pre-screen and verify all such information/content that is stored in their websites.[4]

The High Court of Delhi in *Kent RO Systems Ltd.* v. *Amit Kotak*[5] reiterated the position that the intermediaries are not required to make a self-determination of copyright/design infringement by third party products sold on its website and is only required to take down the same only on receipt of complaint. Certain product listings of water purifier systems hosted on *eBay.in* were alleged by Kent RO Systems Ltd. to infringe its registered designs under the Designs Act, 2000. It sought for a direction from the High Court of Delhi to takedown, remove and delist all products infringing their registered designs and an injunction restraining the offering for sale of the infringing goods on eBay platform along with accounts of profit.

1 *Shreya Singhal* v. *Union of India,* (2015) 5 SCC 1.

2 J. Sai Deepak, The Shreya Singhal Judgement and Intermediary Liability: What is the Correct Legal Position?, *available at*: http://thedemandingmistress.blogspot.com/2017/04/the-shreya-singhal-judgement-and.html (last visited on December 29,2018).

3 *MySpace Inc*. v. *Super Cassettes Industries Ltd*., 2016 SCC OnLine Del 6382.

4 Intermediaries under the Indian Information Technology Law can Breathe a Sigh of Relief, *available at:* http://www.nishithdesai.com/information/research-and-articles/nda-hotline/nda-hotline-single-view/article/intermediaries-under-the-indian-information-technology-law-can-breathe-a-sigh-of-relief.html?no_cache=1&cHash=80da7b50ba841f87de069feda3ba6697 (last visited on December 29,2018).

5 2017 SCC OnLine Del 7201.

The plaintiff contended that eBay is under an obligation as per section 79(3) read with Rule 3(4)[6] as an intermediary to remove listings that infringe the intellectual property rights upon receiving a complaint/notice. Not only this, but the plaintiff further contended that the defendant should, before hosting a product from any other seller, verify whether the same also infringes the registered design of the plaintiff. Therefore, they need to devise an in-house mechanism wherein it should verify all other products also before hosting.

The contention of the plaintiff was that the liability of the intermediary was not limited just to an effective response to the complaint pertaining to infringing material but required a proactive approach, continuously verifying all subsequent articles displayed for selling by the same sellers.

According to Kent RO Systems, eBay:

- had an obligation under section 79(3) of the Act read with Rule 3(4) of the IT Rules 2011 to remove listings that infringe its intellectual property rights upon receipt of complaint from the plaintiff as well to devise a mechanism to protect further posting of any listing that may infringe its registered designs;
- should not be allowed to claim safe harbour protection under section 79 of the Act for abetting and aiding in the commission/conspiracy of alleged infringement for its omission to remove new listings that may infringe plaintiff's registered design;
- is liable for piracy under section 22 of Designs Act, 2000 for continued hosting of infringing articles amounting to intentionally publishing/causing to be published imitations of designs protected under section 22 of the Designs Act of 2000 in spite of receiving complaint in this regard from the plaintiff.

eBay countered the arguments of the plaintiff contending that so long as it had complied with all of its obligations under section 79 of the Act as well as Rules thereunder as an intermediary, it would not be /cannot be held liable for any information, data or communication posted on its website as it was merely providing access to such information/data/communication and was not involved in any selection, modification or transmission.

It also informed the court that it had already removed all such content from its platform alleged by plaintiff to be infringing its right in the registered design on complaint received from the plaintiff and assured the same practice in future as well, in response to any further complaint received. Relying upon division bench decision in *MySpace* case[7] that section 79(3) of the Act posit upon the intermediary an obligation to remove such information or disable access to such link on receiving a written complaint/mail/notice from the affected person within 36 hours, failing which the intermediary will be denied safe harbour immunity.

6 Rule 3(4) of Information Technology(Intermediary Guidelines) Rules 2011.

7 *MySpace Inc.* v. *Super Cassettes Industries Ltd.*, *supra* note 3.

The plaintiff contended that the safe harbour exemption under section 79(3) does not apply if the intermediary has either failed to expeditiously remove or disable access to the infringing material or information or has conspired, abetted or aided/ induced commission of unlawful act. Referring to para 64 of *My Space* judgment,[8] where draft report of the OECD[9] suggesting adoption of filtering tools to identify subscribers uploading infringing content as suggested by the Irish high court in *EMI* v. *UPC,*[10] was mentioned before the court. Though the observance of due diligence by the defendant was not denied by the plaintiff, it argued that defendant in allowing infringing products to be sold from newly appearing URLs would be abetting and aiding infringement within the meaning of section 79(3) of the Act.

The single judge refused to go by the interpretation suggested by the plaintiff as according to him the plaintiff were required to plead and prove 'conspired', 'abetted', 'aiding' and 'inducing', legal terms, meaning of which has been settled for long. Neither the legislature intended to vest *suo moto* powers with the intermediary to detect and refuse the hosting of infringing content nor they are possessed with the prowess to judge whether infringement has occurred or not, a technical question which even the courts struggle to decide. Therefore, the single judge refused to accept that in the *My Space* judgment,[11] the division bench anywhere held that the intermediaries are required to conduct such self-determination or provide filtering. Also to require an intermediary to do such a screening would amount to an unreasonable interference with its right to carry on its business.

The legislature has deliberately set a low due diligence standard to be met by the intermediaries which was further diluted by the Supreme Court in *Shreya Singhal*[12] judgment. Therefore, it was not open for the single judge to read in an obligation on the intermediaries to censor content on *a suo moto* basis putting the safe harbour provision in case of IP infringement on a more secure legal footing. However, separate legal obligations were created for intermediaries by the Supreme Court in *Sabu Mathew George,*[13] an auto block obligation, to screen and block content in a case involving advertisement for pre-natal sex determination diagnostic techniques and tools in the light of increasing incidents of female foeticide.

On November 16, 2016 in the case of *Sabu Mathew George* v. *Union of India*[14] the apex court discussed the issue of internet intermediary liability in two situations: one; for causing advertisements, and two; for causing organic searches, on pre-natal

8 *Ibid*.

