9

CYBER LAW

Deepa Kharb[*]

I INTRODUCTION

CYBER LAW, a swiftly progressing field that intersects with numerous conventional legal disciplines, has undergone substantial transformations since 2014.This survey examines the evolving landscape of cyber law by analyzing the judicial decisions in 2021. It delves into crucial areas such as online privacy, data protection, cybercrimes, and electronic evidence, providing valuable insights into the development of cyber law in India. This survey serves as a practical guide for navigating the intricate challenges of the digital realm. Additionally, it presents a critical perspective on the court's reasoning, identifying points that may be subject to further debate. Overall, the survey underscores the dynamic nature of cyber law and its significant impact on the legal framework, reflecting the judiciary's efforts to adapt to the challenges posed by the digital age.

II ADMISSIBILITY OF ELECTRONIC EVIDENCE: SECTION 65B IEA

The introduction of sections 65A and 65B in the Evidence Act in 2000 provided a framework for the admissibility of electronic evidence, with section 65B (1) allowing for the admissibility of a paper printout of information contained in electronic records subject to the conditions specified in section 65B(2).

However, the requirement for a certificate under section 65B of the Indian Evidence Act for electronic records to be admissible in court has been a matter of debate among legal scholars and courts. While the Supreme Court in *Anvar P.V.* v. *P.K. Basheer*[1] (*Anvar* hereinafter) held that such records cannot be admitted as secondary evidence unless the requirements of section 65B are met, the court in *Shafhi Mohammad* [2] (*Shafhi* hereinafter) concluded that the certificate requirement may be waived wherever the interest of justice so justifies say when the electronic device storing the records is inaccessible or where the electronic device is produced by a party who is not in possession of such device, as a result of which such party would not be in a position to secure the requisite certificate.

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

1 (2014) 10 SCC 473.

2 (2018) 2 SCC 801 (decided on Apr. 25, 2018).

In a recent decision, *Arjun Panditrao Khotkar* v. *Kailash Kushanrao Gorantyal*[3] (*Arjun Panditrao Khotkar* hereinafter), a three-judge bench[4] of the Supreme Court clarified that the certificate required under section 65B(4) is a prerequisite for the admissibility of electronic evidence. The bench affirmed the correctness of the *Anvar* ruling in its interpretation, while finding that the *Shafhi* decision's division bench had erroneously "clarified" the requirement. The court also noted that the certificate is not necessary if the original electronic record is produced in court, however, compliance with section 65B is compulsory before a 'computer output', which is considered secondary evidence of an electronic record, can be admitted as evidence.

The court stated that if a person refuses to provide the certificate required under section 65B (4) of the Indian Evidence Act, a party can make an application to the judge requesting the production of the certificate. The court also explained that if it is impossible for the person to provide the certificate, or if the law excuses the person from doing so, then the party should be excused from the mandatory requirement of section 65B (4).[5] The court instructed trial courts to summon the person(s) specified in section 65B (4) when a defective certificate is given or when a certificate is refused, and require them to provide the necessary certificate. The court clarified that since section 65(B) does not talk about the stage at which such certification can take place, this is subject to the discretion exercised by the courts in civil cases, and in criminal trials, the accused must be supplied with all documents that the prosecution seeks to rely upon before the trial. The courts must balance the rights of the parties while examining any application by the prosecution under sections 91 or 311 of the Criminal Procedure Code, 1973 or section 165 of the Evidence Act, ensuring no serious or irreversible prejudice to the accused.

Although the relaxation of the strict requirements under section 65B (4) was aimed at easing the burden on parties who have made best efforts to obtain a certificate but failed to do so, it has been argued that such an exception goes beyond what the statute permits and creates further ambiguity. Furthermore, the obligation on the courts to summon the authorized person(s) to produce the certificate could result in a prolonged mini-trial within the trial, adding to the already overburdened judicial system and causing delays and additional expenses for the parties involved.

After the *Arjun Panditrao Khotkar*[6] case, various high courts in India have followed its ratio in their respective judgments especially on the exception created. They have held that electronic evidence must be accompanied by a certificate under section 65B of the Indian Evidence Act to be admissible in court. Failure to comply with this requirement results in the electronic evidence being inadmissible.

3 2020 SCC OnLine SC 571(decided on July14, 2020).

4 Bench consisting of RF Nariman, S. Ravindra Bhat, and V. Ramasubramanian

5 Due to the applicability of the Latin maxims *'lex non cogit ad impossibilia'* (the law does not demand the impossible) and *'impotentia excusat legem'* (when there is a disability that makes it impossible to obey the law, the alleged disobedience of the law is excused).

6 *Supra* note 3; 2020 SCC OnLine SC 571(decided on July14, 2020).

In *Rakesh Kumar Singla* v. *Union of India*[7] the petitioner, under the NDPS Act, filed a bail petition claiming they were unlawfully detained as no contraband was found in their possession at the time of arrest. The Narcotics Control Bureau (NCB) presented statements from a co-accused and the petitioner as evidence. However, the court emphasized that the determination of the petitioner's guilt or innocence should be based on the evidence presented during the trial. The NCB opposed the bail application, citing WhatsApp chat screenshots as evidence connecting the petitioner to the illicit drugs. Nevertheless, the court stated that WhatsApp messages cannot be considered as valid evidence without a certificate under section 65B of the Indian Evidence Act, as per the recent Supreme Court judgment in the case of *Arjun Panditrao Khotkar* v. *Kailash Kushanrao Gorantyal.*[8] Therefore, the court concluded that the WhatsApp messages, in their current state, hold no evidentiary value. Investigating agencies may rely on WhatsApp messages during a crime investigation, but a certificate under section 65B of the Indian Evidence Act is necessary for their admissibility.

