9

CYBER LAW

*Deepa Kharb**

I INTRODUCTION

CYBER SPACE continues to spawn unique and abrupt questions demanding legal innovation and activism. A perusal of the cases decided by the Supreme Court and various high courts during the year under investigation reveals a variety of issues coming before the courts like those concerning intermediary liability, blocking of websites, admissibility of electronic evidence *etc.* The survey presents a critical analysis of judicial pronouncements delivered by the apex court and high courts in the year 2018 that have either laid down new principles or propounded debatable prepositions in order to elucidate the scope and extent of cyber law.

II 'GENERALIA SPECIALIBUS GENERAL NON-DEROGANT'

In relation to electronic records, Supreme Court judgment in *Anwar*[1] declared a new law in respect of the evidentiary admissibility of the contents of electronic records, the special procedure created under section 65A and 65B of the Evidence Act, 1872, giving effect to the *'generalia specialibus general non-derogant'* rule (the general does not detract from the specific; a restatement of the principle *lex specialis derogate legi generali* meaning special law repeals general law). It held that the provisions of sections 65A and 65B of the Evidence Act, 1872 created special law that overrides the general law of documentary evidence procedure in sections 63 and 65. Till this judgment, courts have been applying sections 63 and 65 on electronic evidence, ignoring sections 65A and 65B of the Evidence Act.

Relying on the principle of *lex specialis derogate legi generali* (special law repeals general law) Supreme Court in *Sharat Babu Digumarti* v. *Govt. of NCT of Delhi*[2] held that once the criminal act is sufficiently covered by the 'special' provision of the Information Technology Act, 2000 (IT, Act) it shall prevail over the general and prior laws like Indian Penal Code, 1860 (IPC) to avoid violation of the principle of double jeopardy.

Recently, a two judge bench of the High Court of Bombay *vide* its judgment in *Gagan Harsh Sharma* v. *State of Maharashtra*[3] held that when an offence is sufficiently

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

1 *Anvar P.V* v. *P.K. Basheer* (2014) 10 SCC 473.

2 2016 SCC OnLine SC 1464.

3 2018 SCC OnLine Bom 13046.

covered under the provisions of the IT Act, the IT Act being the *lex specialis* will apply to the exclusion of the IPC. On the basis that the ingredients of offences alleged under IPC were the same as compared to the ingredients of the offences alleged to have been committed under IT Act, the court quashed the FIR insofar as the investigation into the offences punishable under the IPC were concerned.

In this case an FIR was filed by Manorama Infosolutions Private Ltd. ('Manorama' hereinafter) against the accused under sections 43, 65 and 66 of the IT Act and under sections 408 and 420 of the IPC for theft of its healthcare software. It was alleged by Manorama that certain employees of theirs along with third parties had gained access to their computer system and stole certain source code to create their own software.

The question for consideration of the High Court of Bombay was, whether the offences alleged under sections 43, 65 and 66 of the IT Act could be tried together with the same offence alleged to have been committed under the IPC under section 408,420.

It was contended by the petitioners that since the alleged offences can be sufficiently dealt with under the 'special' provisions of the IT Act, the FIR to the extent it concerns the offences under IPC, should be set aside. Further, it would deprive the accused the benifit as being bailable and compoundable under IT Act in contrast to provisions under IPC for the same offence.

A reference was made to the Supreme Court decision in *Sharat Babu Digumarti,*[4] where the accused were charged with offences under section 67 of the IT Act and section 292 of the IPC. The question for the consideration of the Supreme Court was whether the accused, discharged under section 67 of IT Act, could still be prosecuted under section 292 of IPC. Placing reliance on non-obstante provisions under section 81 of IT Act and section 67A and 67B, the apex court dropped the charge under section 292 of IPC. It believed that if the legislative intent is discernible that a latter enactment shall prevail, it should be respected and given effect.

The decision was footed on the basis that sections 67, 67A and 67B was a complete code regarding offence concerning publishing and transmitting obscene material in electronic form and non-obstante provision under section 81 makes IT Act a special law which shall prevail over the general law, IPC.

Similarly, referring to *State (NCT) of Delhi* v. *Sanjay*[5] where the Supreme Court while considering the phrase 'same offence' was deciding whether illegal mining of sand under Mines and Minerals (Development and Regulations) Act 1957 would oust the jurisdiction/application of sections 378 and 379 of IPC. Supreme Court held that the principle of double jeopardy will not apply where the ingredients of both the offences are different.

The High Court of Bombay noted that the offence in question involved the use of computer source code and computer systems for stealing software, an offence under section 43 and section 66 of the IT Act. It further held that the terms 'dishonestly' and

4 *Supra* note 2.

5 2014 SCC OnLine SC 672.

'fraudulently' used in section 66 referred to the definitions given under IPC. When an offender is prosecuted under both enactments and the ingredients of the offence alleged under IT Act are the same as compared to the offence alleged IPC, it would amount to being prosecuted for the same offence twice. This would, therefore, amount to a violation of the principle of protection against double jeopardy as per article 20(2) of the Constitution of India.

Incorporating the principles of *Sharat Babu*[6] and *Sanjay,*[7] the High Court of Bombay held the IT Act is a complete code in itself and a special enactment for various aspects of electronic data and computer systems.[8]

> ….The Act of accessing or securing access to computer/computer system or computer network or computer resources by any person without permission of the owner or any person who is in charge of the computer, computer system, computer network or downloading of any such data or information from computer in a similar manner falls within the purview of Section 43 of the Information Technology Act, 2000. When such Act is done dishonestly and fraudulently it would attract the punishment under Section 66 of the Information Technology Act, such Act being held to be an offence. The ingredients of dishonesty and fraudulently are the same which are present if the person is charged with Section 420 of the Indian Penal Code. The offence of Section 379 in terms of technology is also covered under Section 43. Further, as far as Section 408 is concerned which relates to criminal breach of trust, by a clerk or servant who is entrusted in such capacity with the property or with any dominion over property, would also fall within the purview of Section 43 would intents to cover any act of accessing a computer by a person without permission of the owner or a person in charge of computer and/or stealing of any data, computer data base or any information from such computer or a computer system including information or data held or stored in any removable storage medium and if it is done with fraudulent and dishonest intention then it amounts to an offence. The ingredients of an offence under which are attracted by invoking and applying the Section 420, 408, 379 of the Indian Penal Code are covered by Section 66 of the Information Technology Act, 2000 and prosecuting the petitioners under the both Indian Penal Code and Information Technology Act would be a brazen violation of protection against double jeopardy.
>
> In such circumstances if the special enactment in form of the Information Technology Act contains a special mechanism to deal with the offences falling within the purview of Information Technology Act, then the invocation and application of the provisions of the Indian Penal Code being applicable to the same set of facts is totally uncalled

6 *Supra* note 2.

7 *Supra* note 5.

8 *Supra* note 3.

> for. Though the learned APP as well as Shri. Gupte has vehemently argued that the prosecution under the provisions of the Indian Penal Code can be continued and at the time of taking cognizance the Competent Court can determine the provisions of which enactments are attracted and it is too premature to exclude the investigation in the offences constituted under the Indian Penal Code, we are not ready to accept the said contention of the learned Senior Counsel, specifically in the light of the observations of the Apex Court in the case of *Sharat Babu Digumarti* (Supra). We are of the specific opinion that it is not permissible to merely undergo the rigmarole of investigation although it is not open for the Investigating Officer to invoke and apply the provisions of the Indian Penal Code, in light of the specific provisions contained in the Information Technology Act, 2000 and leave it to the discretion of the Police Authorities to decide in which direction the investigation is to be proceeded. The Information Technology Act, 2000 being a special enactment, it requires an able investigation keeping in mind the purpose of the enactment and to nab the new venturing of crimes with the assistance of the Technology.[9]

Therefore, quashing the proceedings against the petitioners, it was held that the offences in question are sufficiently covered under the IT Act and the IT Act being *lex specialis* would override the general law *i.e.,* the IPC. However, there is a need to excercise judicial caution against over-emphasis or reliance on the doctrine of double jeopardy or mechanical application of this special-general canon in every second criminal case in the absence of any conflict between the two. The expressions 'same offence' and 'conflict' has to be sufficiently satisfied, like it was done in *Sharat Babu Digumarti*[10] requiring utmost precaution as different legislations operate in different fields in respect of such offences and may have been passed with different intentions altogether. The possibility of co-existence of charges under different laws for the same act/transaction is also well recognised.