9 OECD Draft Report "The Role of Intermediaries in Advancing Public Policy Objective" dated 29th September 2010.

10 [2009 no. 5472 P].

11 *My Space Inc*. v. *Super Cassettes Industries Ltd*. *Supra* note 3.

12 *Shreya Singhal* v. *Union of India,* (2015) 5 SCC 1. *Supra* note 1.

13 *Sabu Mathew George* v. *Union of India,* (2017)2 SCC 521.

14 2016 SCC OnLine SC 681.

determination or pre-conception selection of sex (PNDPS) to be displayed on their platforms and passed an order worth mentioning here.

The publishing, distributing or communicating, or causing to be published, distributing or communicating advertisements on pre-natal sex determination is a punishable offence in India as per section 22 of the Pre-conception and Pre-natal Diagnostic Techniques (Prohibition of Sex Selection) Act, 1994 (PCPNDT Act). The petitioner, an activist, submitted that despite the legal prohibition, the respondents, namely, Google India, Yahoo India and Microsoft Corporation (I) Pvt. Ltd., display advertisements for the sale of sex determination kits online in violation of the legal provision contained in the PCPNDT Act, 1994. A writ was filed by the practitioner, a doctor, in 2008 expressing his concern about the modus operandi adopted by the respondents entertaining advertisements, either directly or indirectly, in violation of section 22 of the PCPNDT Act, in detriment to the balancing of sex ratio in India.

The Court took serious concern and the following order was passed against the three software companies: [15]

> Explaining the same, it is submitted by the learned Solicitor General that all the three companies are bound to develop a technique so that the moment any advertisement or search is introduced into the system, that will not be projected or seen by adopting the method of 'auto-block'. To clarify, if any person tries to avail the corridors of these companies, this devise can be adopted so that no one can enter/see the said advertisement or message or anything that is prohibited under the PCPNDT Act, 1994, specifically under section 22 of the said Act.[16]

In this order, the apex court held that intermediaries are responsible for the content that is displayed on their platforms. While it was contended by respondent-companies that access to information of any nature, unless it is not advertisement, which is prohibited under section 22 of the 1994 Act, would come within the freedom of access to have information, the bench took reference from affidavit filed by Union of India which read:[17]

> Section 22 and the explanation appended to it are very wide and does not confine only to commercial advertisements. The intention of law is to prevent any message/communication which results in determination/selection of sex by any means what so ever scientific or otherwise. The different ways in which the communication/messages are given by the internet/search engine which promote or tend to promote sex selection are prohibited under section 22.

15 *Id.*, order passed on 16-11-2016.

16 *Ibid.*

17 *Sabu Mathew George* v. *Union of India,* 2016 SCC OnLine SC 681 para 6.

The apex court held that although it can't be doubted that there has to be freedom of access to information, however, such freedom cannot violate a law of the land.

Taking note of the innovative approaches/techniques adopted on internet to send across information and advertisements pertaining to gender test, gender test in pregnancy, gender test kit in India etc, the court categorically held that intermediaries were responsible to take down such content under section 22 of the PCPNDT Act. The whole objective of PCPNDT Act according to the two judges stands defeated by adopting a restrictive construction of the term 'advertisements' in the abovementioned provision.

This order was criticised for failing to distinguish advertisements from organic searches and for recommending the development and application of filtering tools/ technology by the search engines to 'auto block' the content that infringes the PCPNDT Act. This doctrine of auto block was a clear deviation from the precedent laid down in *Shreya Singhal*[18] wherein the apex court widened the scope of safe harbour provision for intermediaries under section 79 of the Act by requiring taking down of the content only after it is confirmed by judicial or executive order.[19] In its April 2017 order, the three judges bench adopted a two prong approach in respect of advertisements it maintained the auto block mechanism and directed the respondents to establish an 'in-house expert body' to take down content punishable under section 22. For general content available online on PNDPS it refrained from giving a similar ruling as the internet user has right to access information, knowledge as essential part of freedom of expression, a constitutionally protected right. The nodal agency in the government on receiving complaint is required to intimate the intermediary who shall take down the infringing content from its website.

III BLOCKING OF WEBSITES

The constitutional validity of section 69A of the Act which deals with blocking of the contents of a website was challenged in *Shreya Singhal*[20] wherein the apex court, upholding the validity of the provision, gave three guidelines to restrict the misuse of this section: the government is satisfied that it is necessary to do so; only in cases set out in article 19(2) and; the reasons for the same are recorded in writing. However, these options to restrict the contents of a website may be used in genuine cases in the incidents of propagating hate speech, communal disharmony as well as areas of potential threat to society.

In *Sneha Kalita* v. *Union of India*[21] a writ petition was filed to sought directions to intermediaries[22] to observe due diligence by not hosting/taking down the links to

18 *Supra* note 1.

19 *Ibid.*

20 *Id.* at para 114.

21 2017 SCC OnLine SC 1471(decided on November 20, 2017).

22 Intermediaries including the NSPs, ISP, Web Hosting Service Providers, Cyber Cafe etc.

the Blue Whale game as well as to Government to take immediate measures to ban/ block all sites (section 69A) linked with the abovementioned online game or any other form of violent or immoral games similar in nature.

The game, termed as the 'suicide game' led to an abetment to suicide whereby the creators seek out their players who were in depression and send them an invitation to join. Then an anonymous group administrator, 'the curator,' would hand out 50 self harming tasks to the 'selected players' required to be completed, documented and posted during a 50-day period and ultimately brainwashing them to commit suicide. This game was reportedly responsible for several teenage suicides not only in India but in some other countries too.

The bench headed by Chief Justice in one of the orders directed the government to constitute an experts committee and take various other steps to spread awareness in this regard through telecast of educative messages/clips on Doordarshan prepared in consultation with Ministry of Child Welfare and MHRD. The apex court was appraised of the steps taken by the government in this regard like setting up of an expert committee, the CERT-In and how it was engaged in stopping the aforesaid games, so that unwarranted incidents do not occur.