In *Mahendra N. Pardeshi* v. *State of Maharashtra*[9] the prosecution attempted to prove the content of a DVR as evidence in a bribery case under section 7 and 13(1)(d) read with 13(2) of Prevention of Corruption Act, 1988, but failed to produce the original DVR or a certificate under section 65-B(4) of the Indian Evidence Act. The court held that verbal evidence about the contents of an electronic record is considered secondary evidence and the prosecution must prove that the contents of the DVR were heard. The court found that the prosecution failed to provide evidence that the contents of the DVR were heard and the witness could not confirm the conversation's content. Additionally, since the record was deleted, the court drew an adverse inference against the prosecution and dismissed the case.

In *Yogesh Arun Wakure* v. *State of Maharashtra***,**[10] the appellant, an accused facing the charge of murder punishable under section 302, 201, 323, 143, 147, 149 read with section 135 of the IPC with others, tried to establish his presence inside the hotel on the basis of the CCTV footage. However, an eye-witness claimed to have seen the present appellant at the crime spot around the time of murder.

It was contended from the appellant side that the trial court should not have disregarded the IO's report based on call detail records (CDR) and subscriber detail records (SDR) without considering section 65B and relied solely on the word of mouth of the eye-witness as it is often said that "humans may lie, but documents would not lie" or "documents would speak louder than words". The apex court has held in *Anvar*[11] that electronic records must be produced according to section 65B, after which their genuineness can be questioned and resort can be made to section 45A of the Evidence Act for seeking an opinion of the examiner of electronic evidence. The court directed the Registrar to transmit the documents, including the CDR/SDR record and DVD, to

7 MANU/PH/0011/2021.

8 *Supra* note 3.

9 2020 SCC OnLine Bom 7873(Decided on Oct. 23,2020).

10 2021 SCC OnLine Bom 354 (Decided on Mar. 10, 2021).

11 *Supra* note 1.

the trial court in a sealed envelope. The trial court will open the envelope upon receipt, and the contents will be a part of the original record.

In the case of *Pramod* v. *State of Maharashtra,*[12] the accused faced charges under various sections of the Indian Penal Code, 1860 including murder, kidnapping, and destruction of evidence. The prosecution sought to rely on electronic evidence in the form of Call Data Records (CDR) to prove their case.

The defense counsel argued that the electronic evidence presented by the prosecution is not admissible because the certificates do not comply with section 65B (4) of the Evidence Act. The certificates do not identify the electronic record containing the statements and do not specify the devices or computers over which they had control. The defense counsel also pointed out that none of the certificates are signed by a person occupying a responsible official position in relation to the operation of the relevant device or the management of the relevant activities. Therefore, the certificates relied upon by the prosecution in support of electronic evidence are not admissible in evidence. The defense counsel did not dispute the exchange of calls between the accused persons or the findings of the trial court regarding the cell phone locations of the accused persons and exchange of calls between them at the relevant time.

Sections 65A and 65B of the Evidence Act, deal with the admissibility and contents of electronic records as evidence in court. Electronic records are considered to be complete in themselves and can be admissible as evidence subject to the provisions of Section 65B (4) of the Evidence Act. Section 65B(1) of the Evidence Act distinguishes between the original electronic record and the output from such devices, which is a copy or data derived from the original document. The original electronic record is the one on which the information is first stored, and the secondary document is the one that contains the information derived from the original electronic record. The same was expounded by the Supreme Court in the case of *Arjun Panditrao Khotkar* in the following words:[13]

> 73.2. The clarification referred to above is that the required certificate under Section 65B(4) is unnecessary if the original document itself is produced. This can be done by the owner of a laptop computer, computer tablet or even a mobile phone, by stepping into the witness box and proving that the concerned device, on which the original information is first stored, is owned and/or operated by him. In cases where the "computer" happens to be a part of a "computer system" or "computer network" and it becomes impossible to physically bring such system or network to the Court, then the only means of providing information contained in such electronic record can be in accordance with Section 65B(1), together with the requisite certificate under Section 65B(4). The last sentence in *Anvar P.V. (supra)* which reads as "…if an electronic record as such is used as primary evidence under Section 62 of the Evidence Act…" is thus clarified; it is to be read without the

12 2021 SCC OnLine Bom 3344

13 *Arjun Panditrao Khotkar supra* note 3 in para no. 73.

> words "under Section 62 of the Evidence Act,…" With this clarification, the law stated in paragraph 24 of *Anvar P.V. (supra)* does not need to be revisited.

Sections 65A and 65B of the Evidence Act deal with the admissibility and contents of electronic evidence. A section 65B(4) certificate is mandatory for secondary evidence and can be given by a person in a responsible position related to device operation or management. The court relied on previous rulings *Arjun Panditrao Khotkar* [14] and *Engineering Analysis Centre*[15] to hold that the prosecution should be relieved of the obligation to provide a section 65B(4) certificate if they have made efforts to obtain it but have no control over the relevant third-party companies. The court found that the electronic evidence produced by the prosecution was admissible in and sufficiently corroborated the circumstantial evidence presented. The certificates produced by the prosecution were found to identify the electronic records and describe the manner in which they were produced as mandated by apex court in *Anvar*. The court noted that section 65B(4) is mandatory but any infirmity in the certificates can be overlooked given the circumstances.

