# 9

# CYBER LAW

*Deepa Kharb**

## I INTRODUCTION

THE PRESENT survey is an attempt to cover the ratio of various judicial pronouncements by the apex court and high courts of the country relating to the Information Technology Act, 2000 during the year 2019. Some significant principles have been added to the existing corpus of the literature on the surveyed subject though some principles enunciated by the courts require further refining or have to be substituted by some alternative principles or evolve new principles taking into account the new challenges presented by social media and e-commerce business which would ensure better governance in cyber space and instill faith, transparency and accountability in the system.

## II BLOCKING OF WEBSITES

Online piracy has become a menace which even the courts find difficult to tackle. The Copyright Act, 1957 confers a bundle of exclusive rights on the owner of a "work" and provides for remedies in case the copyright is infringed. However, with the court process being technical and time consuming, getting 'take down' orders from the court is too incommodious and arduous for the right holders. These URL/ site specific injunction remedies are not effective anymore and blocking orders against one particular URL are frustrated as these websites mirrored and multiplied immediately after such orders. Digital piracy has had a very real and tangible impact on the film industry and the rights of the owners.

The High Court of Delhi in an *ex parte* decision in *UTV Software Communication Ltd.* v. *1337X.to*[1] therefore, issued dynamic blocking injunction against few 'rogue websites' which were infringing the plaintiff's copyrighted work, publishing pirated movies by streaming and/or enabling download. Internet Service Providers ("ISPs") and the government departments concerned were also directed to block access to such "rogue websites" and "hydra headed websites".

The matter was pertaining to multiple suits filed by the plaintiffs- UTV Software Communications Ltd., Twentieth Century Fox Film Corporations and others- companies engaged in the business of creating content, producing and distributing

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

1 2019 SCC OnLine Del 8002; (decided on Apr. 10, 2019)

cinematographic films in India and around the world. An injunction was sought primarily, restraining infringement of copyright on account of defendants communicating to the public the plaintiffs' original content/cinematographic works without authorization.

The defendants that were impleaded in these suits ranged from certain identifiable websites and John Doe/Unknown parties communicating the plaintiffs' copyrighted work without any authorisation to including the registrants of the defendant-websites, uploaders, creators of redirect/mirror/alphanumeric websites; multiple ISPs along with Department of Telecommunication ("DoT") and Ministry of Electronics and Information Technology ("MEITY")grouped as non-contesting parties, against whom no relief was claimed.

Since the matter involved questions of law of general public importance, the court appointed an *amicus curiae*[2] to assist the court in the matter. The court discussed the relevant law on the subject section 2(y),(f) and (ff), 14(d), 51(a)(i) and (ii), 52(1)(c) and 55 of the Copyright Act; and sections 2(1)(w), 69-A and 79 of the Information Technology Act, 2000; along with relevant case laws, both domestic and foreign.

The court felt that it was important to create a distinction between accidental and intentional piracy by the websites. It identified Flagrantly Infringing Online Locations ("FIOLs") or Rogue Websites which primarily and predominantly share infringing/pirated content or illegal work. The court provided an indicative list of non-exhaustive list of factors for identifying such rogue websites:[3]

> a. whether the primary purpose of the website is to commit or facilitate copyright infringement;
>
> b. the flagrancy of the infringement, or the flagrancy of the facilitation of the infringement;
>
> c. Whether the detail of the registrant is masked and no personal or traceable detail is available either of the Registrant or of the user;
>
> d. Whether there is silence or inaction by such website after receipt of take down notices pertaining to copyright infringement;
>
> e. Whether the online location makes available or contains directories, indexes or categories of the means to infringe, or facilitate an infringement of, copyright;
>
> f. Whether the owner or operator of the online location demonstrates a disregard for copyright generally;
>
> g. Whether access to the online location has been disabled by orders from any court of another country or territory on the ground of or related to copyright infringement;

2 Hemant Singh, a regular practitioner in IPRs cases was appointed as the *amicus curiae* in the matter.

3 *Supra* note 1, para 59.

h. whether the website contains guides or instructions to circumvent measures, or any order of any court, that disables access to the website on the ground of or related to copyright infringement; and

i. the volume of traffic at or frequency of access to the website;

j. Any other relevant matter.

The court, referring to *Eros* v. *BSNL*[4] and the qualitative approach in the *Department of Electronics and Information Technology (DEITY)* v. *Star India*[5] case, held that the test for determining a 'Rogue Website' should be qualitative and not quantitative. Holding only that website which exclusively contains infringing content as a rogue website (i.e. quantitative approach) would prompt these websites to upload a small portion of legitimate content and escape injunction while predominantly containing pirated content. These websites were overwhelmingly infringing, observed the court, and therefore, *prima facie* the stringent measure to block the website as a whole was justified.