III INTERMEDIARY LIABILITY

The intermediaries were put under an obligation by Central Government under Intermediary Guidelines of 2009 to take down unlawful content hosted/uploaded within 36 hours of receiving 'actual knowledge'.[11] In *Shreya Singhal*[12] however, the court read down the 'actual knowledge' under section 79(3) (b) to mean receipt of a court order/notification directing intermediaries to remove or disable access to content

9 *Ibid.*

10 *Supra* note 2.

11 Information Technology (Intermediary Guidelines) Rules, 2011 Rule 3 (2) of the Intermediary Guidelines stipulates that intermediaries are required to inform their users not to host, display, upload, modify etc. information of the nature mentioned under that rule. Rule 3(4) is the takedown provision which states that any information which is in contravention of Rule 3 (2) must be disabled by an intermediary within thirty-six hours of "obtaining knowledge by itself or [receiving] actual knowledge by an affected person in writing ….".

12 *Shreya Singhal* v. *Union of India* 2015 SCC OnLine SC 248.

expeditiously. It was expected to provide 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.[13]

The High Court of Delhi however in its judgment in *MySpace Inc.* v. *Super Cassettes Industries Ltd.*[14] in 2016 held that *Shreya Singhal*[15]standard was only applicable to social media intermediaries and it would be sufficient if a specific notice or red flag raised by the owner of intellectual property right. *MySpace*[16] though is considered to be a landmark judgment in terms of definitive application of the provisions under section 79 of the IT Act to intellectual property violations held that the provisions must be construed in conformity with the copyright law of India, The Copyright Act, 1957. The division bench 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 the content. As a result of this judgment, the take down notice regime started in India, allowing IPR holders to take actions through take down notices without having the need to seek a court order. In *Kent RO,*[17] the High Court of Delhi reiterated the position that 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 the receipt of complaint. Further, to require an intermediary to do such *suo moto* screening would not be appropriate here as neither it was intented by the legislature nor they are possessed with the prowess to judge IP infringement, a technical question which even the courts struggle to decide according to the single judge.

The single judge judgment (dated November, 2 2018) in *Christian Louboutin SAS* v. *Nakul Bajaj*[18] raised the bar considerably for e-commerce-based intermediaries to claim exemption from liability in relation to any sale in violation of the provisions of Trade Marks Act, and 1999 has turned out to have far-reaching effects on intermediary liability jurisprudence in India. The appeal was filed by the plaintiff, a manufacturer of luxury shoes and handbags under the name of its founder, Christian Louboutin, a famous designer of high-end luxury products.

The plaintiff's alleged that the defendants, through their website *www.darveys.com*, offer for sale and sell various products on their website, bearing the luxury brands/names of the plaintiff with a claim that the products are 100% authentic. The plaintiff has alleged trade mark infringement against the defendant by *inter alia* selling goods that are counterfeit or impaired. The defendants also use the image of the founder of the plaintiff, and the names "*Christian*" and "*Louboutin"* are used as meta-tags on the defendant's website to attract internet traffic.

13 Deepa Kharb, "Cyber Law" *LIII ASIL (Indian Law Institute, 2017).*

14 2016 SCC OnLine Del 6382.

15 *Supra* note 12.

16 *Supra* note 14.

17 2017 SCC OnLine Del 7201.

18 2018 SCC OnLine Del 12215 decided on Nov 2, 2018.

The high court analysed the meaning of "intermediary" under the Information Technology Act and whether "every company which runs an e-commerce website automatically come under the definition of intermediary?

The court held that *Darveys.com* was not an intermediary. After an exhaustive discussion, it concluded that the role of the defendant's website was more than an intermediary as it was identifying the sellers, enabling the sellers actively, promoting them and selling the products in India. The court noted that the conduct of intermediaries, in failing to observe 'due diligence' with respect to intellectual property rights, could amount to 'conspiring, aiding, abetting or inducing' unlawful conduct would disqualify it from the safe harbour exemption, as per section 79(3)(a).

The court further held that when an e-commerce website is involved in or conducts its business in such a manner, which would see the presence of a large number of elements enumerated above, it could be said to cross the line from being an "intermediary" to an "active participant". In such a case, the platform or online marketplace could be liable for infringement in view of its active participation. So long as they are mere conduits or passive transmitters of the records or of the information, they continue to be intermediaries, but merely calling themselves as intermediaries does not qualify all e-commerce platforms or online market places as one.

The ruling introduced the concept of an 'active' marketplace and a 'passive' marketplace for the first time in India, and held that the safe harbour provision of the IT Act would only be available to a passive marketplace.[19] Listing out 26 services,[20] like providing logistics support services, product listing services, product review services, call centre assistance, payment gateway services, *etc.*, which if undertaken by a marketplace, could make it an active participant and therefore ineligible for the safe harbour exemptions granted under section 79 of the IT Act. Where preventive measures are undertaken by a marketplace to ensure that no unlawful acts are committed by the sellers on its marketplace and due diligence conducted by it on the sellers would also be considered while determining the applicability of the safe harbour provision.

Further, where an intermediary is charged with conspiring, aiding, abetting or inducing an unlawful act or authorizing communication of an unlawful act, the provisions of the law, the violation of which the intermediary has been charged with have to be seen *i.e.,* sections 101 and 102 of the Trade Marks Act,1999 here.

In the context of *Darveys.com*, therefore, the active use of its mark, displaying advertisements containing the mark, enclosing the goods with its own packaging and selling them onwards, would according to the court, amount to falsification and infringement under section 29 of the Trademark Act, 1999 and hence constitute aid, abetment or inducement under section 79 of the IT Act.

19 Marketplaces that are mere conduits or passive transmitters of records or information are passive marketplaces.

20 The court culled out 26 tasks which if performed (all/most of them), by online marketplace in course of their business and their failure to observe due diligence, would take them out the 'safe harbour' of s. 79 of IT Act, 2000 and render them active participant.

The court, then went on to examine the role played by the defendant's website *i.e., www.darveys.com* upon which the court observed that the website guarantees authenticity/genuineness of the products, facilitates the purchasing and sourcing of products from third party sellers and arranges for the transport of goods. In the warranty section, however, the website the website claims that warranty and exchange terms are provided by the respective boutiques/sellers which are located abroad and the products sold through the website are not subject to warranty or exchange policy of the respective manufacturers. No warranty is provided in respect of quality, tone, truth, unity of any data, matter, product or service. It also claims that sales are made directly by the boutiques and invoices raised are by the suppliers to the customers.

The prices of the products are maintained and changed at the discretion of *darveys.com*. In the shipping page, it claims that upon the boutique/seller forwarding the product to the shipping bearer, the title and risk for loss of any item is placed on the customer. This shows that even before the customer obtains the delivery of the product, the risk is passed on to the customer. The products are claimed to be checked by *darveys.com*. Surprisingly, the website does not have a list of boutiques/sellers from whom the website is sourcing the products.

The court took into account the legal position on intermediary liability in Europe and US. In *L'Oreal SA* v. *eBay International AG,*[21] CJEU held that for claiming immunity under article 14(1) of the EU Directive 2000/31, an online platform must serve/act as an intermediary. If the operator provides assistance, "*which entails, in particular, optimising the presentation of the offers for sale in question or promoting them",* even if the operator has not played an active role and if he provides the above service, the operator can claim protection as an intermediary. However, if the said intermediary on becoming aware of any counterfeit/potentially trademark infringing products being listed on its platform fails to act expediously, the immunity ceases to exist for such a platform. This decision aimed to reduce the width of safe harbour immunity by distinguishing between neutral and active roles, holding that the intermediary would be liable if it played an active role, such as assistance to the customers, including "optimising the presentation of the offers for sale in question or promoting those offers"

Relevant observations are as under:[22]

> 144. In view of the foregoing, the answer to the tenth question is that the third sentence of Article 11 of Directive 2004/48 must be interpreted as requiring the Member States to ensure that the national courts with jurisdiction in relation to the protection of intellectual property rights are able to order the operator of an online marketplace to take measures which contribute, not only to bringing to an end infringements of those rights by users of that marketplace, but also to preventing further infringements of that kind. Those injunctions must be effective, proportionate, dissuasive and must not create barriers to legitimate trade.

21 [2012] All E.R. (EC) 501.