The prosecution in *State of Maharashtra, through the Police Station Officer* v. *Sagar Vishwanath Borkar*[16] case relied on CCTV footage, which was copied onto a pen drive and a certificate under section 65B of the Evidence Act was taken. However, the prosecution failed to produce primary evidence in the form of the hard disc of the CCTV footage. The court held that the prosecution needed to comply with sub-section (4) of section 65B of the Evidence Act, which requires evidence of a person in a responsible official position in relation to the operation or management of the CCTV system. The mere exhibition of the CCTV footage by the trial court and the absence of objections by the accused are not sufficient to make the footage admissible. The court cited *Arjun Panditrao Khotkar* [17]to support this ruling. As a result, the CCTV footage cannot be relied upon as admissible evidence by the prosecution as it was not supported by a certificate under section 65B(4) of the Evidence Act. The court opined that the trial court was correct in refusing to rely on this evidence for non-compliance with section 65B(4) of the Evidence Act.

In *Sanjib Sarkar* v. *Rajasree Roy,*[18] a matrimonial dispute concerning the annulment of marriage under section 25(III) of the Special Marriage Act, the admissibility of electronic evidence, including Facebook posts and pictures, submitted by the respondent/wife was challenged by the appellant/husband's counsel on the grounds of lack of certification under section 65B (4) of the Indian Evidence Act. The court considered the arguments and referred to the law laid down in the *Arjun Panditrao Khotkar* case,[19] which distinguished between the manner of tendering primary and

14 *Supra* note 3.

15 2021 SCC OnLine SC 159(Decided on Mar. 2, 2021).

16 2021 SCC OnLine Bom 2725(Decided on Sep. 7, 2021).

17 *Supra* note 3.

18 2021 SCC OnLine Cal 2916(Decided on Nov. 11, 2021).

19 (2020) 7 SCC 1, *supra* note 3.

secondary evidence in electronic form. The court held that the required certification was not necessary for original documents produced by the owner of the device who can prove ownership and operation by stepping into the witness box. However, in situations where the source of information is part of a computer or computer network, certification under section 65B(4) is required. In the present case, the electronic evidence relied upon by the respondent was sourced from her original electronic device and therefore, certification was not required. The court found that the evidence presented by the respondent was admissible and she had proved her contention relating to fraud practiced on her.

In another case of *Sachin Makade Bablu Bhagwan Dangre* v. *Narcotics Control Bureau,*[20] the accused individuals were charged with dealing in illegal medical drugs, it was argued by accused that no such drugs were found in their possession or at their places of residence or work. The sole evidence against them was supposedly retrieved from their electronic devices, which have been contested as inadmissible without a certificate under section 65B of the Indian Evidence Act. The defense argued that the possibility of future criminal behavior must be taken into account under section 37 NDPS, and that the recovered Tramadol tablets from Dipu Singh cannot be linked to the accused individuals. Additionally, the information extracted from their electronic devices cannot be accepted without the requisite certificate under section 65B of the Indian Evidence Act.

The court, citing the cases of *Arjun Panditrao Khotkar* [21] and *Engineering Analysis Centre of Excellence Private Limited* v. *The Commissioner of Income Tax,*[22] stated that the mandatory obligation under section 65B(4) of the Indian Evidence Act may be waived if the respondent has made all reasonable attempts to obtain the necessary certificate, even if it was to be provided by a third party who was not under their control.

Although the National Control Bureau (NCB) obtained section 65B certificates from a cyber forensic expert who analyzed the electronic devices and extracted the data, the court concluded that it was not sufficient grounds to grant the accused individuals bail at this time. The court dismissed both petitions, but granted them the freedom to reapply for bail after examining public witnesses regarding the recovery. All pending applications were also resolved.

In an interesting application filed by the petitioner under article 227, *Sitanshi* v. *Vandana Sharma,*[23] seeking directions for Bharti Airtel Limited to preserve and produce the CDR of the respondent's mobile number. The petitioner argued that the CDRs should be preserved since they may be relevant and required at the time of the trial. However, the Trial Court rejected the application, as filed under Section 151 of the Civil Procedure Code, 1908, stating that it amounted to a roving inquiry and invasion of privacy. The Delhi High Court noted that the directions given by the Supreme

20 2021 SCC OnLine Del 5121(Decided on Nov. 29, 2021).

21 *Supra* note 3.

22 2021 SCC OnLine Bom 2725(Decided on Sep. 7, 2021).

23 2021 SCC OnLine Del 4497(Decided on Sep. 20, 2021).

Court in *Arjun Panditrao Khotkar* case on preserving CDRs were in the context of records seized during investigation and cannot be invoked in this case. The Supreme Court's directions on maintaining CDR and relevant records were only for those seized during investigation, as stated in paragraph 62. Paragraph 72 directs courts dealing with electronic evidence to ensure preservation and production of certificates for such records seized during investigation. The high court found no infirmity in the trial court's order and did not interfere.

The High Court of Delhi in *Megha Enterprises* v. *Haldiram Snacks Pvt. Ltd.,*[24] heard a petition under section 34 of the Arbitration and Conciliation Act, 1996. The petitioner challenged an arbitral award dated October 26, 2020, arguing that the arbitral tribunal erred in accepting an electronic letter as evidence without proof and affidavit under section 65B of the Evidence Act. However, the court rejected the argument, stating that the Indian Evidence Act does not apply to arbitrations, and the petitioners did not raise any objections before the arbitrator. The court found evidence showing that the respondent sent an email acknowledging the balance confirmation of Rs. 19,03,77,000/-, which was mentioned in a letter issued by the respondent. The email and letter are admissible as evidence under various provisions, including section 4 of the Information and Technology Act, 2000. The respondent did not dispute the transmission of information in electronic form. Therefore, emails acknowledging the debt due to the petitioner also meet the requirements under section 18 of the Limitation Act, 1963.