With regard to section 69A of the Information Technology Act, 2000, which empowers MeitY to issue directions for blocking of public access to any information through any computer resource in the interest of sovereignty and integrity of India, defence of India, security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offence relating to above, it was put forth that in the absence of any downloadable applications of the game, there was very little scope for using technical solutions to identify or block the game. Further, the children were sharing Blue Whale Challenge Game among secretive groups on social media networks like WhatsApp and Facebook.

The three judges' bench emphasised on creating awareness in the society about the dangers of the game and sanctity of life. It issued directions to the Chief Secretaries of the States and Union Territories through their concerned departments to spread awareness in the schools run by the State, about the danger such games propagate by bringing people into a trap. The Supreme Court stated that the children must grow up with awareness that such a thing exists and they shall scrupulously avoid it. The awareness campaign need not be about the game, but about the dignity of life and not to waste it and not to fall in anyone's trap.

The Court also expected the parents, the children, the educators and, eventually, the State shall live up to their respective roles. Sometimes legal measures alone are not sufficient to counter a problem like this and the parents as well as the teachers can ensure that the children of young age do not get into the traps of such things. It is in solitude that children watch/play such games. Therefore, a need for the parental care, concern, love, affection and instilling sense of optimism in children was highlighted before the Court which can keep them away from even searching for these kinds of games.

After all the beauty of life is not to have a meeting with death, but to keep death away and that makes the mind victorious. Nothing is worth ruining oneself.[23]

In yet another case, the Supreme Court was summoned asking for directions to the Government for blocking of websites/access to information on websites that are harmful, harassing, defamatory, invasive of privacy, threatens the unity of India or threatens public health or safety under section 69A of the Act.

In 2015, the apex court received a letter from NGO-Prajwala to bring attention to the existence as well as rampant circulation of videos of sexual violence depicting rape, gang rape and child pornography over internet. Taking cognizance *suo moto* on the contents of letter, the court passed an order[24] constituting a committee to examine technological solutions (like auto blocking) to the problem impleading Google, Facebook, WhatsApp, Yahoo and Microsoft as parties. The committee was to assist and advise the court on the feasibility of ensuring that such videos are not available for circulation in order to protect the identity and reputation of victims. Further, circulation of such content is not in public interest at all.

A comprehensive report was submitted by the committee after extensive deliberations and discussions which consisted of some proposals and suggestions[25] some of which were:

- search engines expand the list of keywords (in Indian and vernacular languages also) which may be used by user to search CP content[26] including RGR[27];
- Creating an administrative mechanism, Central Reporting Mechanism (Indian Hotline Portal) for reporting and maintenance of data in India;
- Need to strengthen law enforcement in this area-Online Portal proposed to provide for anonymous reporting of identified CP/RGR; GoI to identify and authorize specific authority/entity for receiving Complaints of CP/RGR online and for initiating action thereon within specified timelines; Such authority to have immunity and permission to verify CP/RGR content and to initiate take downs; Government of India team/authority to also immediately send communications to concerned police stations for registration of FIR and initiation of prosecutions;
- Creation of infrastructure/Training/Awareness building- Internet companies should provide technical support and assist in capacity building to the relevant agencies in India including law enforcement and NGOs through a series of

23 *Supra* note 21 at 679 para 14.

24 Order passed on 22nd March, 2017.

25 Part I of Chapter 7 contains proposals on which the committee was able to arrive at consensus whereas Part II contains proposals over which there was no consensus.

26 Child Pornography (CP) Content.

27 Rape/Gang Rape (RGR) Content.

trainings on online crime investigations, and trainings on using relevant Internet tools;

- Developing "proactive detection" technology for real time screening through artificial intelligence for identifying rogue sites that contains CP and RGR content and blocking these sites.

The Supreme Court directed that guidelines, standard operating procedures, as well as technology for auto-deletion of content be put in place to deal with videos, imagery, sites and other similar content in relation to child pornography, rape and gang rape. A bench of Justice Madan B Lokur and Justice UU Lalit made this observation during an in-camera proceeding held in the matter of *Re Prajwala Letter*.[28] These recommendations to some extent go against previous Supreme Court orders — those given in the *Shreya Singhal*[29] case. There are voices being raised against the censorship and monitoring enabled, and a few voices in support of it. Those supporting cite recent events such as fake news and related mob violence and lynching, and the circulation of rape videos as justification.

However, while imposing greater responsibility on the intermediaries, it is essential that these do not interfere with the people's right to freedom of speech, and that the intermediaries are not put in a position to self-censor or police content. According to the directions issued by the Supreme Court in *Shreya Singhal*[30] case an intermediary should not be required to apply its own mind in judging the lawfulness of content. Further, laws declaring vague and broad categories of content as unlawful violate the fundamental right to freedom of speech.

The proposed requirement under the law, for an intermediary to deploy automated tools and other mechanisms to 'proactively' identify, remove and disable access to unlawful information or content, then the intermediary is required to use tools for content that is harmful, harassing, defamatory, invasive of privacy, threatens the unity of India, threatens public health or safety, and so on.

This requirement violates both the requirements of the *Shreya Singhal* judgment[31] - it requires an intermediary to apply its own mind, in relation to the countless pieces of content it hosts, for identifying and removing a vague category of information — 'unlawful content' even waiving the judicial order requirement for the removal of this specific form of content. In the present case the Supreme Court did require the use of automated tools, but to deal with specific forms of content only, namely, child pornography, rape videos and gang rape videos. A limited provision of that nature, requiring an intermediary to deploy automated tools for specific forms of content, and not all unlawful content, would allow dealing with the issue as a reasonable restriction, without violating people's right to freedom of speech.

28 MANU/SCOR/45933/2017 date of order: October 23, 2017.

29 *Supra* note 1.