The court therefore introduced the concept of dynamic injunction to the Indian jurisprudence inspired from a High Court of Singapore decision in *Disney Enterprises, Inc*. v *M1 Limited* [6] where the judge held that:[7]

> I found that the court has the jurisdiction to issue a dynamic injunction given that such an injunction constitutes "reasonable steps to disable access to the flagrantly infringing online location". This is because the dynamic injunction does not require the defendants to block additional FIOLs which have not been included in the main injunction. It only requires the defendants to block additional domain names, URLs and/or IP addresses that provide access to the same websites which are the subject of the main injunction and which I have found constitute FIOLs (see [19] - [29] above). Therefore, the dynamic injunction merely blocks new means of accessing the same infringing websites, rather than blocking new infringing websites that have not been included in the main injunction.
>
> In relation to S 193DB(3)(d) of the Copyright Act, *i.e.,* the effectiveness of the proposed order, the dynamic injunction was necessary to ensure that the main injunction operated effectively to reduce further harm to the plaintiffs. This is due to the ease and speed at which circumventive measures may be taken by owners and operators of FIOLs to evade the main injunction, through for instance changing the primary domain name of the FIOL. Without a continuing obligation to block additional domain names, URLs and/or IP addresses upon being informed of such

4 2016 SCC OnLine Bom 10315 (Single Judge Bench)

5 High Court of Delhi (Division Bench) FAO (OS) 57/2015).

6 [2018] SGHC 206.

7 *Id.,* at para 38.

> sites, it is unlikely that there would be effective disabling of access to the 53 FIOLs.[8] (*emphasis supplied*)

High Court of Delhi observed that though the dynamic injunction was issued by the Singapore court under the provisions of section 193DDA of the Singapore Copyright Act, 1987 no similar procedure exists in India. In order to meet the ends of justice and to address the menace of piracy, the court, in exercise of its inherent power under section 151 CPC, espoused the concept of dynamic injunctions whereby it extended the blocking injunction against the mirror/redirect/alphanumeric websites under Order I Rule 10 CPC as these websites merely provide access to the same websites which are the subject of the main injunction.[9] The dynamic injunction would remove the need for the plaintiffs to return to court to apply for an amendment of the main injunction or for a new order.

In his report the *amicus curie* suggested the court follow the three step verification test laid down by the High Court of Bombay in *Eros International Media* v. *BSNL* (2016) to categorise any website hosts infringing as well as legtimate content third party content. Also the court should follow the principle of proportionality to justify interference with right to access internet.

However, the *amicus curie* suggested the court to exercise power under section 151 CPC to issue dynamic injunctions against mirror websited as blocking domain names was not effective in such cases.

Taking into account the argument raised by the *amicus curiae*, the court agreed that it is not disputed that given the wide ramifications of site-wide blocking orders, there has to be judicial scrutiny of such directions and that ISPs ought not to be tasked with the role of arbiters, contrary to their strictly passive and neutral role as intermediaries.[10]

Website blocking in the case of rogue websites, like the defendant-websites, strikes a balance between preserving the benefits of a free and open Internet and efforts to stop crimes such as digital piracy. The court was also of the opinion that it has the power to order ISPs and DoT as well as MeitY to take measures to stop current infringements as well as if justified by the circumstances prevent future ones.

The court further directed the MeitY/DOT to explore the possibility of framing a policy under which a warning is issued to the viewers of the infringing content, if technologically feasible in the form of e-mails, or pop-ups or such other modes cautioning the viewers to cease viewing/downloading the infringing material. In the event the warning is not heeded to and the viewers / subscribers continue to view, access or download the infringing/pirated content, then a fine could be levied on the viewers/subscribers.[11]

8 *Id*., para 42.

9 *Supra* note 1 at para 99.

10 *Id.,* para 100.

11 *Id*., para 104.

III ADMISSIBILITY OF ELECTRONIC EVIDENCE

**Section65B(4) certificate- A *sine-qua-non* or a mere procedural requirement?**

Section 65B of the Act provides the procedure regarding admissibility of electronic records. Sub-section 4 section 65B provides for the condition of obtaining a certificate before adduring electronic evidence.

This provision baffle the courts during trials because of the conflicting views among the judgements of the Supreme Court on it. Some approaches adopted by different courts regarding admissibility of electronic record under section 65B in the year 2019 are discussed hereunder.

After coming of the *Shafhi Mohammad* v. *State of H.P*[12] ruling, the *Anwar* v. *Basheer*[13] mandate has been diluted to a large extent. Every year we witness a divided approach among various cases decided by different benches where some continue to support the *Anwar* mandate and hold section 65B certificate as a mandatory requirement whereas in other cases, it is being treated as a mere procedural requirement and held even avoidable in few circumstances in the interest of justice. In *R. Subramanian* v. *ICICI Bank Ltd.*[14] in a case under Prevention of Money Laundering Act, 2002(PMLA), the High Court of Madras followed the ruling in *Shafhi Mohammad*[15] holding the 65B certificate as a procedural requirement and not a mandatory condition for the admissibility of electronic record in certain circumstances. The petitioner had challenged in a review petition the order passed by the Debt Recovery Appellate Tribunal (DRAT) since the account statement marked by the respondent bank was not accompanied by the 65B(4) certificate. However, the high court observed that the bank had submitted a certificate as per section 4 of Bankers Book Evidence Act,1891 bearing the signature of the authorized signatory of the respondent bank to hold the electronic record reliable, the condition laid down in 65B(4) as per *Anwar* ruling was satisfied. An argument was put forth by the respondent that mode and method of proof is procedural and objections if not taken at the trial should not be allowed at appellate stage in view of *Sonu@Amar* v. *State of Haryana.*[16] Further, no objections were raised by the petitioners at the time of marking the evidence nor the entries made in the statement of accounts were disputed when they had all the opportunities to do so, the petitioner were not entitled to raise objection later on.