The petitioner in *Lalu* v. *Sheeja*[25] had filed an original petition to cancel a divorce decree obtained by the first respondent, citing fraud. The petitioner had submitted an application under section 45 of the Evidence Act to submit two CDs for voice identification. However, the court below had dismissed the application, stating that it did not comply with section 65B(4) of the Indian Evidence Act. The petitioner challenged this order in the original petition.

The petitioner had also filed an application to send a CD to an expert for voice comparison, but the court had dismissed the application because it did not comply with section 65B(4) of the Indian Evidence Act. Nevertheless, the petitioner argued that a certificate was not required at this stage, as the CD only needed to be examined by an expert. Additionally, the petitioner had produced the mobile phone containing the primary evidence. According to section 14 of the Evidence Act, the court should rely on relevant evidence produced by the parties in matrimonial disputes. The court should not prevent a party from adducing relevant evidence to prove their case. As such, the court was wrong in disallowing the prayer sought in the application.

The apex court, in *Arjun Panditrao Khotkar* v. *Kailash Kushanrao Gorantyal,*[26] had held that a certificate under section 65B (4) was unnecessary if the original document itself was produced. In proceedings under the family court, the technicalities of the Indian Evidence Act regarding the admissibility or relevancy of evidence were

24 2021 SCC OnLine Del 2641(Decided on Apr. 15, 2021).

25 2021 SCC OnLine Ker 9833(Decided on Sep.17, 2021).

26 *Supra* note 3.

not strictly applicable. The court had the discretion to rely on the documents produced if it was required to assist the court in effectively dealing with the dispute. The petitioner had wanted an expert opinion on the disputed conversation between the parties to the proceedings, which was relevant under section 45 of the Evidence Act. The court should not preclude a party from adducing evidence that may be relevant in accordance with the Evidence Act to prove their case. Thus, the court below was wrong in disallowing the prayer sought for in the application.

The court allowed the petitioner's application and set aside the impugned order. It directed the court below to summon Jeena along with the petitioner's power of attorney holder and respondent no. 3 to record their voices. The recorded conversation and CD will be sent to an examiner for electronic evidence opinion, with the petitioner bearing the expenses.

In *M.P. Mathew* v. *Central Bureau of Investigation*[27] the public prosecutor filed an application to summon a witness to produce a certificate under section 65B of the Evidence Act for certain documents already marked during the trial. The accused challenged this order but the special court allowed it. The court held that the certificate can be produced at any stage of the trial, but the rights of all parties must be balanced. The petitioner's senior counsel argued that they should be allowed to challenge the admissibility and marking of documents during the final hearing. The court dismissed the petition but allowed the petitioner to raise these contentions during the final hearing of the case.

In *Rajendra Agrawal* v. *State of Chhattisgarh*[28] the petitioner and co-accused, both, were charge-sheeted for the aforesaid offences under sections 500 read with section 120B of the IPC and 67 of the IT Act. The court found that no offense under section 67 of the IT Act was made out against the petitioner based on the contents of the FIR as it was neither found obscene nor lascivious. As a result, the charge under section 67 of the IT Act was quashed.

Additionally, the certificate under section 65-B(4) of the Evidence Act was mandatory to be filed with the charge-sheet, which was not done in this case. The court reiterated that the requirement of producing a certificate under section 65-B of the Evidence Act is mandatory in cases where secondary evidence is presented and oral evidence in the place of such certificate cannot possibly suffice as section 65-B(4) is a mandatory requirement of the law as established in the *Anvar P.V.* case. It quoted ratio of the Supreme Court from *Arjun Panditrao Khotkar*[29] to clarify the position of law on admissibility of electronic evidence under section 65B: [30]

> 61. We may reiterate, therefore, that the certificate required under Section 65-B(4) is a condition precedent to the admissibility of evidence by way of electronic record, as correctly held in *Anvar P.V*. (supra), and incorrectly "clarified" in *Shafhi Mohammed* (supra). Oral evidence

27 2021 SCC OnLine Ker 4035(Decided on Nov. 1, 2021).

28 2021 SCC OnLine Chh 903(Decided on Apr. 6, 2021).

29 *Arjun Panditrao Khotkar* v. *Kailash Kushanrao Gorantyal, supra* note 3 at para 22.

30 *Ibid.*

> in the place of such certificate cannot possibly suffice as Section 65-B(4) is a mandatory requirement of the law. Indeed, the hallowed principle in *Taylor v. Taylor*, which has been followed in a number of the judgments of this Court, can also be applied. Section 65-B(4) of the Evidence Act clearly states that secondary evidence is admissible only if led in the manner stated and not otherwise. To hold otherwise would render Section 65-B(4) otiose."

III OBSCENITY-SECTION 67,67A

Scope of provisions-Interpreting 'sexually explicit' act/conduct under section 67A and B

In *Sanjay Zacharias* v. *Stephen George*[31] the petitioner filed a petition under section 482 of the Criminal Procedure Code, 1973 to quash the proceedings initiated against them based on a complaint and FIR filed by Stephen George, a former MLA. The petitioner, who is the General Secretary of the Kerala Congress (M) and a former MLA, claims that the accused forged electronic records containing sexually explicit materials with the intent to defame prominent political figures. They argue that the allegations are politically motivated and deny any association with the social media account in question. The petitioner's counsel disputes the application of section 67A of the IT Act, which is a non-bailable offense, and argues that if any offenses were committed, they would fall under the bailable offense of section 67. The petitioner also asserts that they are a victim of social bullying and harassment by political opponents.