30 *Ibid.*

31 *Ibid.*

An alternative could be amendment of section 67B under the Information Technology Act, an extremely strict provision in relation to the creation, consumption, publication, etc., of child pornography, to include rape and gang rape videos as well. This will ensure that all persons, and not just intermediaries, are subject to equally strict obligations in relation to such content.

Section 69A comes with certain safeguards, but it is unclear if the scope of censorship under section 79(3)(b) (the provision that requires an intermediary to remove unlawful content on receiving a governmental direction to do so) is limited to section 69A, or extends beyond it. If it does extend beyond it, then this power of censorship also lacks the procedural safeguards that are necessary for restricting the right to freedom of speech, as is required under the *Shreya Singhal* judgment.[32]

IV SECTION 65 B-ADMISSIBILITY OF ELECTRONIC EVIDENCE

The jurisprudence over admissibility of electronic evidence has reverted to uncertainty once again. After overruling *Navjot Sandhu,*[33] the three-judge bench of the Supreme Court in *Anwar PV*[34] tried to settle the law and brought back the relevance of section 65B of the Indian Evidence Act (IEA hereinafter), restoring the requirement of a certificate to establish the admissibility of a secondary electronic record. This position has been unsettled once again in the recent judgment of the Court in *Sonu*[35] where a two judge-bench refused to be completely bound by *Anwar* holding that non-compliance of said provision cannot be brought up in appellate stage. The judgment appears to have unsettled the law on admissibility of electronic records under section 65B of the Indian Evidence Act as it has reduced the mandate of certificate to a mere procedural requirement which can be derogated if not objected to in the court of first instance.

The 65B provision was introduced in the IEA with a view to facilitate for the admissibility of secondary evidence with a view to facilitate admissibility of secondary evidence in electronic record, where it was difficult to produce primary evidence pertaining to it. It ensures safeguard against tempering and manipulation by attaching authenticity and genuineness with it. The provision mandates submitting of a certificate signed by a person occupying a responsible position in relation to the device, stating the manner of production of the electronic records and the particulars of the device used in producing the record.

The law laid down in the *Navjot*[36] judgment in 2005 had effectively diluted section 65B, causing much ambiguity, when it was held that secondary evidence may be

32 *Ibid.*

33 *State (NCT of Delhi)* v. *Navjot Sandhu, (*2005)11 SCC 600.

34 *Anwar P.V.* v. *Basheer,* (2014) 10 SCC 473.

35 *Sonu* v. *State of Haryana,* (2017) 8 SCC 570.

36 *Supra* note 33.

filed under sections 63 and 65, and that the absence of certificate under section 65B (4) does not render such evidences inadmissible..

However, the three judge bench of the Supreme Court in *Anwar P.V.* case[37] settled the law on the admissibility of electronic evidence in 2014 after a series of conflicting judgments given by various high courts and the trial courts. Placing reliance on the *non obstante* clause in section 65B of the Indian Evidence Act, 1872 (Evidence Act) the Court held that special provision under section 65A and 65B will prevail over the general law on secondary evidence under sections 63 and 65 of the Evidence Act. Therefore, for an electronic record to be admissible as secondary evidence in the absence of the primary, the mandatory requirement of section 65B certification is required to be complied with. This judgment brought section 65 B back to relevancy, thereby bringing some clarity to the nine year long jurisprudential conundrum revolving around it.

However, recently, in *Sonu* v. *State of Haryana,*[38] a two judge bench of the Supreme Court has held that a CDRs (Call Detail Records), without any section 65-B certification, could be relied upon to support the conviction. Though the judges have shown concern regarding the application of principle laid down in the *Anvar* case to pending appeals, they have also acknowledged the fact that the three judges in the *Anvar* case have nowhere expressly said that the ruling would apply prospectively only. Despite knowing their limitations in that regard, the judges in *Sonu*[39] in fact went a step ahead to recommend that a proper bench ought to consider this in the future and proceeded to dismiss the appeals by refusing to apply the law in *Anvar.*

This was a case of abduction and murder where the crucial convicting factor of one of the accused was the CDRs of his mobile phone. The CDRs were produced by the telecom companies but without the mandatory 65B certificate. The appellant's counsel, referring to the judgment of this Court in *Anvar,* argued that the CDRs are not admissible under section 65B of the Indian Evidence Act, 1872 as they were not certified in accordance with sub-section (4) thereof. Quoting *Anwar*[40] as under:

> The evidence relating to electronic record, as noted hereinbefore, being a special provision, the general law on secondary evidence under section 63 read with section 65 of the Evidence Act shall yield to the same. *Generalia specialibus non derogant*, special law will always prevail over the general law. It appears, the court omitted to take note of sections 59 and 65-A dealing with the admissibility of electronic record. Sections 63 and 65 have no application in the case of secondary evidence by way of electronic record; the same is wholly governed by sections 65-

37 *Supra* note 34.
38 *Supra* note 35.
39 *Ibid.*
40 *Supra* note 34.

> A and 65-B. To that extent, the statement of law on admissibility of secondary evidence pertaining to electronic record, as stated by this Court in *Navjot Sandhu*, does not lay down the correct legal position. It requires to be overruled and we do so. An electronic record by way of secondary evidence shall not be admitted in evidence unless the requirements under section 65-B are satisfied. Thus, in the case of CD, VCD, chip, etc., the same shall be accompanied by the certificate in terms of section 65-B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible.[41]

The State however, opposed the contention stating that objections as to admissibility of an electronic evidence could have been raised before the trial court only when the CDRs were adduced as evidence. Referring to its ruling in *Padman*[42] and *Gopal Das* v. *Sri Thakurji,*[43] that objections, when relate to inherent inadmissibility, should be allowed even at the appellate stage and not when they relate to method/ mode of proof of evidence or that the mode of proof put forward is irregular or insufficient as in the present case. The issue of objection to inherent inadmissibility of a document being a fundamental issue can be allowed even at the later stage where the opposite party failed to raise flag at trial stage.

The issue which required consideration in the present case was regarding allowing of an objection to the admissibility at appellant stage, a question that has been raised for the first time before the Supreme Court.