The court ruled that since this issue was left open by the three judges bench *Anwar* therefore, by virtue of the ratio laid down by two judge bench of apex court in *Sonu*[17] applicable here, the petitioners are not allowed to raise objections to the marking of the evidence at appellate stage. The court observed that the ratio of *Shafhi*

12 2018 SCC OnLine SC 56.
13 (2014) 10 SCC 473.
14 2019 SCC OnLine Mad. 465.
15 *Supra* note 12.
16 (2017) 8 SCC 570.
17 *Ibid*.

*Mohammad*[18] was applicable to the case in hand and held that the production of certificate can be relaxed in the interest of justice since huge public money was involved and allowed the bank to recover defaulted loan dues from retail chain Subhiksha and its guarantors.

In *CBI* v. *AS Narayan Rao,*[19] an appeal filed by the CBI challenging acquittal of the accused for the offence of illegal gratification under section7 and 13(2) read with section13(1)(d) of the PCA where, to establish demand and acceptance of bribe, the prosecution relied on three audio cassettes copied from DVR. The admissibility of the evidence was challenged by the appellants on the ground that neither any DVRs (original devices recording commission of offence) were produced nor any certificate under s. 65B was submitted. The defendant challenged genuineness of the evidence alleging audio tapes to be tempered. The High Court of Delhi howbeit dismissed the appeal in the given case holding that in an appeal against acquittal high court can interfere only if the impugned judgment is perverse or illegal. Where two views are possible and the view expressed by the trial court is one of the plausible views based on the appreciation of evidence led before it, then the high court will not ordinarily interfere in the judgment of acquittal by reversing the same.

However, the Supreme Court in *State by Karnataka Lokayukta Police Station, Bengaluru* v. *M.R. Hiremath*[20] was quite clear in its approach. It applied the principle laid down in its earlier decision in *Union of India* v. *CDR Ravindra V Desai*[21] whence the Supreme Court had emphasised that non-production of a certificate under section 65B on an earlier occasion is a curable defect. Reliance was also placed on the judgment of the Supreme Court in *Sonu alias Amar* v. *State of Haryana,*[22] wherein it was held that the crucial test was whether the defect could have been cured at the stage of marking the document. Applying the said test it held that if an objection was taken to the CDRs being marked without a certificate, the court could have given the prosecution an opportunity to rectify the deficiency.

Having regard to the said principle of law, the bench held that the high court erred in coming to the conclusion that the failure to produce a certificate under section 65B(4) of the Evidence Act at the stage when the charge-sheet was filed was fatal to the prosecution. The need for production of such a certificate would arise when the electronic record is sought to be produced in evidence at the trial. It is at that stage that the necessity of the production of the certificate would arise.

In *Vijaykumar Piraji Chinchalkar* v. *State of Maharashtra*[23] in a matter related to sections 7 and 13(1) (d) read with 13(2) of the Prevention of Corruption Act, 1988, the single judge bench of High Court of Bombay rejected the contention of the prosecution that section 65B(4) requirement of certificate was no longer the *sine qua*

18 *Supra* note 12.

19 2019 SCC OnLine Del8956

20 2019 SCC OnLine SC 734.

21 2018 SCC OnLine SC 399

22 2017 (8) SCC 570.

23 2019 SCC OnLine Bom.1807 (decided on Sep. 9, 2019).

*non* for the admissibility of the electronic record after coming of the *Shafhi Mohammad*[24] ruling from the apex court. The court after referring to the relevant paragraphs of *Anwar*[25] and *Shafhi Mohammad*[26] judgments made an observation that the applicability of the mandatory procedural requirement under section 65B(4) of the Indian Evidence Act,(IEA hereinafter) of furnishing the certificate is against the person who is in the control of the device and is in a position to issue certificate under law and not of the opposite party. Since in the given case, the electronic evidence was in the possession of the prosecuting agencies and as such it was mandatory on their part to comply with the provisions of section 65B(4) and the same was not done. *Shafhi Mohammad* [27] case according to the court was applicable in cases where the evidence was in possession of third person and as such it was not possible to produce the certificate.

This case involved offence under section7,13(1)(d) and 13(2) of Prevention of Corruption Act,1988 where the accused was held guilty of demanding and accepting illegal gratification by the trial court on the basis of a transcript of conversation recorded on DVR between the complainant PW1 and the appellant-accused and statement of PW1 as recorded in evidence. No section 65B(4) certificate was produced to establish the reliability of the electronic evidence. The High Court of Bombay was approached by the appellant-accused in appeal against the lower court order challenging that the evidence was not worthy of establishing the charges. The present court ruled that to hold the appellant guilty in the case under such sections, the prosecution was required to prove demand and acceptance of bribe against him by cogent evidence. However, the electronic evidence was held not worthy of being read in evidence otherwise also, even if the admissibility of the electronic record is brushed aside, not being in tune with the statement of the complainant as PW1.

On a similar account, the High Court of Delhi in a criminal appeal filed before it by the accused-appellant, challenging his conviction by the sessions court in a kidnapping case, referred to the relevant excerpts of the *Shafhi Mohammad* [28] judgment to decide on the admissibility of electronic evidence in the absence of section 65B certificate. The court in this case *Gulshan* v. *State*[29] repeated in para 31 of its judgment that the requirement of producing a certificate under section 65B is a procedural aspect which can be relaxed whenever required and justified, in the interest of justice. Therefore, rejecting the contention of the appellant that the scientific evidence involving the comparison of his fingerprints with the chance prints lifted from the car used in kidnapping was not admissible against him for want of such certificate, the court supported the conviction by the trial court by allowing reading the evidence as it was also in tune with the testimonies of the witnesses.