22 *Ibid.*

Therefore, the national courts in the EU have to determine whether the role of the service provider is neutral or not. CJEU held that operators of online marketplaces have a duty not only to bring to an end infringement but also to prevent further infringement, ruling in favour of L'Oreal.

Referring to the "Inwood test" developed in respect of contributory trademark infringement in *Inwood Laboratories Inc.* v. *Ives Laboratories Inc*:[23]

> ...[i]f a manufacturer or distributor intentionally induces another to infringe a trademark, or if it continues to supply its product to one to whom it knows or has reason to know is engaging in trademark infringement, the manufacturer or distributor is contributorily responsible for any hard done as a result of the deceit.[24]

The court, therefore, held that the liability of a service provider like eBay could be only when it is informed of the infringement but ignores to take action.

The court observed that there is no uniformity in the manner in which the intermediaries have been treated in different jurisdictions. However, the underlying principles appear to be the same, in order to determine whether the intermediary is active or passive, negligent or compliant. Referring to the observations of the single judge in *Kent RO Systems*:[25]

> To hold that an intermediary, before posting any information on its computer resources is required to satisfy itself that the same does not infringe the intellectual property rights of any person, would amount to converting the intermediary into a body to determine whether there is any infringement of intellectual property rights or not. All persons claiming any intellectual property rights will then, intimate the intermediaries of their claims and the intermediaries then, before hosting any material on their computer resources would be required to test the material vis-a- vis all such claims lodged with them, else would be liable for infringement.

My reading of the IT Rules aforesaid obliges the intermediary to remove/disable the information hosted on the portal only on receipt of complaint. The IT Rules, according to me do not oblige the intermediary to, of its own, screen all information being hosted on its portal for infringement of the rights of all those persons who have at any point of time complained to the intermediary.[26]

On the basis of the above, the high court decreed the present suit by directing *Darveys.com* to inter alia disclose complete details of all its sellers, their addresses and contact details on its website with immediate effect, to obtain a certificate from its sellers that the goods are genuine, to notify the trademark owner before offering their products for sale (in case of sellers located outside India), to enter into an agreement with the sellers (in case of sellers based in India) guaranteeing the authenticity of the products and consequences of violation, and to remove all metatags consisting of plaintiff's mark.

23 456 U.S.844

24 *Ibid.*

25 2017(69) PTC 551(Del).

26 *Ibid.*

The views in the *Christian Louboutin* were upheld by the court in three other cases namely *Luxotica Group S.P.A.* v. *Mify Solutions Pvt Ltd.,*[27] *Skullcandy Inc* v. *Shri Shyam Telecom*[28] and *L'Oreal* v. *Brandworld*.[29]

In the case of *Luxottica Group S.P.A.* v. *M/s Mify Solutions Private ltd*,[30] the major issue in the case was to determine whether the online shopping market place, *www.kaunsa.com*, is an intermediary or not and if so, to what effect? Referring to the case of *Christian Louboutin SAS* v. *Nakul Bajaj*[31] with regard to the role of intermediaries and their liabilities, the Supreme Court discussed the protection of section 79 read section 2(w) and rule 3 of IT Rules, 2011. It held that the safe harbour provisions are for protecting intermediaries against unnecessary harassment, however, no intermediary is allowed to infringe IP rights. IP rights override the protection granted *via* section 79 of IT Act, 2000 to intermediaries. The judgment further recognised that stricter measures are needed for curbing sale of counterfeit products on online marketplaces holding the defendants liable for playing active role in the transaction-they guarantees that the products are authentic, offers warranties and guarantees on the product, payments are taken care of by the website. It accordingly held that in the facts as set out above, "*www.kaunsa.com*" is not an intermediary entitled to exemption under section 79 of the IT Act. As per the provisions of section 79 of the IT Act read with the Intermediary guidelines, the platform cannot be treated purely as an intermediary. Therefore, the defendants were held liable for infringing the trademark and copyright.

In the case of *L'Oréal* v. *Brandworld,*[32] the court observed that though the role of the website was shown to be that of an intermediary, several other features of the website point to the fact that *shopclues.com* is not merely an intermediary *e.g.,* website facilitating payment and allowing sellers to use its partners for logistical support, website guarantees genuineness of products *etc*. The REPLICA window on the website encourages sellers to post look alike products as the feature of the replica window would constitute aiding and abetment of violation of intellectual property. These factors, according to the court, disqualify *www.shopclues.com* for the exemption under section 79 of the IT Act, 2000 as the role of the website is more than that of an intermediary.

Similarly, in *SkullCandy Inc.* v. *Shri Shyam Telecom*[33] the court reiterated that before going further with the analysis, it is important to establish first that an online service provider comes under the ambit of section 2(w) of the IT Act, 2008 *i.e.,* it is an 'intermediary'. Once that is true then the next big question is whether the service provider is more than an intermediary or whether it followed the conditions for

27 2018 SCC OnLine Del 12307(decided on Nov. 12, 2018).

28 2018 SCC OnLine Del 12308 (decided on Nov. 12, 2018).

29 MANU/DE/4083/2018.

30 *Supra* note 26.

31 *Supra* note 18.

32 *Supra* note 28.

33 2018 SCC OnLine Del 12308.

exemption of liability *i.e.* whether the online service provider acted with "due diligence," and tried to remove content on notification from the rightful owner of the content or not.

However, court also took into account in these cases that online service providers cannot be made liable all the time and it depends from each case to case after analysing whether they had major control with them like in *Christian Louboutin*[34] and *Luxottica*[35] case.

Therefore, we have seen that despite the ruling of the Supreme Court of India in *Shreya Singhal,*[36] courts have distinguished the 'actual knowledge' requirement for matters of free speech from claims of IP infringement. In cases of IP, courts have operationalised the notice and takedown mechanism, wherein rights owners can request for infringing content to be taken off by intermediaries on intimating them of the infringement (the notice and takedown mechanism).

Though the Supreme Court's judgment in *Shreya Singhal*[37]clarified that intermediaries are not responsible for judging the legitimacy of content on their platforms, the last two years have seen litigation that involved intermediaries to act as content monitors. A number of petitions have been filed before different courts seeking to expand the scope of intermediaries' obligations with respect to user-generated content and these litigations to an extent have been successful in doing so. Courts in judgments like *Sabu Mathew George* v. *Union of India*[38] *and Re: Prajwala*[39] *etc* have been asking intermediaries to proactively filter their platforms for illegal content. Courts have imposed proactive content monitoring obligations on online intermediaries by blocking access to pornographic content. In other cases courts have ordered judgments or personal information to be removed from online repositories or search engine results recognising right to be forgotten arising from the right to privacy and right to reputation. Such decisions by courts brings back the confusion over the level of due diligence which is to be followed by intermediaries to protect their safe-harbour in cases involving. Some judgments from 2018 have been covered in this segment of survey where such attempts have been made at expanding the scope of intermediary liability.

On December 24, 2018, MeitY released the Draft Information Technology [Intermediaries Guidelines (Amendment) Rules], 2018 ("the Draft Rules") inviting comments to amend the existing Intermediaries Guidelines. Rule 3(9) of the Draft Rules requires intermediaries to deploy automated tools[40] for proactive filtering of unlawful content, takedown of illegal content within 24-hours among other things.

34 *Supra* note 18.

35 *Supra* note 29.

36 *Supra* note 12.

37 *Ibid.*

38 2017 SCC OnLine SC 1545.

39 MANU/SCOR/45933/2017.

40 Automated moderation systems that are in use today rely on keyword tagging which is then followed by human review.

IV BLOCKING OF WEBSITES-SECTION 69A IT ACT

In *Re: In the Matter of Incidence of Gang Rape in a Boarding School, situated in Bhauwala, District Dehradun* v. *State of Uttarakhand*[41] the high court directed implementation regarding the ban on pornographic websites, non-compliance of which will lead to suspension of licenses of internet service license holders.

The court took *suo motu* cognizance of the news reports pertaining to the gang rape of a minor girl in a boarding school in Dehradun where the accused boys watched a pornographic movie before sexually assaulting the minor girl. In the said incidence, FIRs were registered and the four accused were charged under section 376 and 201 of the IPC and POCSO Act, 2012. The court noted that the Ministry of Communication and Information Technology, Department of Telecommunications, Government of India, in July 2015, had issued a notification banning pornographic websites. Observing the absence of implementation of the directions on the notification, the court issued following directives:

i. Directions shall be issued to all the Internet Service License Holders to punctually obey the Notification dated 31st July, 2015 and to block the transmission or publication of obscene material in any electronic form, transmitting of material containing sexually explicit conduct or act and also transmitting or publishing of material depicting children in sexually explicit conduct or act forthwith.

ii. In case of non-compliance with the said 2015 notification, suspension of licenses of of the Internet Service License Holders under Section 25 of the Information Technology Act, 2000.