The bench placed great reliance its judgment in *R.V.E. Venkatachala Gounder* v. *Arulmigu Viswesaraswa*[44] to take observation that the admissibility of the electronic evidence could not be challenged at the appellant stage in every case. If there were any discrepancies, it should have been raised before the trial court itself when the evidence was submitted. Where the defect was curable at the stage of marking the document by giving the prosecution an opportunity to rectify the deficiency, it's merely a procedural irregularity. However, when the documents are *per se* inadmissible, it is a fundamental issue and objections pertaining to it can be taken even at the appellate stage.[45]

When the objections to the mode of proof are permitted to be taken up at the appellate stage by a party, the other side is denied the opportunity of rectifying the deficiencies.

The court though adhered to the *Anwar* mandate of complying with the mandatory requirement of section 65B but at the same time refused to be completely bound by it,

41 *Ibid.*

42 *Padman* v. *Hanwanta*, AIR 1915 PC 1.

43 AIR 1943 PC 83.

44 (2003) 8 SCC 752.

45 *Ibid.*

holding that non compliance cannot be brought up at the appellant stage. Differentiating between substantial and procedural acceptance, it held that in a criminal trial, if a piece of evidence was not contested when it was first submitted, it could not be disputed at the appellant stage.

The two judge bench also expounded on the doctrine of prospective ruling, borrowed from American jurisprudence, to hold that it was not prudent to apply the judgment in this case retrospectively as it would lead to reopening of old /already decided. Further, this issue was left undecided by *Anwar*, a case decided by a bigger bench.

The bench expressed concerns regarding the application of *Anvar* to pending cases as being unfair, thereby adversely affecting the administration of justice, but left the question open to be decided by an appropriate bench.

The judgment does not condone non submission of certificate nor reverses the Anwar mandate and at the same time, for practical reasons, applies it prospectively. However, the binding value of *Anwar* on future cases has become uncertain and it remains to be seen if the Supreme Court's decision will be used to reopen or challenge admissibility of evidence in pending trials where the requirement under section 65B were not complied with. Also it will be worthy to see the impact of this judgment on the ongoing trials and proceedings. Unsettled position of law can lead to grave miscarriage of justice.

A positive development on the issue is that in view of these observations made by two judges, an application in *Anwar P.V.* v. *Basheer*[46] was placed before Chief Justice of India for posting the matter before an appropriate bench.

Section 65B applicable to secondary evidence and not primary

The Madurai bench of High Court of Madras in *Karuppasamy* v. *State of Tamil Nadu*[47] in a review petition in a matter under section 498A IPC observed that primary evidence of an electronic record under section 62 of IEA would be admissible in evidence, without compliance with the condition in section 65B of the Act. Justice A.M Basheer Ahmed observed:[48]

> Admissibility of the secondary evidence of electronic record depends upon the satisfaction of the conditions as enumerated under section 65-B of the Evidence Act. On the other hand, if primary evidence of electronic record adduced that is the original record itself is produced in Court under section 62, the same is admissible in evidence without compliance with the conditions in section 65(b).[49]

46 MA.1563/2017 (IN C.A. NO. 4226/2012) dated December 11, 2017.

47 MANU/TN/1577/2017.

48 *Id.* at para 7.

49 *Ibid.*

In *Md. Rashid* v. *State,*[50] a criminal appeal was filed by the accused against the trial court order on the sentence holding the appellant guilty for the offence punishable under section 302 IPC and punished to undergo imprisonment for life. The appellant contended that his presence at the hotel where the girl was found murdered was not established as the electronic evidence in this case, the CCTV footage of the hotel, was submitted without section 65B certificate and therefore, not admissible in evidence.

The Delhi high court observed that the mandate of certificate under section 65B is limited to secondary evidence by way of electronic record and not primary evidence, an issue already settled by the decision of the Supreme Court in *Anwar P.V.* v. *Basheer:*[51]

> The situation would have been different had the appellant adduced primary evidence, by making available in evidence, the CDs used for announcement and songs. Had those CDs used for objectionable songs or announcements been duly got seized through the police or Election Commission and had the same been used as primary evidence, the High Court could have played the same in court to see whether the allegations were true. That is not the situation in this case. The speeches, songs and announcements were recorded using other instruments and by feeding them into a computer, CDs were made there from which were produced in court, without due certification. Those CDs cannot be admitted in evidence since the mandatory requirements of section 65-B of the Evidence Act are not satisfied. It is clarified that notwithstanding what we have stated herein in the preceding paragraphs on the secondary evidence of electronic record with reference to sections 59, 65-A and 65-B of the Evidence Act, if an electronic record as such is used as primary evidence under section 62 of the Evidence Act, the same is admissible in evidence, without compliance with the conditions in section 65-B of the Evidence Act.[52]

The Court relied upon its ruling in *Kishan Tripathi*[53] where it took reference from *Anwar,* to hold that CCTV footage stored directly in the hard disk/drive of a computer being self-generated without human intervention, is not secondary evidence requiring certification under section 65B.[54] It further observed that CCTV footage is captured by the cameras and can be stored in the computer where files are created with serial numbers, date, time and identification marks. These identification marks/ details are self generated and recorded, as a result of pre-existing software commands.

50 2017 SCC OnLine Del 8629, decided on May 3, 2017.

51 *Supra* note 34 at para 24.

52 *Ibid.*

53 *Kishan Tripathi @ Kishan Painter* v. *The State,* 2016 SCC OnLine Del 1136 .