The senior counsel for the petitioner argues that the decision in *Majeesh K. Mathew* v. *State of Kerala*[32] has little relevance to the current case as it involved different facts and emphasized that the facts of that case involved oblique utterances made against a woman through social media, whereas the current case does not involve similar circumstances.

During the proceedings, the petitioner's counsel argued that the content in question does not have a sexual tone and asserted that the petitioner is being falsely interpreted and harassed. However, the counsel for the first respondent argued that the offense under section 67A of the IT Act is applicable, as the petitioner intended to defame a prominent political figure. The director general of prosecution also opposed the application, emphasizing the importance of understanding the content in its context. The court rejected the petitioner's counsel's interpretation, considering it distorted and taken out of context to suit the petitioner's convenience.

The court observed that the crucial point revolves around whether the petitioner made sexually explicit postings on social media, particularly a caricature and an image depicting a song. The court rejected the interpretation made by the petitioner's counsel, stating that every word should be understood in its context. The court considered the interpretation presented by the petitioner's counsel as distorted and taken out of context

31 2021 SCC OnLine Ker 13947(Decided on Nov. 25, 2021).

32 2018 (4) KHC 253.

to suit the petitioner's convenience. The settled proposition of law, as established by the Supreme Court in *Devidas Ramachandra Tuljapurkar* v. *State of Maharashtra,*[33] emphasizes that an objective assessment must be made to determine whether the matter in question is obscene. The court must consider contemporary community standards and eliminate subjective elements or personal preferences. In this case, the expression "KER_380669_6.png" is argued to have a sexually explicit tone, resembling the opening lines of a Malayalam film song, which suggests oral sex. Therefore, it is contended that Section 67A of the IT Act is applicable, and the argument that it has no application cannot be accepted.

Moreover, the court highlights that the petitioner's previous application for anticipatory bail was dismissed, and the same arguments cannot be used to quash the proceedings. Ultimately, the court finds no merit in the application and dismisses it, allowing the proceedings to continue.

In *Suvojit Chowdhury* v. *State of Maharashtra*[34] *(with Sherlin Chopra* v. *State of Maharashtra)* the applicants/accused sought protection from arrest for offenses under sections 292 of the Indian Penal Code, sections 67 and 67A of the Information Technology Act, 2000, and sections 3 and 4 of the Indecent Women Representation Act, 1986 related to broadcasting and exhibiting indecent videos, audio files, and messages containing sexually explicit content through Over-The-Top (OTT) platforms on the internet for illegal financial gains. Raj Kundra, the Director of Arms Prime, was implicated by co-accused for instigating them to act in obscene films. The applicants did not cooperate in providing details about the creation of vulgar videos. Statements of co-accused and witnesses established their involvement in video graphing and publishing objectionable obscene material on both free and paid apps, satisfying the elements of the alleged offense, particularly under section 67A. The request for pre-arrest bail was rejected, but an ad-interim order of protection was extended for four weeks from the date of the order.

In another case *Pramod Anand Dhumal* v. *State of Maharashtra*,[35] The applicant, an editor of a local Marathi newspaper and a social activist, sought pre-arrest bail for offenses under section 354-D of the Indian Penal Code (IPC) and section 67A of the Information Technology Act (IT Act). The complainant had received offensive and sexually explicit messages with images from the applicant's cell phone on her Facebook account. Despite expressing her disinterest, the applicant continued to send obscene messages along with a hyperlink containing lascivious material. The complainant filed a complaint, resulting in the registration of a case against the applicant under section 354-D of the IPC and section 67A of the IT Act.

The court observed that the material sent by the applicant did not meet the criteria for "material containing sexually explicit acts" required by section 67A of the IT Act. Instead, it fell under section 67, as it tended to excite lust but did not directly depict sexual activity in a detailed manner. Therefore, *prima facie*, the offense may

33 (2015) 6 SCC 1.

34 2021 SCC On Line Bom 11930(Decided on Nov. 25, 2021).

35 2021 SCC OnLine Bom 34.

attract section 67 and not section 67A of the IT Act. The court found the applicant prima facie involved in the offense of stalking under Section 354-D of the IPC, which is bailable as a first offense. Considering the evidence and the punishment prescribed for the offense under section 67 of the IT Act, the court granted pre-arrest bail to the applicant, as custodial interrogation was not required for electronic evidence.

A prayer was filed in *Vijesh* v. *State of Kerala*[36] to quash all proceedings against the accused under sections 66(A) and 67(A) of the IT Act, 2000, among others, using section 482 of the Criminal Procedure Code (Cr. PC). The second respondent, a lady, was the *de facto* complainant in the case. According to the prosecution's case, during the inaugural function of a jewelry store, celebrities from television and cinema were invited, resulting in a crowd where people took photos with them on their mobile phones. Subsequently, in January and March 2012, videos titled "Mallu Aunti Harassed" and "Paravoor Peedanam" were uploaded on YouTube, allegedly containing the second respondent's photographs from the inauguration along with derogatory remarks. The petitioner was accused of offenses under sections 66(A) and 67(A) of the IT Act.

However, it is important to note that section 66(A) of the IT Act has been declared unconstitutional by the Supreme Court in the case of *Shreya Singhal* v. *Union of India*.[37] Therefore, the criminal proceedings related to the offense under Section 66(A) of the IT Act cannot be sustained. The only remaining offense alleged against the petitioner is the one under section 67(A) of the IT Act, which deals with punishment for publishing or transmitting sexually explicit material in electronic form.