In another case of *Facebook* v. *State of West Bengal*[42] an order was passed by *Chief Metropolitan Magistrate* (CMM) in 2017 issuing directions to the petitioner to remove the entire Facebook pages available at, "The Darjeeling Chronicle". Pursuant to that order of the learned CMM, a notice was sent by the local police under section 91 Cr PC on June 19, 2007 asking the petitioner to immediately block and remove the relevant pages.

The petitioner challenged the said order as well as the action of the local police on following grounds:-

(i) That the impugned order was passed by the CMM mechanically, without any application of mind.

(ii) The said order was beyond the jurisdiction of the said court in view of Rule 10 of Information Technology Rules, 2009.

(iii) That the CMM has acted without adhering to the relevant sections 177 to 184 Cr PC which deals with the jurisdiction of a criminal court,

(iv) That the learned trial court ought to have considered sections 95 and 96 Cr PC, since it is a special statue.

(v) Relevant rules *i.e.,* IT (Procedures and Safeguards for blocking for access to information by public) rules were not complied with.

41 2018 SCC OnLine Utt 871 (decided on Sep. 27, 2018).

42 2018 SCC OnLine Cal 2, (decided on Jan. 3, 2018).

The court was therefore, under an obligation to see whether the procedural aspects have been complied with or not. On perusal of the order, the High Court of Calcutta found that there was no registration of FIR at the behest of the investigation officer as required under Rule 10 of Information and Technology Rules, 2009. The advocate general extended justification for the prosecution on the ground of reasonable apprehension of other turbulent activities in that area.

Counsel appearing on behalf of the petitioner contended that the provisions laid down in Information and Technology (procedure and safeguards for blocking for access of information by public) Rules 2009 have not been complied with. According to him, it ought to have been routed through by the designated officer.[43] Section 69A of the IT Act mandates creation of a nodal agency by the state government to handle such complaints. The agency needs to send its observation to CERT-In after going through the complaint. The CERT-In then needs to send a directive to the company or the owner of the website with a plea to block the page. However, none of these above stated procedures were followed in this case.

The high court observed that the rules were very specific on this count. On a conjoint reading of rule 5 and rule 6 it appears that the designated officer upon a request from the nodal officer of an organisation or a competent court by order direct any agency of the government or intermediary to block for access by the public any information. The said rules of 2009 also speak that even if any information other than the one from the nodal officer of the organisation is received, shall be sent with the approval of the chief secretary of the state to the appropriate authority for blocking of access. However, in this case those procedures and those rules were not complied with at all, observed the high court.

43 Information and Technology Rules, 2009, r. 3: The Central Government shall designate by notification in Official Gazette, an officer of the Central Government not below the rank of a Joint Secretary, as the "Designated Officer", for the purpose of issuing direction for blocking for access by the public any information generated, transmitted, received, stored or hosted in any computer resource under ss. (2) of s. 69A of the Act.

R. 4: Every organization for the purpose of these rules, shall designate one of its officer as the Nodal Officer and shall intimate the same to the Central Government in the Department of Information Technology under the Ministry of Communications and Information Technology, Government of India and also publish the name of the said Nodal Officer on their website.

R. 5: Direction by Designated Officer-The Designated Officer may, on receipt of any request from the Nodal Officer of an organization or a competent court, by order direct any Agency of the Government or intermediary to block for access by the public any information or part thereof generated, transmitted, received, stored or hosted in any computer resource for any of the reasons specified in ss. (1) of s. 69A of the Act.

R. 6. Forwarding of request by organisation-

(1) Any person may send their complaint to the Nodal Officer of the concerned organisation for blocking of access by the public any information generated, transmitted, received, stored or hosted in any computer resource:

Provided that any request, other than the one from the Nodal Officer of the organisation, shall be sent with the approval of the Chief Secretary of the concerned State or Union territory to the Designated Officer.

Provided further that in case a Union territory has no Chief Secretary, then, such request may be approved by the Adviser to the Administrator of that Union territory.

Exigencies were pleaded by the advocate general submitting that situation was of such a nature for which the blocking of access to those pages was the need of the hour. High court found that on a careful reading of section 69A (1), it appears that to prevent incitement to the commission of any cognizable offence an officer specially authorized can invoke the said rules and the officer-in-charge of a police station is bound to register the same. This is a mandatory requirement and not optional. Here no FIR was lodged and for taking action under section 69A of the Act, FIR is mandatory. The Act, read with the relevant rules does not say that the court is authorized to do it. The court assumes its jurisdiction only in terms of Rule 5 and Rule 10 of the Information Technology (Procedure and Safeguards for Blocking for Access to Information by Public) Rules, 2009. Therefore, a court cannot assume these responsibilities since the IT Act 2000 is a complete code in itself.

The court therefore ruled that the chief metropolitan magistrate has passed the order on a wrong premise without applying his mind, nor considered the scope of application of the IT Act and relevant rules. Accordingly, the impugned order was set aside.

Geoblocking

The position in India, insofar geo-blocking and global injunctions is concerned, is not fully settled. In *You Tube* v. *Geeta Shroff* [44] single judge of this court was dealing with an offensive post, which was only removed from the India domain and not from global platforms.

The appeal here was filed due to non-compliance of the injunction order passed in 2015 by the trial court, directing the appellant to remove the offensive post with the tagline "*Indian Money Hungry Dr Geeta Shroff Must Watch",* damaging the fair name of the respondent. The appellant contended that the post was uploaded from outside India. According to the appellant, they were constrained from complying with the impugned directions to disclose the identity of the uploader unless they were directed to do so by an American Court as per the SPEECH Act, 2010 (US statute) or seek diplomatic procedures such as the Hague Evidence Convention, 1970. Further, the appellant submitted that compliance with the injunction order was not possible due to technological reasons.

In this context, the appellant submitted that the orders of the Indian court cannot be given effect to because the video linked on Youtube was not uploaded from India and the SPEECH Act constrains the appellant from disclosing such information. He cited before the court the case of *Google LLC* v. *Equustek Solutions Inc.*[45] where the Supreme Court of Canada ordered Google to remove content globally. The order of the Canadian Supreme Court was stayed by the District Court of California. With reference to the SPEECH Act, the American Court held:[46]

> ..... [T]he Canadian order would eliminate Section 230 immunity for service providers that link to third-party websites. By forcing

44 2018 SCC OnLine Del 9439, (decided on May 17, 2018).

45 [2017] 1 S.C.R. 824 (Can.).

46 *Ibid.*

> intermediaries to remove links to third-party material, the Canadian order undermines the policy goals of Section 230 and threatens free speech on the global internet.....

The court thereafter, observed that the interim order dated June 4, 2015 recorded, in effect, that the appellant had not specifically disputed that the offending post was posted from India. Since the said order was not challenged, it has, therefore, attained finality. Thus accordingly, the appellants were required to comply with it.

In fact, the court observed that even if the post was uploaded from outside India, the same ought to have been disclosed to the court at the initial stage and not after the interim order had attained finality. Thus, the appeal of Google was dismissed as withdrawn. The appellant was also directed to pay Rs 50,000 per hearing as costs. The said order dated May 17, 2018 was challenged before the Supreme Court. which was dismissed as withdrawn on October 26, 2018. Thus, this judgment in *Geeta Shroff,*[47] resulted in global blocking of the offending content, initiating a new concept in India.

Recently a case[48] was filed before the High Court of Delhi seeking a global injuction. This is in continuation of an order passed against *Juggernaut Books Pvt. Ltd.,* (CM (M) 556/2018) by the High Court of Delhi September 2018, where publisher and author were restrained from publishing, distributing and selling the book 'Godman to Tycoon - The Untold Story of Ramdev' without deleting the offending defamatory portions. The petition was filed as fresh case against Facebook, Google, Twitter, YouTube *etc.* to restrain the publication of videos and content based on the contents of the book/summanising the book. In the coming days we can expect another judgement on geo blocking.

V SECTION 65 B-ADMISSIBILITY OF ELECTRONIC EVIDENCE

The jurisprudence over mode and manner of admissibility of electronic evidence or records during the course of trial continues to remain uncertain.