54 *Ibid.*

The capture of visual images on the hard disc is automatic in the sense that the video images get stored and recorded *suo-moto* when the CCTV camera is on and is properly connected with the hard disc installed in the computer. It is apparent in the present case from the evidences led that no one was watching the CCTV footage when it was being stored and recorded. The recording was a result of commands or instructions, which had already been given and programmed into the computer. The original hard disc, therefore, could be considered the primary and direct evidence. Such primary or direct evidence would enjoy a unique position as anyone who watches the said evidence would be directly viewing the primary evidence. Section 60 of the Evidence Act states that oral evidence must be direct, i.e., with reference to the fact which can be seen, it must be the evidence of the witness, who had seen it, with reference to the fact, which could be heard, it must be evidence of the witness, who had heard it and if it relates to the fact, which could be perceived by any other sense or any other manner, then it must be the evidence of the witness, who says who had perceived it by that sense or by that manner. Read in this light, when we see the CCTV footage, we are in the same position as that of a witness, who had seen the occurrence, though crime had not occurred at that time when the recording was played, but earlier.[55]

Therefore, the hard disk being primary evidence was held admissible *per se* under section 62 of the Evidence Act. Since the authenticity and genuineness can be challenged by the other party, therefore, the hard disk must pass the integrity test to rule out any possibility of manipulation, fabrication or tempering, the court held.

Evidentiary Value of Electronic Evidence

Bombay high court passed a landmark judgment on appreciation of electronic evidence in a case involving dishonour of cheque. One of the issues in *Jaimin Jewelery Exports Pvt. Ltd.* v. *State of Maharashtra*[56] was whether the complainant had proved that the cheques were issued by the accused towards legally enforceable debt/liability. The complainant company had relied upon statement of account, a print out of the electronic records maintained by the complainant company in the course of business in Exh. 'FF'.

The admissibility of the said statement was challenged by the accused on the grounds that:

i. CW2[57] was not the author of the statement and had no knowledge about the entries made in the said statement;
ii. CW3,[58] who had issued 65B certificate was not competent to issue such certificate;

55 *Ibid.*

56 2017(3) Mah.L.J. 691 (decided on March 14,2017).

57 CW2 Mr. Mahesh Malunjkar, Senior Officer, Legal.

58 CW3 Mr.Santosh Sawant, Senior Manager, Client Relationship and IT.

iii. The said certificate did not contain the details required under section 65B(4) clauses (a) to (c) of Indian Evidence Act.

Though the question of competence of CW3 to issue certificate under section 65B(4) of the Act was not addressed by the sessions judge prior to this court, the Magistrate rejected the contentions and held that section 65B nowhere require that certificate can be issued only by a person having access to the system and CW3 working as IT Head can be assumed to have control and lawful access over the entire computer system of the complainant company.

In the present case, the said statement was not accompanied by a certificate as contemplated under sub-section (4) of section 65B. The Complainant Company tried to rectify this defect by examining CW3 at the stage of final hearing. The certificate was produced by him, however, no reason was assigned by the complainant company for not producing it along with the statement. The court was, therefore, led to infer that the certificate was created subsequently to fill in the lacuna in the evidence of CW2. It was observed by the court that both CW2 & CW3 had no personal knowledge about the transaction and the genuineness of the entries reflected in Exh. FF.

The court held that section 65B only relates to the admissibility of electronic records and authenticates the genuineness of the copy /the printout, dispensing with the need to produce the original. The amended section merely prescribes the mode for proof of contents of electronic records. The certificate does not prove the actual correctness of the contents/entries or absolve from the proof of genuineness of the entries in the electronic record.

Furthermore, there is no presumption regarding the genuineness of the entries in electronic records. Therefore it was necessary for the complainant company to prove the correctness of the entries.

Referring to *Anwar P.V.*[59] both the witnesses examined by the complainant company, CW2 & CW3, did not have any personal knowledge regarding the entries made in the said statement at Exh. FF and were therefore not competent to depose about the correctness of the entries.

V INTERNET PRIVACY

In India, though the right to privacy is not expressly mentioned in the Constitution but through various judgments, the Supreme Court and the high courts have held it to be implicit in right to life and personal liberty guaranteed under article 21[60] and that it is not given but exists.[61] Privacy may have different aspects starting from 'the right to

59 *Supra* note 34.

60 *Kharak Singh* v. *Sate of U.P.,* (1964) 1SCR 332.

61 *K.S. Puttaswamy* v. *Union of India,* (2017) 10 SCC 1 para 575-577 and 582.

be let alone'[62] –in respect of his own as well as in relation his family. One such aspect is an individual's right to control dissemination of his personal information and this aspect has assumed importance in information age in view of the technological advancement.[63]

The apex court recently in its the landmark decision in *Justice K.S. Puttaswamy* v. *Union of India*[64] gave recognition to right to privacy as a fundamental right and went ahead to identify the 'right to be forgotten'- in physical and virtual medium like internet under the umbrella of informational privacy. Justice Sanjay Kishan Kaul recognised that in case of internet the right to privacy would transform into right to be forgotten. In his concurring judgment, he recognised the concerns of surveillance, and profiling in respect of the state actors on one hand and the generation, collection and use of data by non-state actors on the other and felt the need to protect certain information from state as well as non-state actors. The right of an individual to exercise control over his personal data and to be able to control his/her own life would also encompass his right to control his existence on the Internet.[65] He stated: [66]

> The impact of the digital age results in information on the internet being permanent. Humans forget, but the internet does not forget and does not let humans forget. Any endeavour to remove information from the internet does not result in its absolute obliteration. The foot prints remain. It is thus, said that in the digital world preservation is the norm and forgetting a struggle.
>
> Whereas this right to control dissemination of personal information in the physical and virtual space should not amount to a right of total eraser of history, this right, as a part of the larger right of privacy, has to be balanced against other fundamental rights like the freedom of expression, or freedom of media, fundamental to a democratic society.[67]

Therefore, the Court held that all aspects of earlier existence are not to be obliterated, as some may have a social ramification. If a similar right is to be recognised, it would only mean that an individual who is no longer desirous of his personal data to be processed or stored, should be able to remove it from the system where the personal data/ information is no longer necessary, relevant, or is incorrect and serves no legitimate interest. Such a right, however, cannot be exercised where the

62 *R. Rajagopal* v. *State of Tamil Nadu,* (1994) 6 SCC 632; *K.S. Puttaswamy* v. *Union of India supra* note 61 at para 583.