According to section 67(A) of the IT Act, the accused must have published or transmitted sexually explicit material in electronic form. The alleged publication of the respondent's photograph during the jewelry store's inaugural function, as admitted by the respondent, does not qualify as sexually explicit material.

The prosecution's argument that uploading photographs of the respondent with sexually colored remarks like "Mallu Aunti Harassed" and "Paravoor Peedanam" etc fulfills the requirements of Section 67(A) of the IT Act is invalid. The use of sexually colored remarks does not amount to the publication or transmission of sexually explicit material. The term "sexually explicit" has a specific meaning and does not include news or informational material. Since the offense under section 66(A) of the IT Act has already been declared unconstitutional, the continuation of criminal proceedings against the petitioner is an abuse of the court process and should be quashed under section 482 of the Cr PC.

The court concluded that the initiation and continuation of criminal proceedings against the petitioner were an abuse of the court process. Exercising its inherent extraordinary powers under section 482 of the Cr PC, the court ordered that the charge sheet against the petitioner/accused and all subsequent proceedings stemming from it be quashed and set aside.

36 2021 SCC OnLine Ker 854.

37 (2015) 2 KLT 1 (SC).

In *Imran Shabbir Gauri* v. *State of Maharashtra*[38] the appellant, who was the father of the victim, had been convicted by the trial court for several offences, including the possession of pornographic images of the victim on his mobile phone. Specifically, he was found guilty under section 376(2)(i) and 506 of the Indian Penal Code (IPC), as well as under section 4 of the Protection of Children from Sexual Offences (POCSO) Act, 2012. Additionally, he was convicted for the offence punishable under section 67-B of the IT Act, 2000, as he had obtained nude photographs of the victim on his mobile handset on multiple occasions.

During the trial, the court took into consideration the evidence presented, including the Forensic Science Laboratory (FSL) report that confirmed the presence of pornographic images and video clips on the appellant's mobile phone. However, the court expressed concerns about the evidentiary value of the FSL report, as it was unclear whether it constituted substantive evidence or merely corroborative evidence. The court emphasized that the testimony of the individual who witnessed the incident or the victim herself would be crucial as substantive evidence, while the recorded material stored on the memory card could serve as corroborative evidence.

While acknowledging the presence of pornographic images on the appellant's mobile phone, the high court hesitated to establish a direct connection between those images and the victim due to a lack of identification. Although the forensic analysis confirmed the existence of pornographic content to some extent, the court found it challenging to attribute those specific images to the victim. Nonetheless, the appellant was convicted under section 67-B of the Information Technology Act, which pertains to the depiction of sexually explicit acts involving children in electronic form. Even though there was no evidence of the appellant uploading or transmitting these images to anyone else, the act of possessing or depicting children in an obscene, indecent, or sexually explicit manner in electronic form is punishable under clause (b) of section 67-B. Therefore, the court upheld the conviction of the appellant under section 67-B of the IT Act, 2000.

Section 67 and liability of admin of WhatsApp group

In *Kishor* v. *State of Maharashtra*[39] the Nagpur Bench of the High Court of Bombay recently examined the legal responsibility of a WhatsApp group administrator in relation to objectionable content posted by group members. In this case, the applicant (accused No. 2) filed an application to quash a charge sheet and FIR filed against him for offenses under sections 354-A(1)(iv), 509, and 107 of the IPC, 1860, and section 67 of the IT Act, 2000.

The allegations in the FIR stated that as an administrator of a WhatsApp group, the applicant allowed another member (accused No. 1) to use offensive language against a non-applicant (No. 2) in the group. It was further alleged that despite being aware of accused No. 1's actions, the applicant took no action against them, such as

38 2021 SCC OnLine Bom 511(Decided on Mar. 31, 2021).

39 2021 SCC OnLine Bom 654(Decided on Mar. 1, 2021).

removing them from the group or asking for an apology. The FIR was lodged by the non-applicant against both the applicant and accused no. 1.

To address the issue of potential criminal liability of a WhatsApp group administrator, the court first examined the operational dynamics of WhatsApp. It acknowledged that WhatsApp is an instant messaging platform that allows mass communication through chat groups. The group administrator has the authority to add or remove members but does not possess the power to regulate or censor content before it is posted. The court emphasized that individual members can be held liable for their own posts if they violate the law. Without specific provisions establishing vicarious liability, an administrator cannot be held responsible for objectionable content posted by group members. The court stated that establishing vicarious liability would require demonstrating a common intention or pre-arranged plan between the administrator and the group member involved. Merely being a group administrator does not establish common intention, and it is unreasonable to expect administrators to anticipate or have prior knowledge of the criminal actions of group members. Additionally, the liability of an administrator as a creator of objectionable content does not apply in this case.

Regarding the offense under section 67 of the IT Act, the court analyzed the specific language of the section, which punishes the transmission or publication of obscene material in electronic form. The allegations and evidence presented did not support the claim that the applicant disseminated or caused the dissemination of any lascivious or obscene material. Section 67 prescribes that an individual may be subjected to punishment for transmitting, publishing, or causing to be transmitted or published, any material that is obscene in electronic form. One could discern on a careful analysis of the allegations in the FIR and the evidence presented in the form of a charge sheet that there is no claim or evidence that the applicant disseminated or caused to be disseminated any material in electronic form that is lascivious, appeals to prurient interests, or is likely to corrupt or deprave individuals who may view, read, or hear it. The definition of an intermediary also did not apply to the applicant, as there was no accusation of involvement in transmitting or receiving any record or providing related services.