Though the Supreme Court ruling in *Anwar*[49] and later cases clearly and unequivocally stated that any electronic evidence in secondary form filed without meeting the requirements of section 65B (4) will be inadmissible, in 2017, two judge bench in *Sonu* v. *State of Haryana*[50] has expressed doubts over this principle. The bench noted that the law laid in *Anwar*[51] judgment has not clarified whether the judgment is to be applied prospectively or retrospectively also. Since this question has been left open in *Anwar*[52] decision, it will be used to reopen or challenge the admissibility of evidence in pending trials where the requirements under section 65B were not complied with according to the bench. The court in *Sonu*[53] case held the requirements of section 65B to be relating to method of/mode of proof (objection to

47 *Supra* note 44.

48 *Swami Ramdev* v. *Facebook,* CS(OS) 27/2019.

49 *Supra* note 1 at 473.

50 (2017) 8 SCC 570.

51 *Supra* note 49.

52 *Ibid.*

53 *Supra* note 50.

which cannot be raised at appellate stage) despite *Anwar* holding that non-compliance with section 65B strikes at the very admissibility of the evidence.[54] This decision by a two judge bench cannot overrule larger bench decision but these observations will definitely affect and delay all other pending trials and appeals across the country.[55]

Earlier too this case in *Abdul Rahaman Kunji* v. *State of W.B,*[56] a Division Bench of Calcutta High Court, while deciding the admissibility of e-mail, held that an e-mail downloaded and printed from the e-mail account of the person can be proved by virtue of section 65b read with section 88A of the IEA. The oral testimony of the witness who had downloaded and printed the said mails is sufficient to prove the electronic communication even in absence of a certificate in terms of section 65 B of the IEA.[57]

In *Suhas Mahadev Roge* v. *State of Maharashtra*[58] an application was filed for bail during the pendency of appeal. The prosecution case rested entirely on circumstantial evidence since none of the eyewitnesses supported the case. The trial judge had relied on call detail records (CDRs) for conviction, relying upon the case of *State (NCT of Delhi)* v. *Navjot Sandhu,*[59] the law existing on that date. However, subsequently the *Anwar* ruling came requiring a certificate issued by the competent authority under section 65B of Evidence Act, 1872 for relying on the evidence. The question before the high court was whether in the light of *Sonu* judgment the admissibility of CDRs without section 65B certificate can be raised at appellant stage or going by the observation of two judge bench in *Sonu,* the *Anwar* mandate cannot be applied retrospectively? The high court referred to excerpts from *Sonu* case wherein the two lordships observed:[60]

> …There is no doubt that the judgment of this Court in *Anvar's* case has to be retrospective in operation unless the judicial tool of 'prospective overruling' is applied. However, retrospective application of the judgment is not in the interests of administration of justice as it would necessitate the reopening of a large number of criminal cases. Criminal cases decided on the basis of electronic records adduced in evidence without certification have to be revisited as and when objections are taken by the Accused at the appellate stage…….

Therefore according to the high court the CDRs could not be taken into consideration at appellate stage and only if *Anwar* law is changed in near future, the said evidence can be taken into consideration. The *Anwar* ruling was further diluted

54 Anuj Beri, Sonali Malik *et al.,* India: Supreme Court On Admissibility Of Electronic Records As Secondary Evidence, *available at:* http://www.mondaq.com/india/x/614920/trials+appeals+compensation/Supreme+Court+on+Admissibility+of+Electronic+ Records+as+Secondary+evidence (last visited on Dec. 23, 2018).

55 *Ibid.*

56 2014 SCC OnLine Cal 18816; See also *Ram Kishan Fauji* v. *State of Haryana* 2015 SCC OnLine P and H 5058.

57 *Ibid.*

58 2018 SCC Online Bom 3398.

59 (1980) 2 SCC 559.

60 *Supra* note 48 at para 37.

by its interim order in *Shafi Mohhammad* v. *State of Himachal Pradesh*[61] in 2018 wherein it observed that that a party, who is not in the possession of a device which has produced an electronic document, cannot be required to produce a certificate under section 65B of Evidence Act, 1872. The court further held that the requirement of producing a certificate under section 65B can be relaxed in the interest of justice by the court.

The key issue that was considered was:

i. whether a video recording of the scene of crime during investigation should be necessary to inspire confidence in the evidence collected and in the given context;

ii. what would be the scope of applicability of the procedural requirements under Section 65(B)(4) of the Act for furnishing a certificate in case of electronic evidence produced by a person not in custody of the device generating such evidence?

During the course of hearing in the case apprehension was expressed on the question of applicability of conditions under section 65B(4) of the Evidence Act,1872 to the effect that if a statement was given in evidence, a certificate was required in terms of the said provision from a person occupying a responsible position in relation to operation of the relevant device or the management of relevant activities.

It was submitted that if the electronic evidence was relevant and produced by a person who was not in custody of the device from which the electronic document was generated, requirement of such certificate could not be mandatory. Diluting the ratio of *Anwar*[62] ruling further it held that electronic evidence is admissible under the Act. Section 65A and 65B are merely clarificatory and procedural in nature and cannot be held to be a complete code on the subject.

The court observed that it will be wrong to deny to the law of evidence advantages to be gained by new techniques and new devices, provided the accuracy of the recording can be proved. Such evidence should always be regarded with some caution and assessed in the light of all the circumstances of each case.

The bench also made reference to the case of *Tomaso Bruno* v. *State of Uttar Pradesh*[63] that observed that advancement of information technology and scientific temper must pervade the method of investigation. Electronic evidence was relevant to establish facts. Scientific and electronic evidence can be a great help to an investigating agency.

That if the electronic evidence is authentic and relevant the same can certainly be admitted subject to the court being satisfied about its authenticity and procedure for its admissibility may depend on fact situation such as whether the person producing such evidence is in a position to furnish certificate under section 65B (h).

That the applicability of procedural requirement under section 65B(4) of the Evidence Act, 1872 of furnishing certificate is to be applied only when such electronic evidence is produced by a person who is in a position to produce such certificate being in control of the said device and not of the opposite party. In a case where

61 (2018) 5 SCC 311, decided on April 3, 2018.

62 *Supra* note 49.

63 2015 SCC On Line SC 52.

electronic evidence is produced by a party who is not in possession of a device, applicability of sections 63 and 65 of the Evidence Act, 1872 cannot be held to be excluded. That it will be denial of justice to not permit a person who is in possession of authentic evidence/witness but on account of manner of proving, such document is kept out of consideration by the court in absence of certificate under section 65B(4) of the Evidence Act , which party producing cannot possibly secure. Thus, requirement of certificate under section 65B(h) is not always mandatory.

Court tried to clarify legal position on the subject on the admissibility of the electronic evidence, especially by a party who is not in possession of device from which the document is produced. Such party, according to the court, cannot be required to produce certificate under section 65B(4) of the Evidence Act, 1872 .That the applicability of requirement of certificate being procedural can be relaxed by court wherever interest of justice so justifies.

This interim decision seems to have restricted the applicability of the statutory certificate required under 65B(4) of the Act or may have carved out an exception to applicability thereof.[64] This judgment may provide sanctity to considerably significant evidence that was earlier not taken into account in view of being procedurally uncertified in accordance with section 65B(4) of the Act. It will be interesting to observe how the other court(s) interpret the view taken by the apex court.[65]

It is being argued by some that this interim decision by a two judges bench in a SLP although cannot technically overrule a three judge bench decision of 2014 but will facilitate production of false evidence and change the onus of proving that it is inadmissible on the defense.[66] The *Anwar* judgement had clearly segregated 'admissibility' from 'genuineness' and had indicated how the two should be handled by the court. The current order has completely ignored this part of the *Anwar* judgement and is not a correct interpretation. In future, reliance on electronic records during investigation is bound to increase. The law therefore needs to be laid down in this regard with certainty.