63 *Supra* note 61 at para 583.

64 *Ibid.*

65 *Id.* at para 629.

66 *Id.* at para 631.

67 *Id.* at para 635.

information/ data is necessary, for exercising the right of freedom of expression and information, for compliance with legal obligations, for the supra performance of a task carried out in public interest, on the grounds of public interest in the area of public health, for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, or for the establishment, exercise or defence of legal claims. Such justifications would be valid in all cases of breach of privacy, including breaches of data privacy.[68] The apex court took notice of the fact that the European Union Regulation of 2016 has also recognized 'the right to be forgotten'. The Data Protection Directive adopted in 1995 implicitly gave way to the 'right to be forgotten' with its primary objective of protecting the Fundamental Rights without hindering the free flow of data.

VI RIGHT TO BE FORGOTTEN

Right to be forgotten was considered to be distinct from right to privacy as privacy protects the information that is not publicly known whereas right to be forgotten involves removal of information, that was publicly known at a certain time, from the public domain and restricting access of third parties to such information. The concept of right to be forgotten on internet was developed for the first time in *Google Spain SL* v. *Mario Costeja González,*[69] where the Court of Justice of European Union (CJEU hereinafter) recognised right to be forgotten as part of right to privacy. In this case, Mario Costeja González alleged that Google search of his name continuing to show results of bankruptcy proceedings against him leading to an auction notice of his home, which had been repossessed, infringing his right to privacy. He filed a complaint with the Spanish Data Protection Agency AEPD to have the online newspaper reports about him as well as related search results appearing on Google deleted or altered as they were no longer relevant. While AEPD did not agree to his demand to have newspaper reports altered, it ordered Google Spain and Google, Inc. to remove the said links from their search results. The appeal was filed before the Spanish high court, which referred the matter to CJEU.

CJEU held that individuals have the right, though not absolute, to seek removal of links from search engines with personal information about them when the information is 'inaccurate, inadequate, irrelevant or excessive. The court also ruled that, these rules would also apply if the search engine providers have branch office or subsidiary in the Member State even if their physical servers are located outside the jurisdiction of the relevant Member State of EU.

The ruling recognised 'right to be forgotten' in instances of breach of right to privacy where the data is no longer relevant, inaccurate and the same has been incorporated in data protection laws including the EU's GDPR (General Data

68 *Id.* at para 636.

69 *Google Spain SL* v. AEPD and *Mario Costeja González*, 2014 ECLI:EU:C:2014:317.

Protection Regulation). After this judgment Google created a platform through which an individual can make request for taking down/delinking of a specific search result bearing its name. In India, there is no legal recognition of this right under the IT Act or the rules made thereunder.

The concept travelled beyond borders and came up before the Delhi high court in *Laksh Vir Singh Yadav* v. *Union of India,*[70] wherein the petitioner, an NRI, prayed for deletion/taking down of a judgement in a criminal case, involving his ex-wife and mother-in-law to which he was not party, from search engine results. Google, however, contended that in spite of disabling or blocking a site in its search engine, that webpage will remain on the original website and would be accessible on other search engines. The judgment will address lot of questions pertaining to this new evolving concept.

In India, the plea of 'right to be forgotten' came up before the Gujarat and Karnataka high courts wherein both came up with contradictory decisions. Although the petitioner was not granted any relief by the Gujarat high court, but where it was necessary to protect and maintain the modesty and reputation of a woman, the Karnataka high court did not deny the right to control ones' personal information.

In *Dharamraj Bhanushankar Dave* v. *State of Gujarat*[71] petitioner sought remedy under article 226 of the Constitution of India against the publication of a judgment by an online portal (India Kanoon) and the same was shown by search engine Google in its search results, inspite of being a non-reportable judgment.

The petitioner was accused for different offences including culpable homicide amounting to murder under various sections of the Indian Penal Code. The petitioner was acquitted by sessions as well as division bench of the High Court. The petitioner, when undertook procedure for migrating to Australia, came to know that the judgment was easily available on the abovementioned portal. The petitioner claimed that such publication violated article 21 and the same has also adversely affected his personal and professional life. The petitioner therefore, prayed for permanent restraint on free public exhibition of the judgment after exhausting other remedies.

The Court observed that there was no legal basis to order such removal as the petitioner could not clearly establish violation of his rights under any specific provisions/law and, it would also not be covered under the ambit of article 21 of the Constitution, as prayed.

The court clarified that the classification of reportable or non-reportable is made for the reporting of a judgment in law-reporter and not its publication anywhere else, therefore, merely publishing on the website would not amount to same being reported while taking into consideration the important fact that High Court was a court of record.

In *Sri Vasunathan* v. *The Registrar General,*[72] a woman, hereinafter called X, had filed an FIR against a man, Y, involving crimes of grave nature such as forgery,

70 WP(C) 1021/2016).

71 2015 SCC OnLine Guj 2019, decided on 19 January, 2017.

72 2017 SCC OnLine Kar 424 decided on January 23, 2017.

compelling to get married and extortion. A civil suit was also filed for annulment of her marriage with him along with a request for an injunction to restrain Y from claiming any marital rights. Later, there was an out-of-court settlement leading to closure of cases and subsequently X got remarried.

Her father filed another petition before the Karnataka high court some time later upon realizing that an online search would reveal his daughters' connections to all the legal disputes, claiming that it could result in affecting X's personal life and her public image. The court was also requested to mask X's name in cause title of the cases as well as for any other copy available at online portals.

The single judge recognized that there occasioned a serious apprehension of repercussions not only on her relationship with her present husband but also on her public image. Thus, the Court upheld the petitioners' claim and recognized the 'right to be forgotten' under her right to dignity under article 21. As per Justice Byrareddy, concluding the judgment: [73]

> This would be in line with the trend in the Western countries where they follow this as a matter of rule 'right to be forgotten' in sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned.

Thus, the Court recognized the need to maintain privacy of women in certain delicate and complex cases wherein her status and character are called into question. Such a law could protect them in their personal and social lives from any kind of discrimination or ridicule in public or private lives.