After reviewing the material in the charge sheet, it was clear that the essential elements of the alleged offenses were not disclosed. Continuing with the proceedings against the applicant would amount to an abuse of the court process. As a result, the court quashed the FIR, charge sheet, and all proceedings against the applicant for offenses under sections 354-A (1)(iv), 509, and 107 of the IPC and section 67 of the IT Act.

The petitioner in *Rajendra Agrawal* v. *State of Chhattisgarh*[40] case sought the quashing of charges against them under section 67 of the Information Technology (IT) Act and section 500 of the IPC through section 482 of the Cr PC. Their argument was that the WhatsApp messages allegedly sent by their co-accused on their behalf

40 2021 SCC OnLine Chh 903(Decided on Arp. 6, 2021).

were not of an obscene or lascivious nature, and therefore, no offence under section 67 of the IT Act was established against them.

The court carefully examined the provisions of section 67 of the IT Act and compared them with sections 294 and 292(1) of the IPC, which deal with the concept of obscenity. It noted that while there are similarities between these provisions, there are also distinct differences in their language and requirements. Specifically, in order for an act to fall within the scope of section 67 of the IT Act, it must have the potential to deprave and corrupt individuals who are likely, considering all relevant circumstances, to read, see, or hear the content in question.

Therefore, the court highlighted that the mere publication, transmission, or causing of publication or transmission in electronic form is not sufficient to bring an act within the purview of section 67 of the IT Act. The content must possess a quality that tends to deprave and corrupt individuals who are likely to come across it. This distinction is important in determining whether the alleged WhatsApp messages can be considered an offence under section 67 of the IT Act.

In essence, the court emphasized that the content in question should have a potentially harmful impact on the moral and ethical standards of the readers, viewers, or listeners, taking into account all relevant factors. The petitioner's argument relied on the assertion that the WhatsApp messages did not meet this standard of obscenity or lasciviousness required by section 67 of the IT Act. Setting aside the FIR and the consequent criminal proceedings initiated against the petitioner, the court held: [41]

> The words in the said WhatsApp message are not capable of arousing sexual thoughts or feelings in the minds of the petitioner or respondent No. 2 or other four persons to whom the message has been sent by the co-accused and it does not involve lascivious elements arousing sexual thoughts or feelings or the words in the said message have no effect of depraving persons, and defiling morals by sex appeal or lustful desires, though the words may be extremely un parliamentary, unprintable and abusive in nature, but it cannot be brought within the broad contours of the penal provisions as contained in Sections 294 & 292 of the IPC corresponding to Section 67 of the IT Act. Even according to the complainant, it is only defamatory and as such, the ingredients of offence under Section 67 of the IT Act are not at all attracted.

Viewing child pornography privately - an offence?

In *P.G. Sam Infant Jones* v. *State*[42] the prosecution alleged that the petitioner accessed, a M.E degree holder and pursuing Ph.D. at that time, downloaded, and shared child pornographic material using an Airtel SIM card and his email and Facebook accounts.

The petitioner's counsel argued that the petitioner was present in the hostel during the relevant time and that the evidence provided thus far was insufficient to

41 *Ibid.*

42 2021 SCC OnLine Mad 2241(decided on June 11, 2021).

prove that the petitioner personally committed the alleged acts. Furthermore, there is no evidence indicating that the content in question involved child pornography. The act of viewing pornography in private does not typically constitute an offense, as there is no specific provision in place that prohibits such private acts, the counsel for accused argued.

While there are arguments suggesting that child pornography falls under an individual's freedom of expression and privacy, it is important to highlight that child pornography is an exception to this principle. The high court observed that section 67-B of the Information Technology Act, 2000 deals with child pornography and imposes penalties for various acts related to it. The provision covers publishing, transmitting, creating, collecting, seeking, browsing, downloading, advertising, promoting, exchanging, or distributing material in any electronic form that depicts children engaged in sexually explicit acts. It also includes activities such as cultivating, enticing, or inducing children into online relationships for sexually explicit acts, facilitating online abuse of children, and recording one's own abuse or the abuse of others involving sexually explicit acts with children. Consequently, viewing child pornography is considered an offense and is punishable under the law.

After considering the circumstances of the case, the court found that the incident occurred nearly a year ago and it seems to be an isolated incident. Even the prosecution did not allege that the possession or transmission of the material was for commercial purposes. The court made a distinction between individuals who consume child pornography on a one-time basis and those who actively transmit, distribute, or show such material in the digital realm. It emphasized the seriousness of the issue and the need for a strong approach to combat child pornography. The court acknowledged that once someone enters the digital space, their activities can be monitored by either the government or the operators of social networking sites. It further highlighted that:[43]

> It is obvious that the moment one steps into digital space, one comes under the surveillance either of the State or those manning the social networking sites. If one is zealous about privacy, the only option is to stay outside such networks. Of course, in the current world, it is not a viable option.

Court mandated both the central and state governments to raise awareness about the provisions of the POCSO Act under section 43, however, it was acknowledged that this alone may not be enough and emphasized that moral education is considered to be the only effective solution to address this issue: [44]

> 11…..It is only the Bharatiya culture that can act as a bulwark. The menace of child pornography can be tackled only if all of us inculcate the right values.

43 *Ibid.*

44 *Ibid.*

IV RIGHT TO BE FORGOTTEN

S.K. Kaul J.,in *K.S. Puttaswamy* v. *UOI* observed:

> Right of an individual to exercise control over his personal data and to be able to control his/her own life would also encompass his right to control his existence on the Internet.