24 *Supra* note 12.

25 *Supra* note 13, para 14,15 and 22.

26 2018 SCC OnLine SC 56.

27 *Supra* note 12.

28 *Supra* note 12.

29 2019 SCC OnLine Del. 6552(decided on Jan. 17,2019).

The Supreme Court in case of *State of Karnataka* v. *M. R. Hiremath* again pointed out that failure to produce section 65B certificate along with charge sheet not fatal to prosecution. Holding that the high court has erred in its conclusion of quashing the proceedings against the accused.

In other cases where secondary evidence was submitted in evidence without the certificate, courts have generally held the evidence as inadmissible reaffirming the *Anwar* mandate. In *Sanjay Kumar Singh* v. *CBI*[30] the conviction of the appellant under section13(1)(d) of Prevention of Corruption Act,1988 (PCA hereinafter) read with section120B IPC was based on evidence including digital evidence in the form of audio cassettes prepared from DVR. Hearing the appeal filed by the appellant challenging the trial court conviction order against the said appellant, High Court of Delhi held that the evidence was not reliable in the absence of section65B certificate and in the absence of digital evidence his conviction was not sustainable. The convictions of other accused in the case though were sustainable on independent evidences available against them and not affected by the acquittal of the said accused.

In *Samsung (India) Electronics (P) Ltd.* v. *MGR Enterprises*[31] also the High Court of Delhi relied upon the principle laid down in *Anwar*[32] and dismissed a petition filed against the order of the Metropolitan Magistrate, holding that the petitioner was unable to prove the legal liability of the respondents for the offence under section 138 (dishonour of cheque) of the Negotiable Instruments Act, 1881.The computer-generated copy of the ledger statement of the respondent's account, according to the bench, would be admissible only when accompanied by a certificate under section 65-B of the Evidence Act and in the absence therefore, it would be inadmissible.

The petitioner had filed a complaint under section 138 against the respondents on account of the cheque given by them being dishonoured on presentation, on account of "insufficient funds". The respondents were appointed as the dealer of the petitioner's products. According to the petitioner, the respondent defaulted in paying a certain sum of money to them, after which the petitioner presented the cheque provided by the respondents for satisfying the outstanding dues. The respondent's, however, disputed any liability.

To prove their case, the petitioner produced a computer-generated copy of the ledger statement of the respondent's account maintained with the petitioner. Petitioner contended that since no objection was raised qua the mode of proof at the time of exhibiting the copies of the ledger account, the same are duly exhibited, proved and admissible in evidence.

The court observed in para 22 of its judgment that the legal position on the point is thus well settled i.e. if the document is otherwise inadmissible for want of a certificate or any other requirement of law, its exhibition in the course of trial does not make the document admissible in law. Though an objection as to the mode of

30 2019 SCC OnLine Del. 8247

31 2019 SCC OnLine Del 8877 (decided on May 24,2019).

32 *Supra* note 13.

proof can be waived off and should be taken at the first instance, however, the objection as to the admissibility of a document which goes to the root of the matter can be taken at any stage." Since the petitioner did not submit the section 65-B certificate, the computer-generated ledger produced by it was held inadmissible. The court repeating the Supreme Court preposition in *Anwar* case,cited para 20 of *R.V.E. Venkatachala Gounder* v. *Arulmigu Viswesaraswami*[33] to support its refusal to interfere in the findings of the Metropolitan Magistrate.

**Section 65B certificate-condition for secondary evidence only**

There still exists a legal uncertainity in judgements given by lower and some high courts on whether the requirement of certificate mentioned under section 65B(4) is a mandatory pre-condition before producing only secondary evidence as a document as far primary evidence also.

In 2017, the Supreme Court in the matter of *Vikram Singh* v. *State of Punjab,*[34] referring to *Anwar,*[35] clarified that where electronic record is produced/used as primary evidence, compliance with the conditions under section 65B of IEA is not required and the same is admissible in evidence. The High Court of Delhi in *Chattarpal Lodha* v. *State of NCT*[36] in a case filed under section13(1)(d) and (2) of Prevention of Corruption Act read with section120B of IPC reiterated the same that where the original device(hard disk) recording, the CCTV footage was produced in evidence as per section 62 of the Evidence Act, the required certificate under section 65B(4) is unnecessary. The requirement of section 65B certificate as mandated in *Anwar* was applicable where in the absence of primary evidence, a copy of such electronic record, recorded in different device and medium was filed as evidence to establish the authenticity of the said secondary evidence.

**Contents of a memory card- document or material object?**

Giving prominance to larger public interest while balancing inter fundamental rights becomes necassary in certain unprecedented situations. The court in the present case observed that right to fair trial has both prespectives-right to a fair trial of the accused and right to privacy of the victim. The constitutional courts need to weigh the conflict to award justice to both the parties and society at large serving the ends of justice constituting rule of law.

In *P. Gopalkrishnan* v. *State of Kerala*[37] the Supreme Court bench held that the contents of a memory card or a pen drive in relation to a crime amount to a 'document' and not a 'material object' and the accused would be entitled to a copy of the same to prepare his defence under section 207 of the Code of Criminal Procedure, 1973. However, if the electronic evidence pertained to a rape case then the trial court, keeping in mind the sensitivity of the contents, the privacy, dignity and identity of the victim

33 (2003) 8 SCC 752.