The above decision, however, contradicts freedom of speech and the right to information directly. Right to know is the most important facet of democracy. There is a continuous conflict between the right to privacy and the right to freedom of expressions. While implementing the right to be forgotten, a very fine balance has to be struck between the freedom of speech and expression, public interest and personal privacy. Also, in the absence of a global framework on this, the restriction could also be geographical and the information could still be accessible from foreign extension of the search engine.

Even though section 69A of the IT Act and the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 hold relevance, there is still a lack of clarity about the parameters of an individual's right to be forgotten and what restrictions can be imposed on the same. In the absence of data protection legislation, an ad-hoc jurisprudence will lead to divergent views being taken upon this issue, without a clear legal direction. Further, in most of the matters concerning the right to erasure, private parties are the data controllers. Therefore, the existing jurisprudence on the right to privacy as interpreted under article 21 may also be of limited value.

73 *Id.* at para 5.

The right to be forgotten needs to be a right qualified by conditions very clearly, and its conflict with the right to freedom of expression under article 19. Therefore, it is imperative that a comprehensive data protection law addresses these issues.

VII OBSCENITY

The Bombay high court giving a wider interpretation to 'sexually explicit act/ conduct' under section 67A held that sending an obscene image can also come under sexually explicit act as it need not be a bilateral activity but can be a unilateral activity also. In *Jaykumar Bhagwanrao Gore* v. *State of Maharashtra*[74] the accused was charged with section 67A of IT Act, 2000 for asking to send her obscene messages and images over phone to the complainant along with sections 354A(ii)(iii)(iv), 354A(2), 354(D)(i)(ii), 354D(2), 506, 509 of IPC. In an application/plea for anticipatory bail, it was contended that section 67A is not applicable in the given case though he may be charged with section 67 of the Act on the assumption that he has sent those messages even though he denied sending any such. Section 67A is the only non-bailable offence he is charged with which can lead to his arrest whereas section 67 is a bailable provision. The argument of the accused is that the requirement under section 67A is not merely sending of obscene messages or pictures which are lascivious or appealing to the prurient interest, but the complainant must also show some sexually explicit act or conduct on the part of the accused. It was argued that 'explicit' means there should be a detailed complete activity and no such videos or pictures were sent so prima facie no non-bailable offence under the IT Act was committed.

The court was convinced on the basis of evidence tendered before it that images were sent from the cell phones seized and the phones and mobile number belong to the accused. The court perused the obscene images sent from the cell phone of the accused and observed that the images do not show the actual act of sexual intercourse/ activity. However, the court at the same time held that a sexual explicit activity must not necessarily be a bilateral activity and can be unilateral too provided it is explicit and not implied. An image of male genital organ would be lascivious and appealing to prurient interest falling under section 67 but the image exhibiting erected handled penis as sent by accused in the present case would amount to sexually explicit activity directly falling under section 67A. The court held that a prima facie case is established and the nature of offence required a custodial interrogation and therefore rejected the anticipatory bail application of the accused.

VIII CONCLUSION

The year 2017 saw the apex court diluting the ratios of *Anwar* and *Shreya Singhal* to a large extent. The survey of cyber law during the year under review shows that in

74 2017 SCC OnLine Bom 7283.

certain spheres like intermediary liability, admissibility of electronic evidence, the courts have deviated from established norms. The Supreme Court in *Sonu* has held that a CDRs (Call Detail Records), without any section 65-B certification, could be relied upon to support the conviction on technical grounds that the piece of evidence was not contested when it was first submitted. Though raising of concern by two judge bench over law laid down in *Anwar* being applied retrospectively has led to the filing of an application in *Anwar* to clarify the lacuna in the judgment which is a positive development. It will save reopening/challenging admissibility in pending trials where requirements under section 65B were not complied with.

The legal framework on intermediary liability has also varied in the context from privacy to e-commerce and intellectual property. In the light of EU decision in Google case, the *Sabu Mathew and Kent RO* rulings by Indian courts, there is a need to streamline different approaches/models existing on intermediary liability because of its reach of effect on the rights of individuals and public at large. It is required to achieve an appropriate balance between freedom of speech, privacy through the right to be forgotten cases, hate speech cases and intellectual property violation cases.

Some very significant developments took place this year like recognition of new age concept of informational age, the right to be forgotten in *Sri Vasunathan* in sensitive cases involving women in general and highly sensitive cases involving rape or affecting the modesty and reputation of the person concerned and adopting of 'auto-block measures' by the apex court in *Sabu Mathew George* to highlight its commitment towards prevention of female foeticide in India. However, this has led to the demand of a data protection code in the country. The Data Protection Bill pending before the parliament recognises right to be forgotten, though a very limited aspect of it in a single provision. The right like other fundamental rights is not absolute and can be applied only when data becomes inadequate, irrelevant, excessive or no longer necessary. Also deletion and delinking are two different aspects attached to right to be forgotten and have different applications. This right expands the power of private intermediaries. The function of balancing rights (privacy versus speech) in the digital context has been outsourced to the private sector by the Google judgment. However, the Indian judiciary has acted cautiously in *Sabu* and *Re Prajwala,* passing on a set of words and phrases, that defeats the purpose of section 22 of PCPNDT Act or any other law prevalent, prescribed by expert nodal committee and tested by judiciary, to be blocked by the intermediaries preserving the freedom to access information. Still the court has failed to address how these changed scenarios can be balanced with the procedural safeguards. These are one sided mechanisms but there is a need to have a counter-notice mechanism for the author of the content specifically in copyright/design/ trademark infringement cases as available under Digital Millennium Copyright Act, 1998.

The recognition of right to privacy in *K S Puttaswamy* case as a constitutionally protected right not only under article 21 but also arises in varying contexts from other facets of freedom and dignity recognised and guaranteed by the fundamental rights contained in Part III of the Constitution of India and it will be interesting to see how jurisprudence evolves on right to privacy and right to be forgotten in coming year.