However, judges of the different high courts and trial courts continued reliance upon the ratio of the *Anwar*[67] judgment in matters related to admissibility of electronic evidence before the coming of *Shafhi*[68] ruling in the month April 2018. In *ICICI Bank*

64 Rajiv Shanker Bhatnagar *et al*., Supreme Court Elucidates upon the Scope and Necessity of Certificate under section 65B of the Indian Evidence Act, 1872, *available at:* http://www.mondaq.com/india/x/677072/trials+appeals+compensation/Supreme+Court+ Elucidates+Upon+The+Scope+Necessity+Of+Certificate+Under+Section+65B+Of+The+Indian+Evidence+Act+1872 and https://www.khaitanco.com/PublicationsDocs/Khaitan%20&%20Co-Ergo-Update-23Feb2018RB.pdf?cv=1(last visited on Oct. 23,2018)

65 *Ibid.*

66 Vijayashankar Na, Recipe for corruption in Judiciary- Supreme Court judgement in *Shafhi Mohammad* v. *State of Himachal Pradesh, available at:* https://www.naavi.org/wp/recipe-for-corruption-in-judiciary-supreme-court-judgement-in-shafhi-mohammad-v-state-of-himachal-pradesh/ (last visited on Oct. 24,2018)

67 *Supra* note 49.

68 *Shafhi Mohhammad* v. *State of Himachal Pradesh supra* note 61.

Limited v. *Kamini Sharma*[69] the High Court of Delhi observed that the plaintiff bank has filed the certificate under section 65B through its witness and also certified all the copies of electronic records including bank statements etc., thus the requirements under section 65B have been fulfilled.

There is however some serious re-thinking required on the manner in which electronic documents are to be proved, observed the court. Certificates under section 65B accompanying the printouts have simply become standard formats. Cross examination on these certificates can involve debates on model of computer, printer, questions as to who took printouts *etc.* Courts, therefore, need to take a pragmatic attitude in these cases. Unless there is a serious challenge to the electronic documents *i.e.,* tampering, forgery, hacking, misuse of an email address, change in contents *etc.*, usually printouts of electronic documents ought to be allowed to be read in evidence. The complex procedure laid down for proving of electronic documents can prove to be extremely cumbersome and can have enormous impact especially in commercial transactions. It observed that:[70]

> Section 34 of the Evidence Act clearly provides that the books of accounts maintained in electronic form are relevant. Under Section 62 of the Evidence Act, original documents constitute primary evidence. In the context of electronic evidence, printouts of electronic documents are considered as secondary. However, judicial notice needs to be taken of the fact that most accounts today are not maintained in paper form, but electronic form. The primary evidence could be the server on which the statement of accounts is stored. These servers may store the statement of accounts of multiple clients in the hard drive. It would be an impossibility to require the Plaintiff bank to produce the hard drive of the server in every suit for recovery filed by it. Under such circumstances, the Plaintiff bank has no option but to produce the secondary evidence i.e., a printout of statement of accounts, duly certified by a responsible official of the bank along with a certificate under Section 65B of the Evidence Act. Needless to add, the certificate under Section 65B of the Evidence Act has now become a usual practice in almost all of the suits, inasmuch as, in every such suit, parties are bound to place reliance on electronic documents. The mere fact, that the printout is being filed as secondary evidence along with the necessary certificate, does not make it any less valid. The said accounts statement would be rebuttable if any discrepancy is found or pointed out. But in the absence of the same, there is no reason as to why the statement of accounts filed by the Plaintiff bank should be disbelieved.[71]

69 2018 SCC OnLine Del 6933; Also in *ICICI Bank Limited* v. *Kapil Dev Sharma* 2018 SCC OnLine Del 6946; *ICICI Bank Limited* v. *Sunil Sharma* 2018 SCC OnLine Del 6948; *ICICI Bank Limited* v. *Surbhi Gupta* 2018 SCC OnLine Del 6949; *ICICI Bank Limited* v. *Vinod* 2018 SCC OnLine Del 6947 (decided on Jan. 31, 2018).

70 *Supra* note 69.

71 *Anvar P.V.* v. *P.K. Basheer, supra* note 49.

The court referred to relevant parts of the *Anwar* judgment:[72]

> The evidence relating to electronic record, as noted herein before, 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 special bus non derogant*, special law will always prevail over the general law. It appears, the court omitted to take note of Sections 59 and 65A 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 65A and 65B. To that extent, the statement of law on admissibility of secondary evidence pertaining to electronic record, as stated by this Court in *Navjot Sandhu* case (supra), 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 65B are satisfied. Thus, in the case of CD, VCD, chip, etc., the same shall be accompanied by the certificate in terms of Section 65B obtained at the time of taking the document, without which, the secondary evidence pertaining to that electronic record, is inadmissible.

Further in *ELI Lilly* v. *Maiden Pharmaceuticals* where the Delhi High Court held that the plaintiffs are entitled to file the certificate under Section 65-B of the Evidence Act, even subsequent to the filing of the electronic record in the Court. Order XI Rule 6 of CPC as applicable to commercial suits is also not found to provide to the contrary.

This trend shifted after the coming of *Shafhi*[73] judgment. The High Court of Delhi in *ICICI Bank Limited* v. *Umesh Rai*[74] and some other cases[75] held that in the light of recent judgment, the requirements under section 65B are relaxable:[76]

> Sections 65-A and 65-B of the Evidence Act, 1872 cannot be held to be a complete code on the subject. In *Anvar P.V*. v. *Basheer*, this Court in para 24 clarified that primary evidence of electronic record was not covered under Sections 65-A and 65-B of the Evidence Act. Primary evidence is the document produced before the Court and the expression "document" is defined in Section 3 of the Evidence Act to mean any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter.

72 *Ibid.*

73 *Shafi Mohhammad supra* note 61.

74 2018 SCC OnLine Del 9540.

75 *ICICI Bank Limited* v. *Ashok Sharma* 2018 SCC OnLine Del 9541; *ICICI Bank Limited* v. *Gaurav* 2018 SCC OnLine Del 9539; *ICICI Bank Limited* v. *Shyam Sunder Sharma* 2018 SCC OnLine Del 9544.

76 *Shafhi Mohammad, supra* note 61.

> The applicability of procedural requirement under Section 65-B(4) of the Evidence Act of furnishing certificate is to be applied only when such electronic evidence is produced by a person who is in a position to produce such certificate being in control of the said device and not of the opposite party. In a case where electronic evidence is produced by a party who is not in possession of a device, applicability of Sections 63 and 65 of the Evidence Act cannot be held to be excluded. In such case, procedure under the said sections can certainly be invoked. If this is not so permitted, it will be denial of justice to the person who is in possession of authentic evidence/witness but on account of manner of proving, such document is kept out of consideration by the court in the absence of certificate under Section 65-B(4) of the Evidence Act, which party producing cannot possibly secure. Thus, requirement of certificate is not always mandatory.
>
> Accordingly, we clarify the legal position on the subject on the admissibility of the electronic evidence, especially by a party who is not in possession of device from which the document is produced. Such party cannot be required to produce certificate under Section 65-B(4) of the Evidence Act. The applicability of requirement of certificate being procedural can be relaxed by the court wherever interest of justice so justifies."[77]

In *Victor Chigozie Ezurike and Caleb Mezie Ogbuagu* v. *State of Maharashtra*[78] case also it was found that the prosecution while filing the charge-sheet has not followed proper procedure and the said internet data is not supported by the certificate issued under section 65(B) of Evidence Act, 1872.

In *Sunil Singla* v. *State of Maharashtra,*[79] a case based on the charges of receiving illegal gratification involved an electronic evidence of recordings of the conversation between accused nos. 1, 2, 3 and 4.It was contended by the accused/defendant that there was no certificate as per requirements of section 65B(4) of Evidence Act, 1872. The purported certificate relied upon by the prosecution do not provide details as to the source from which compact disc (CD) containing the conversation was generated. The certificate only talks of a system used to record voice, but it does not certify that the contents of CD was actually the conversation which was transferred from computer containing the system for capturing voice to the CD such conversation has no evidentiary value. The High Court of Bombay observed that there was sufficient prima facie independent evidence against the applicant showing their involvement and *Central Bureau of Investigation* (CBI) has filed certificate at D-7 and thereby complied the condition prescribed under section 65B(4) of the Evidence Act. Hence the ordered that no case for granting relief prayed in this application is made out in the said case.

77 *Id.* at 22.

78 2018 SCC OnLine Bom 6150.

79 2018 SCC OnLine Bom 10093.