34 (2017) 8 SCC 518.

35 *Supra* note 13.

36 2019 SCC OnLine Del 9667.

37 2019 SCC OnLine SC 1532, (decided on Nov. 29, 2019).

involved in the stated offence(s) and more so because of the possibility of misuse of such cloned copy by the accused, could deny a copy but may allow the inspection to the accused and his/her lawyer or expert for presenting effective defence during the trial.

The matter related to Kerala actor Dileep's plea for handing over a copy of the visuals of the alleged sexual crime committed on an actress. The court observed that if the prosecution was to rely on the fact of recovery of a memory card, then it could be treated as a material object. However, if the contents of the memory card are sought to be relied upon by the prosecution, then the same would be documentary evidence.

The judgment referred to section 3 of the Indian Evidence Act, 1872 which includes electronic records in the definition of 'documentary evidence'. The court observed that tape records of speeches, and compact discs containing visuals, etc have been held to be "documents" by precedents. Also, section 2(1)(t) of the Information Technology Act, 2000 [IT Act, 2000] defined "electronic record" to mean 'data, record or data generated, image or sound stored, received or sent in an electronic form or microfilm or computer generated microfiche'. In this backdrop, the court held that the footage/clipping contained in such a memory card/pen drive, being an electronic record as envisaged by section 2(1)(t) of the IT Act, 2000, is a "document" and cannot be regarded as a "material object".

The accused would be entitled to a copy of the same to prepare his defence under section 207 of the Code of Criminal Procedure, 1973. However, where the electronic evidence pertained to a rape case then the trial court, keeping in mind the sensitivity of the contents, could deny a copy but may allow the inspection to the accused and his/her lawyer or expert for presenting effective defence during the trial.

## IV ONLINE OBSCENITY

The Information Technology Act, 2000 has provisions for dealing with various types of cybercrimes.[38] Sections 66E, 67, 67A specifically deal with cybercrime related to pornography. Section 67B provides punishment for publishing or transmitting of material depicting children in sexually explicit act in electronic form.

**Content must be explicit to attract 67 of Information Technology Act, 2000**

Section 67 punishes a person who publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons on being exposed to it. The section is gender-neutral. However, the section is seen to be used to cover cases of all kinds of objectionable and offending posts whether defamatory, hateful or distasteful.

In *Sreekumar V.* v. *State of Kerala*[39] a case pertaining to the posting of obscene remarks on the Facebook page of a woman who was a member of a political party came before the High Court of Kerala.A case was filed by the lady against him under

38 Indian Penal Code, 1860 ss. 43, 43A, 66, 66B, 66C, 66D, 66E, 66F, 67, 67A, 67B, 71, 72, 72A, 73 and 74 provides punishment/penalty for various cyber crimes.

39 2019 SCC OnLine Ker 1305, (Order dated Apr.3,2019).

section 509 of the Indian Penal Code, 1860, section 67 of the Information Technology Act, 2000 and section 120(o) of the Kerala Police Act, 2011. While offences under section 509 IPC and section 120(o) of the Kerala Police Act are bailable offences, 67 offence is grave, non bailable and attracts seven years' jail term and a fine up to Rs.10 lakh. Hence the accused apprehending arrest approached the high court for anticipatory bail.

Applicant-accused participated with a male member of CPI (M) party in a television debate to discuss the Supreme Court's judgment on the right of women devotees of menstrual age to enter and worship in the Sabarimala Temple[40] wherein the member of CPI(M) presented a strong argument in favour of the said judgment. The applicant was agitated by the stand taken by CPI(M)'s member as he believed that women must not be permitted to enter Sabarimala respecting customs and traditions. Following this, he made certain posts on the said member's wife Facebook page who was also a member of CPI-M, a media person and also an assistant professor of law describing her husband in highly abusive language and also made disparaging remarks regarding faith and religion. He also sent obscene messages to the lady with the intention to insult her womanhood and reputation and to cause her mental distress. Learned counsel appearing for the applicant contended that the nature of the factual allegations raised in FIR did not disclose an offence under section 67 of IT Act. Whereas, the public prosecutor appearing on behalf of the state contended that the impugned publication on complainant's Facebook page would be covered under section 67 of IT Act.

The court observed that even if the words are extremely un-parliamentary, unprintable and abusive in nature, so long as the words in question are not one capable of arousing sexual thoughts in the minds of the hearers and does not involve lascivious elements arousing sexual thoughts or feelings or the words do not have the effect of depraving persons, and defiling morals by sex appeal or lustful desires, it cannot be brought within the broad contours of the penal provisions as contained in sections 294 and 292 of the Penal Code corresponding to section 67 of the Information Technology Act, 2000.

The lack of awareness regarding cyber crimes in the police officers was again highlighted in *Subhendu Nath* v. *State of W.B*.[41] High Court of Calcutta felt that there is a crying need to train and familiarise police personnel in this regards. The gist of the allegations in the FIR related to this matter pertaining to a matrimonial dispute between the petitioner and his wife, where it was alleged that the petitioner with the object of defaming and denigrating the wife had posted and circulated objectionable pictures of wife on a social network platform.

Though the FIR was registered *inter alia* on such accusations, offences under sections 66E and 67A of the Information Technology Act were not added to the FIR. The High Court of Calcutta observed that the investigation was conducted by the assistant sub-inspector of police in violation of section 78 of the IT Act. Therefore the

40 *Indian Young Lawyers Assn*. v. *Union of India*, 2018 SCC OnLine SC 1690

41 2019 SCC OnLine Cal 242, (Order dated Feb. 18,2019).

high court taking note of the lack of awareness and preparedness on the part of the members of the police force in the matter of collection, reception, storage, analysis, and production of electronic evidence issued following directions to ensure that the investigation of crimes involving electronic evidence is conducted in a fair, impartial and effective manner in the -

- Proper training of members of police force in reception, preservation and analysis of electronic evidence.

- Only the officers who have been trained in accordance to the manner as stated above shall be involved in the investigation of crimes involving offences under IT Act and the offences in which electronic evidence plays a pre-dominant part.

- Every district shall have a cyber cell comprising of officers with specialised knowledge in the matter of dealing with electronic evidence in order to render assistance to local police.

- A standard operating procedure regarding preservation, collection, analysis and producing electronic evidence to be submitted by Director General of Police, West Bengal on the next date of hearing.

- Specialised forensic units to be set up in the State in order to facilitate examination and/or analysis of electronic evidence.

The bench further stated that:

> "It is also relevant to note that electronic evidence by its very nature is susceptible to tampering and/or alteration and requires sensitive handling. A breach in the chain of custody or improper preservation of such evidence render it vitiated and such evidence cannot be relied in judicial proceedings. Necessary certification under Section 65D of the Information Technology Act is also a pre-requisite for admissibility of such evidence. Even if such certification is present, reliability of electronic evidence depends on proper collection, preservation and production in court. Any lacuna in that regard would render such evidence vulnerable with regard to its probative value. These factors have come to our notice not only in the present case but also in a number of cases argued before us in recent times."

## V INTERMEDIARY LIABILITY

**Holding ISPs liable for IP violations**

The safe barbour jurisprudence has undergone a major shift in last few years on the aspect of immunities afforded to intermediaries in relation to e-commerce intellectual property violation and other unlawful and tortious acts.

In the absence of any holistic policy framework regarding intermediaries, we are witnessing a trend where the courts, as a natural consequence of the certain types of cases being bought before them have evolved a jurisprudence based on the rule of intermediaries in contributing towards on enabling a specific bases and their

corresponding ability to address a specific harm. This calibrated approach, ranging from notice and take down in IP violation on e-commerce to proactive monitoring in rape and pedophilic/rape related content appears to be more effective right now than requiring all types of intermediaries adopting similar policies.

In *Amway India Enterprises* v. *1Mg Technologies Pvt. Ltd*,[42]Amway India Enterprise a subsidiary of Amway Corporation of Michigan, United States of America filed for interim and permanent injunction against the defendant for unauthorised selling of its products at their medical shops as violative of Direct Selling Guidelines, 2016 issued by the government. The plaintiff issued a public statutory warning through newspaper on November 9, 2017, the very next day of getting information about it. The defendants continued selling of their products after removing the unique codes placed on the lid of the products, also without issuing invoice and not providing benefit of plaintiffs return/refund policy. Plaintiff requested for issue of temporary injunction against ecommerce platforms and the sellers selling their products on these platforms without authority. Oriflame and Modicare, other DSEs (Direct Selling Entities) also filed case against Amazon on similar grounds.

The apposite questions before the court was whether ecommerce platforms are intermediaries entitled to safe harbour under section 79 of the Act and whether sale of plaintiff's products amounts to trademark infringement or misrepresentation, dilution, tarnishment or passing off of plaintiff's trademark? Whether the Direct Selling Guidelines, 2016 are valid and binding over the defendants in the present case? If so, whether there is a violation of the guidelines on the part of defendants?

The single judge held defendant's act of unauthorised use of the Plaintiff's trademark and sale of its products was violation of Plaintiff's trademark rights and has resulted into passing off, dilution and misrepresentation as well as violation of Direct Selling Guidelines, 2016 issued by government. The single judge held that the Guidelines were very much valid and binding on ecommerce platforms and sellers on such platforms as law, being issued and notified in terms of the article 77 of the Constitution of India. The court also brushed aside defendant's contention that direct selling was well within their freedom under article 19(1)(g). The single judge observed that the defendants were well aware of the applicability of the Guidelines on them but not only they overlooked the Plaintiff's right to direct distribution of its products and damage caused to the goodwill of the plaintiff but also based their defence on illegality.

The court went on with a detailed reasoning to declare that the defendants were not eligible for immunity under section 79(2)(c) of Information Technology Act( the Act hereinafter) since they failed to observe due diligence as required for claiming exemption from liability in third party acts/transactions. The court held that the role of the defendants was not passive but they were facilitator providing logistic support, packaging and delivery services, hence, do not qualify to be intermediaries under section 79.

42 2019 SCC OnLine Del 9061.

Regarding the infringement of plaintiff's trademark rights of the plaintiff, the court held that first it was required to determine whether the sale of the products by ecommerce platform or by any of the sellers on ecommerce platform is legal and valid and whether the conduct of the ecommerce platform is protected under section 30 of Trademarks Act, 1999 or not and then only it will be determined whether they are guilty of infringement of trademark, passing off, misrepresentation and dilution.