80 (2018) 4 BC 483

In *HDFC Bank Ltd.* v. *Suhrit Services Pvt. Ltd.* [80] according to the High Court of Delhi, trial court took an over-technical approach in this matter by holding that in view of the defects in the certificate under Section 65B of the Evidence Act, the suit is liable to be dismissed. Referring to the diverse judicial interpretations on section 65B given by the Supreme Court in *Anwar*[81] and *Shafhi*[82] and high courts in *ICICI* v. *Kamini Sharma,*[83]*Eli Lily* v. *Maiden Pharmaceuticals,*[84] it decided to go with the Supreme Court ruling in *Shafhi Mohammad* v. *State of Himachal Pradesh*[85] that the requirement of section 65B of the Evidence Act is not always mandatory and that requirement of the said certificate, which is a procedural requirement, can be relaxed by courts in the interest of justice. It held that the applicability of procedural requirement under section 65B(4) of the Evidence Act of furnishing certificate is to be applied only when such electronics evidence is produced by a person who is in a position to produce such certificate being in control of the said device and not of the opposite party. In a case where electronic evidence is produced by a party who is not in possession of a device, applicability of Sections 63 and 65 of the Evidence Act cannot be held to be excluded. In this case has to be held that the plaintiffs are entitled to file the certificate under section 65-B of the Evidence Act, even subsequent to the filing of the electronic record in the court. Order XI Rule 6 of CPC as applicable to commercial suits is also not found to provide to the contrary. Quoting the Supreme Court from *Shafhi*:[86]

> The applicability of procedural requirement under Section 65B(4) of the Evidence Act of furnishing certificate is to be applied only when such electronics evidence is produced by a person who is in a position to produce such certificate being in control of the said device and not of the opposite party. In a case where electronic evidence is produced by a party who is not in possession of a device, applicability of Sections 63 and 65 of the Evidence Act cannot be held to be excluded. In such case, procedure under the said Sections can certainly be invoked. If this is not so permitted, it will be denial of justice to the person who is in possession of authentic evidence/witness but on account of manner of proving, such document is kept out of consideration by the court in absence of certificate under Section 65B(4) of the Evidence Act, which party producing cannot possibly secure. Thus, requirement of certificate under Section 65B(h) is not always mandatory.
>
> Accordingly, we clarify the legal position on the subject on the admissibility of the electronic evidence, especially by a party who is not in possession of device from which the document is produced. Such party cannot be required to produce certificate under Section

81 *Anvar, supra* note 49.

82 *Shafi Mohhammad* , *supra* note 61.

83 *ICICI Bank Limited* v. *Kamini Sharma, supra* note 67.

84 2016 SCC OnLine Del. 5921.

85 *Shafi Mohhammad*, *supra* note 61.

86 *Ibid.*

> 65B(4) of the Evidence Act. The applicability of requirement of certificate being procedural can be relaxed by Court wherever interest of justice so justifies."[87]

In *Ajinkya Suhas Kshirsagar* v. *State of Maharashtra*[88] the learned trial court judge had disbelieved the detailed suicide note of the deceased, wife of the accused in the laptop in the file named "sorry" on the ground that there was no certificate available under section 65B of the Indian Evidence Act. The High Court of Bombay of the view that if the hard-disk was very much available and which was immediately seized after the incident had taken place, the learned trial judge could have viewed the file from the hard-disk only as no certificate was required. Therefore the high court granted bail to the accused and the sentence was suspended

Similarly in *M/s. ICICI Bank Limited* v. *Umesh Rai* [89] the High Court of Delhi observed that the requirements under section 65B are relaxable. In the present case, the Plaintiff bank filed the certificate under section 65B of the Evidence Act through its witness and also certified all the copies of electronic records including bank statements etc., The statement of accounts is duly accompanied by a certificate under section 65B of the Evidence Act. The witness of the Plaintiff bank PW-1 has appeared before the court and has tendered his evidence. There is no reason to disbelieve his deposition and the requirements under section 65B of the Evidence Act have been fulfilled.

Referring to *Kamini Sharma,*[90] where the High Court of Delhi analysed the manner in which section 65B of the Evidence Act needs to be applied considering the judgements of the Supreme Court in *Anvar*,[91] and *Harpal Singh* v. *State of Punjab*.[92] Recently, the Supreme Court also held in *Shafhi Mohammad* v. *State of Himachal Pradesh:*[93]

> "26. Sections 65-A and 65-B of the Evidence Act, 1872 cannot be held to be a complete code on the subject. In *Anvar P.V. v. Basheer*, this Court in para 24 clarified that primary evidence of electronic record was not covered under Sections 65-A and 65-B of the Evidence Act. Primary evidence is the document produced before the Court and the expression "document" is defined in Section 3 of the Evidence Act to mean any matter expressed or described upon any substance by means of letters, figures or marks, or by more than one of those means, intended to be used, or which may be used, for the purpose of recording that matter.[94]

87 *Ibid.*

88 2018 SCC OnLine Bom 2255

89 2018 SCC OnLine Del 9540*;* High Court of Delhi in *ICICI Bank Limited* v. *Gaurav* 2018 SCC OnLine Del 9539 also held that the requirements of s. 65B are relaxable in the light of *Shafhi Mohammad* v. *State of Himachal Pradesh supra* note 59.

90 *ICICI Bank Ltd*. v. *Kamini Sharma, supra* note 67.

91 *Supra* note 49.

92 (2017) 1 SCC 734 : AIR 2016 SC 5389

93 *Supra* note 61.

94 *Ibid.*

In this case the suit has been dismissed by adopting an over-technical approach even on Section 65B of the Evidence Act. The printout was filed as secondary evidence along with the necessary certificate, does not make it any less valid.

In *State* v. *Jaideep,*[95] a case involving offences punishable under section 364-A/ 120-B, the prosecution placed on record the intercepted recorded voice of accused and Call Detail Records(CDRs), which was rejected by the trial court for want of certificate under section 65-B of the Evidence Act, placing reliance on the case of the *Anvar.*[96] The findings arrived at by the trial court were found by the High Court of Delhi to be in consonance with the settled law in *Anwar* and the recent case of *Sonu* v. *State of Haryana*:[97]

> Electronic records play a crucial role in criminal investigations and prosecutions. The contents of electronic records may be proved in accordance with the provisions contained in Section 65B of the Evidence Act. Interpreting section 65B(4), this Court in *Anvar's* case held that an electronic record is inadmissible in evidence without the certification as provided therein. *Navjot Sandhu's* case which took the opposite view was overruled.[98]

VI OBSCENITY

In an interesting case, posting of a smiling emoji with teams in response to a video footage on an official WhatsApp group lead to a complaint under several provisions including section 67 of the IT Act. In *I. Linga Bhaskar* v. *The State,*[99] a case was registered for offences punishable under section 4 of Tamil Nadu Prohibition of Harassment of Women Act, 2002, section 3 (1)(r), 3(1)(t), 3(1)(u) of Scheduled Caste and Scheduled Tribes (Prevention of Atrocities) Amendment Act, 2015 and section 67 of IT Act for posting video footage of three customers who have spoken about their grievance about the BSNL coverage. Due to the posting of crying smiley faces against the second respondent, she was put to mental agony and therefore the case.

The court observed that on a careful reading of section 67 of IT Act, it can be seen that the said provision only prohibits publication of information that is obscene in electronic form. The prohibition against the obscenity as contemplated under section 67 of the IT Act in public interest is violated only when a person publishes or transmits any material which is lascivious or appeals to prurient interest or if its effect is such as to tend to deprave and corrupt persons who are likely to read, see or hear the matter contained in those materials.

The court held that an emoji is sent to express ones feeling about something, it cannot be turned as an overt act on others. It is a comment that may be intended to ridicule or to show ones disapproval in a given content. Such emojis would not hit section 67 of the IT Act. In this case, certainly, the allegations do not indicate any

95 2018 SCC OnLine Del 13290; *State Of Karnataka* v. *A.R. Ranganatha*

96 *Supra* note 49.

97 (2017) 8 SCC 570.

98 *Ibid.*

99 MANU/TN/2474/2018 (Decided June 5, 2018).

publication of obscene material which is lascivious or appeals to prurient interest. The object of section 67 of IT Act is, therefore, about a publication revealing an overt sexual interest or desire or encouraging an excessive interest in sexual matters. Hence, this court is of the clear opinion that the complaint does not disclose an offence under section 67 of the IT Act.

VII COPYRIGHT-PROTECTED SYSTEM AND GOVERNMENT WORK

The declaration of a computer resource as a protected system confers a higher level of protection under sections 66F, 70 and 70A of the IT Act. Lack of ownership over the critical infrastructure can have serious consequences. Supreme Court in *B.N. Firos* v. *State of Kerala*[100] dismissed the appeal of a computer firm challenging a Kerala notification declaring its computer system and network as "protected systems" under the Information Technology Act. The firm had also questioned the constitutional validity of section 70 of the Act alleging that it granted excessive delegation of power to the authorities.