Section 29 though permits use of the trademark to indicate the origin of the goods provided the goods are genuine. However, any conduct of the seller/ecommerce platform resulting in taking unfair advantage of the distinctive character of the trademark like using on packaging or for advertisement would amount to infringement under section 29(6) and (8) of Trademark Act and section 30(3) would not come to the rescue of the seller if the conduct of the seller results in the impairment of the products by changing their packaging, warranty conditions or removal of codes of the products causing damage to the reputation of the mark or undermining the quality of the mark. Even though it was vehemently contended by the defendant parties that present suit was not based on infringement of trademark rights, the court held that it was one of the legal basis for seeking injunctions as per the averments made by the plaintiff in several paragraphs of the plaint filed. Hence the court allowed injunctions against the defendant ecommerce websites restraining them from advertising, displaying, offering for sale products of the plaintiff.

**Intermediary liability for criminal defamation and the immunity under the older version of section 79**

Supreme Court refused to grant protection to Google in an old FIR filed against it holding that section 79 of the Act, prior to its substitution in 2008, did not protect an intermediary in regard to the offence under section 499/500 of the Indian Penal Code. An appeal was filed before the apex court in *Google India Pvt. Ltd*. v. *Visaka Industries*[43] against the decision of the High Court of Andhra Pradesh, where a matter related to criminal defamation filed in 2009 by Visaka Industries in relation to its hosting of a defamatory article titled "Visaka Asbestos Industries Making Gains" published by Ban Asbestos Netwok India(BANI) was heard by the division bench.

It was alleged by Visaka Industries herein that in spite of multiple requests filed by the company, Google failed to take down the defamatory articles published against it under a group named 'Ban Asbestos' hosted on Google Group services. Rather Google approached the High Court of Andhra Pradesh under section 482 to quash the criminal defamation complaint against it, claiming intermediary immunity under section 79 of the IT Act.

High Court of Andhra Pradesh rejected their plea holding Google India liable as intermediary for not taking any action against complaints filed by the respondent. Hence the present appeal was filed by Google before the Supreme Court contending that the parent company was the intermediary here and it was neither the author nor publisher to incur liability.

43 (2020) 4 SCC 162.

The apex court bench felt that it was apposite here to take a deeper look at section79 first and started with the findings of the high court on section79 which were summarised as:[44]

i. The earlier version of Section 79 kept at bay the impact of other laws. After the amendment, Section 79 affords exemption from any other law in respect of the third-party information subject to sub-Section (2) of Section 79.

ii. Intermediary under the extant provisions of Section 79 cannot seek refuge in Section 79 if it failed to expeditiously remove or disable access to the objectionable material or unlawful activity even after receiving actual knowledge thereof.

iii. In the case, it is found that in spite of the first respondent complaint issuing notice about dissemination of defamatory information on the part of A1-accused no.1-appellant did not move its little finger to block the material or to stop dissemination of unlawful and objectionable material. This conduct of the appellant disentitles it from claiming protection either under the provisions of the unamended Section 79 or under Section 79 after substitution. The offence in this case was perpetuated from 1.07.2008 onwards since long prior to the substitution.[45]

The bench observed that section 79, before its substitution, exempted the network service provider/ intermediary from liability in regard to any third party information or data made available by him provided the service provider:

i. Proves that the offence or contravention was committed without his knowledge;

ii. The service provider proves that he had exercised all due diligence to prevent the commissioning of such offences or contraventions.

The extant section79 was confined to the liability of the network service provider arising out of the provisions of the Act and it was not, in short, a bar to the complaint under section 500 of the IPC being launched or prosecuted.

The court also responded to the appellant's contention that not Google India but Google LLP is an intermediary here and that it is mere subsidiary and the services were provided by the parent company Google INC directly to the users. The court held that it was a matter of trial and refused to adjudicate on this contention.

**Ensuring compliance through personal appearance of ISP in IP Infringement**

In *Facebook Inc.* v. *Surender Malik* and *Instagram* v. *Surender Malik*[46] the plaintiff filed for permanent injunction to stop infringement of his trademark 'DA MILANO' and passing off against the infringers for putting up posts on Facebook and Instagram advertising and offering for sale products bearing his trademark DA MILANO alongside impleading Facebook and Instagram under section 79 to ensure

44 *Id* ., para 48.

45 *Ibid.*

46 2019 SCC OnLine Del 9887 (decided on Aug. 28,2019).

that the posts were taken down as well as claiming personal appearance of the defendant. Facebook and Instagram claimed immunity from the liability being exempted under section79 of the Act as well as exemption from personal appearance. The trial court, in the absence of any plausible reason cited by the defendants, disallowed the plea of exemption from personal appearance of Facebook and Instagram as it felt that there was a tendency to prolong the proceedings unnecessarily. Hence Facebook and Instagram challenged the order of the trial court before the High Court of Delhi claiming that they are mere intermediaries their presence is not required.

The High Court of Delhi accepted their contention and held that both the platforms appear to have not played any active role in the infringement activity and the same has also not been alleged by the plaintiff. The court therefore, issued directions to the two platforms to remove such content in future also whenever notified by the plaintiff as per Rule 3(4) of the guidelines and shall also keep intimating the plaintiff on any violation or offending post, allowing exemption from personal hearing to the two platforms.

**Lack of immediate relief against online posting of defamatory, sexually explicit material, pornography or hate speeches/ inconvenience and annoyance after repeal of section66A**

In *Chegudi Ashok Babu* v. *Karunakar Sugguna,*[47] Chegudi and other, claiming to be Pastors of the churches, filed a *pro bono* writ petition for the issue of mandamus for the declaration of release of abusive tele teaser of the short film 'Nene Devuni' on YouTube channel as violation of freedom of religion guaranteed under article25 of the Indian Constitution. Karunakar Sugguna is the writer, director of the movie released under the banner of Shivashakthi Creations. The alleged movie trailer in the 'Second Coming of Jesus' has presented the story in contradiction to the Holy Bible, hurting the feelings of millions of followers of Jesus and has done it intentionally to create religious disturbances in the society between two communities during election time. Therefore it was contended to stall the release of the said movie scheduled to be released on April 27, 2019.

The tele teaser was removed from the YouTube channel and was not available for the inspection by the said high court. Few print outs of the screen shots were produced for the consideration of the court as evidence which were found insufficient by the court to accept the contention of the petitioner. The High Court of Andhra Pradesh at Amrawati observed that the said teaser falls under the definition of electronic mail/electronic mail message as per the explanation to section 66A of the Information Technology Act, 2000. Since the Supreme Court in *Shreya Singhal* v. *Union of India* declared the said section as unconstitutional in 2015, the court focussed upon section 79 of the Act for exploring the liability of YouTube channel in the matter, if any as being the intermediary falling under section 2(1)(w) of the Act and referred to the 'gate keeping' liability model and due diligence requirement under section 79(especially 79(3)(b)) read with rule 3 and 4 as discussed in some relevant literature

47 2019 SCC OnLine AP109 decided on August 2, 2019.

and *Shreya Singhal* judgment. The court was of the opinion that since no remedy could be availed to the petitioners under section 66A after the same stands repealed from the Act, it was open for the petitioner to file a complaint under section 295A IPC and to lodge a formal 'cease and desist' notice to the headquarter of YouTube to block the said teaser and trailer and approach civil court in case of non compliance by the said 'intermediary'.

## VI IDENTITY THEFT IN CYBER SPACE

Digitisation and internet penetration has increased tremendously in last few years in India. The number of internet users in India has reached half a billion as of November 2019 and is growing at a rate of 10 percent every year in urban areas and 15 percent in rural areas.

With the proliferation of identity based e-governance, economic transactions as well as social interactions, identies theft issues have become a serious concern globally. The concerns get further aggrevated in India because of poverty and lack of awreness regarding digital skills and technology *ie.* digital literacy. In the absence of a comprehensive data protection lagislation. Section 66C of the Information Technology Act defines and provides punishment for provision as of now, litigation ais bound to increase in this area in days to come. This case discussed here highlights that mere use of someone's identity is not punishable rather fradulent and dishonest intention must be established in addition to such use to punish a person for identity theft.

In *State of Uttarakhand* v. *Akhtar Ali,*[48] the matter involved a case of kidnapping, rape and killing of a seven year old girl in Uttarakhand. The three accused Akhtar Ali along with Prem Pal Verma and Junior Masih were charged under sections 363, 201, 120-B, 376-A, 302 IPC and sections 16/17 read with sections 4, 5, 6, 7 of the POCSO Act. This appeal was filed by the accused against their conviction.

It was argued on behalf of the accused that mere use of SIM-card of another person does not attract the provisions of section 66C of the Act and as such no offence under section 66C of the Act or section 212 IPC could be made out against them.

The essence of section 66C of the Act, according to the bench, which provides for offences in cases of identity theft, is *fraudulent and dishonest* use of electronic signature, password or any other unique identification feature. In the instant case, though the prosecution tried to establish that since Akhtar Ali was using mobile phones, which were obtained in the name of Laxmi Devi and Mohd. Iqbal, he has committed offence under section 66C of the Act. However, Laxmi Devi and Mohd. Iqbal, in whose names, these numbers were taken were not examined in the court. They have not stated on oath that their identities have been used fraudulently or dishonestly. The court can not presume it. Mere use of identity of some other person for obtaining SIM, in view of this court, does not attract provisions of section 66C of the Act. It requires something more. It is not proved in this case. Therefore, the court was of the view that the charge under section 66C of the Act is not proved against all the three accused persons.

48 MANU/UC/0918/2019 (decided on Oct.18,2019).

## VII CONCLUSION

The year 2019 saw some important deliberations in the area of cyber law. There was a path-breaking judgment in *UTV Software Communication Ltd*.[49] where the High Court of Delhi, despite the lack of sufficient statutory provisions, granted a 'dynamic' blocking injunction against certain websites publishing pirated films whereby the list of blocked websites can be updated as and when mirror websites are brought to the notice of the court by the right holder. Accordingly, the right holders instead of repeating the whole exercise of getting a judicial order from the judge/ bench, can directly approach the joint registrar (judicial officers discharging procedural functions on behalf of the judges) of the high court to extend the injunction against a mirror or indirect replica of the blocked website publishing the same infringing content. Court gave due consideration to the necessity, proportionality and reasonableness of such measures and sufficiently delineated the factors to classify a website as a rogue website. The court was also mindful about the fact that most of the viewers are young people who visit these websites due to the ease of availability of the content without comprehending the wide repercussions for the copyright industry in audio-visual content on internet. It adopted a pro-active approach to balance interests of rights holders against "free internet" by suggesting the government body to explore the possibility of framing a policy and consider cautioning even individual users to refrain from using pirated content but followed by a fine if the user continues to engage with such platforms.

In other areas too like ISP liability and admissibility of electronic evidence further deliberations and clarity was definitely ushered.

49 *Supra* note 1.