In the year 1999, the Government of Kerala along with Centre for Development of Imaging Technology (C-DIT), Thiruvananthapuram launched project 'FRIENDS'(*i.e.,* Fast, Reliable Instant, Efficient, Network for Disbursement of Services) to provide a single window for bill collection. Microsoft Corporation, the world-renowned technology company, offered to develop the software for the Government of Kerala without any consideration.

The controversy, in this case, arose when the appellant, contending copyright in the source code (literary work) found out that the C-DIT were transferring essential rights to a third party which was a breach of contract according to the appellants. He also filed an application to register his copyright. Microsoft Corporation, however, filed criminal as well as civil suits against the appellants and prevented him from registering his copyright in respect to the 'disputed computer system'.

On the other hand C-DIT filed a suit before District Court Thiruvananthapuram seeking a declaration that it was the exclusive owner of the copyright and the sole owner of the Intellectual Property Rights of the FRIENDS application software. It also instituted a criminal case against the appellant for infringement of the application software. In the meanwhile, the state government issued a notification under section 70(1) of the IT Act, to designate the FRIENDS system as a protected system.

The notification was challenged by the appellant before the High Court of Kerala by way of a writ. *Firstly*, the appellant contended that section 70 itself was *ultra vires* because of excessive delegation of legislative powers under the section, which would violate article 14 of the Constitution. *Secondly*, the appellant claimed that the notification violated section 17 of the Copyright Act, 1957 which granted the copyright and the rights to use the software to the appellant.

The high court dismissed the challenge to the constitutionality of section 70(1). The single judge hearing the petition dismissed it. It held that the intellectual property rights in the software vested in the state government so as to entitle it to declare the

100 (2018) 9 SCC 220.

same as a "protected system". According to the high court, if the said provisions are to be read and construed harmoniously the power of declaration of a "protected system" would be only in respect of "Government work", the copyright in which of the government is acknowledged by section 17(d) of the Copyright Act, 1957. According to the high court, the government cannot unilaterally declare any system as protected system other than the work falling under the category of 'government work'.

High court noted that the registration of copyright sought by the appellant had already been negatived by the Registrar of Copyright and Clause 10[101] of the Memorandum of Understanding signed with the Government of Kerala vests intellectual property rights with the Government of Kerala specifically. The agreement between the appellant and C-DIT does not support appellant's claim on intellectual property rights. The high court also took notice of the fact that the appellant claiming the ownership of copyright in the software has neither instituted infringement suit under sections 60 and 61 of the Copyright Act, 1957 nor taken up arbitration as contemplated by clause 7 of the agreement dated February 14, 2001, which was well within his rights. The appellant finally appealed to the Supreme Court.

The apex court observed that the provisions of section 70(1) of the IT Act have to be read conjointly with sections 2(k) and 17 of the Copyright Act, 1957 in order to give due effect to related provisions of the two different enactments made by the legislature. Further, plainly read, the power of declaration of a "protected system" may invade a copyright which may be vested in a private owner, however, such a situation is taken care of by the provisions contained in section 2(k) of the Copyright Act, 1957 which defines "government work" and section 17(d) of the Copyright Act, 1957 which vests in the government, copyright in a government work as defined by section 2(k). The balance is struck by section 17 between copyright pertaining to any other person and copyright vested in the government in a "government work". Therefore, section 70 cannot be construed independent of the provisions of the Copyright Act, 1957. If section 70 of the IT Act has to be read in conjunction with sections 2(k) and 17 of the Copyright Act, 1957 the rigours that would control the operation of sections 70(1) of the IT Act are clearly manifested.

Further, the Supreme Court held that *ex facie*, the first owner of the copyright in this case appeared to be Microsoft, as the appellant had created the software for consideration under a contract. Therefore, the appellant did not have any locus to challenge the notification of a protected system. The Supreme Court therefore, declined to interfere with the division bench's judgement. The court however, declined to establish whether the government was, in fact, the assigned owner of the FRIENDS software, which would be required to uphold the challenged notification under section 70(1) as per its own reasoning.

101 Cl. 10 read as under:

> Departmental Task Force will monitor the actual implementation of the project *vis a vis* the milestones set by the TSP Intellectual Property Rights of the system developed by all the TSPs and Departments shall vest in the Government of Kerala.

The proviso to section 81 of IT Act though creates some ambiguity in relation to the scope of this provision under IT Act *vis-a-vis* Copyright Act, 1957 here because of the confusing language as the non obstante clause provides:[102]

> Act to have overriding effect. — The provisions of this Act shall have effect notwithstanding anything inconsistent therewith contained in any other law for the time being in force.
>
> Provided that nothing contained in this Act shall restrict any person from exercising any right conferred under the Copyright Act, 14 of 1957 or the Patents Act, 39 of 1970.

The apex court could have deliberated upon the scope of the provision to remove the long standing ambiguity here. If we go by the argument that if we restrict section 70(1) by Copyright Act, it would not be in the interest of cyber-security and critical information infrastructure (CII).

Secondly, holding that section 70(1) of the IT Act is constrained by the Copyright Act,1957 would have implications for India's cyber security and critical infrastructure. Section 70 allows the Government to control and restrict access to computer systems or software which it deems are important in the functioning of its critical information infrastructure. If such restriction is limited to only government works under the Copyright Act,1957 the government will be unable to restrict or control access to proprietary software which is (unfortunately) currently applies across a range of essential software, including, importantly, the software for the Central Identities Data Repository, perhaps the most sensitive information database in the country.

VII CONCLUSION

The focus in year 2018 was again on extent and scope of intermediary liability for third party content. With India emerging as a major hub of e-commerce transactions, there has been seen an upswing in intellectual property rights violations through online transactions involving several home-grown and multinational e-commerce players. Some crucial judgments in 2018 by different high courts and the apex court have contributed in the evolution of jurisprudence on intermediary liability analysing the role played by e-commerce platforms.

However, different parameters and more stringent guidelines have been prescribed for social media websites by the courts to deal with issues relating to national security, privacy and dignity of women and children especially. Deviating from earlier decisions, courts have tried to contribute their bit towards evolving jurisprudence in these areas/ issues, balancing the interface of Information Technology Act, 2000 with other laws.

The ministry of Ministry of Electronics and Information Technology in December released the Draft Information Technology (Intermediary Guidelines [Amendment] Rules), 2018. The rules are largely in conformity with developments on this front in various cases before the Supreme Court in last few months. Social media platforms herein are required to end the complete encryption system and remove any "unlawful content" for the sake of the country's security. The social media platforms are also

102 The Information Technology Act, 2000 (Act 21 of 2000), s. 81.

required to trace out the originator of information on its platform as may be required by the government agencies. The intermediaries are obligated to deploy technology based automated tools or appropriate mechanisms, with appropriate controls, for proactively identifying or removing or disabling access to unlawful information or content. This is a reflection of different interpretations adopted by the high courts and the apex court in matters related to extent and scope of the liability of intermediaries, deviating heavily from the interpretation adopted in *Shreya Singhal* that intermediaries are not responsible for judging the legitimacy of content on their platforms. The draft rules incorporating these interpretations given in recent cases not only endanger safe harbour protection of the intermediaries, they also raise concerns for privacy and free speech over internet. 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.

Similarly in matter related to admissibility of electronic evidence, the *Anwar* mandate was further diluted in *Shafhi Mohammad* stating that provisions under sections 65A and 65B of the Evidence Act are by way of a clarification and are procedural provisions. The judgment said that if the electronic evidence was relevant and produced by a person who was not in custody of the device from which the electronic document was generated, requirement of such certificate could not be mandatory. Very categorically it stated that the provision could not be read in derogation of the existing law on admissibility of electronic evidence. Despite that lower trial and high courts are already holding requirement under section 65B relaxable, ignoring *Anwar* mandate altogether. Further it being a two-judge bench ruling, there is need to clarify the legal position *vis-a-vis* a three-judge bench judgment in *Anwar* through a larger bench referral. Though it will be wrong to deny the benefits of new techniques and new devices, provided the accuracy of the record can be proved. A more progressive approach in legislative and judicial developments on these aspects in the coming year are expected and may bring more clarity on the issues.