The introduction of GDPR in the European Union triggered a discussion on privacy concerns in India and led lawmakers to consider the need for a data protection framework. However, India presently lacks such a framework. While some courts have recognized it as part of the right to privacy, others have rejected pleas for removal of personal information due to the lack of legislative sanction. The Information Technology Act, 2000, which regulates the cyber world in India, does not mention the right to be forgotten. The Supreme Court's landmark ruling in the case of *K.S. Puttaswamy*[45] however, established that the right to privacy includes the right to be left alone, which is an essential aspect of an individual's privacy. Also the Indian Personal Data Protection Bill, 2019, does mention the right to erasure.

The right to be forgotten is evolving in India and struggling to be considered a fundamental right, but with increasing concerns about data privacy and exploitation, it is a relief that can be claimed against illegal or unwanted sharing of personal information only. It is important to legally recognize the right to be forgotten as a core part of the right to privacy and a fundamental right.

In *Karthick Theodre* v. *The Registrar General*[46] the petitioner was charged with a criminal offence under sections 417 and 376 of the IPC and the trial court found him guilty and punished him. The petitioner was acquitted of all charges but his name still appears in the judgment as an accused. He approached the High Court of Madras with the request that his name be removed from the judgment as it harms his reputation, despite being acquitted.

The high court agreed that an accused who has been exonerated of all charges has the right to have their name redacted from records to safeguard their right to privacy. However, the court stated that the "right to be forgotten" cannot exist in the administration of justice and giving such a broad directive would open the floodgates of demands. India does not have a system to erase an accused person's records once they have been acquitted, and only "The Juvenile Justice [Care and Protection of Children] Act, 2015" allows for such erasure. It was observed that:[47]

> 31.....This Court honestly feels that our criminal justice system is yet to reach such standards where courts can venture to pass orders for redaction of name of an accused person on certain objective criteria prescribed by rules or regulations. It will be more appropriate to await the enactment of the Data Protection Act and Rules thereunder, which may provide an objective criterion while dealing with the plea of

45 (2017) 10 SCC 1.

46 2021 SCC OnLine Mad. 2755

47 *Ibid.*

> redaction of names of accused persons who are acquitted from criminal proceedings. If such uniform standards are not followed across the country, the constitutional courts will be riding an unruly horse which will prove to be counterproductive to the existing system.

The high court decided that it cannot issue a broad order to redact names from court records without appropriate statutory backing. The court felt that a proper policy must be established to prevent confusion when carrying out such an exercise. The court concluded that without clear guidelines, such a broad order could lead to many complications and that the government must create a statutory framework for such a policy.

In *Jorawer Singh Mundy* v. *Union of India*[48] the petitioner, an American citizen of Indian origin with a background in real estate, filed a petition to remove a judgment *Custom* v. *Jorawar Singh Mundy* [49] from online platforms like Google, Indian Kanoon, and Vlex.in.

The petitioner, Jorawer Singh, an American citizen of Indian origin was charged under the Narcotics Drugs and Psychotropic Substances Act (NDPS Act) in India during a visit in 2009. He was later acquitted of all charges by the trial court and the High Court of Delhi. However, he faced difficulty finding employment due to the online availability of the judgment regarding his involvement in the drug case on platforms such as Google, Indian Kanoon, and vLex.in. He filed a writ petition under article 226 of the Indian Constitution before the High Court of Delhi, requesting the platforms to take down the judgment as it violated his right to privacy under article 21 of the Constitution. The petitioner issued legal notices to the aforementioned platforms. Vlex.in claimed to have removed the judgment, but it remained available on other platforms.

The central question in this case was

i. whether the right to privacy under article 21 of the Indian Constitution includes the right to be forgotten, and

ii. whether a court has the authority to order the removal of information from online platforms?

The High Court of Delhi had to balance the right to privacy against the right to information available to the public and maintenance of transparency in judicial records. While the right to privacy is recognized as a fundamental right, the right to be forgotten is not explicitly mentioned in the Indian Constitution. However, in some cases,[50] courts have recognized the right to be forgotten as a part of the right to privacy. It cited *Zulfiqar Ahman Khan* v. *Quintillion Businessman Media Pvt. Ltd.,*[51] where this court had held as under: [52]

48 2021 SCC OnLine Del 2306.

49 Crl.A. No. 14/2013.

50 *Karthick Theodre v. Registrar General*

51 2021 SCC OnLine Mad. 2755 , and *Subhranshu Rout v. State of Odisha* 2020 SCC OnLIne Ori. 878

52 2019 SCC OnLine Del. 8494.

> 8. In fact, it is the submission of ld. Counsel for the Plaintiff that the Plaintiff's personal and professional life has been hampered irreparably and further damage is likely to be caused if appropriate relief is not granted against the republication of these two articles. The original publisher having already agreed to pull down the same, this Court having directed that the same ought not to be republished, the Plaintiff, thus, has a right to ensure that the articles are not published on multiple electronic/digital platforms as that would create a permanent atmosphere of suspicion and animosity towards the Plaintiff and also severely prejudice his personal and professional life. The printouts of the articles from www.newsdogapp.com, which have been shown to the Court, leave no doubt in the mind of the Court that these are identical to the articles published on www.thequint.com, which has already been pulled down.
>
> 9. Accordingly, ecognizing the Plaintiff's Right to privacy, of which the 'Right to be forgotten' and the 'Right to be left alone' are inherent aspects, it is directed that any republication of the content of the originally impugned articles dated 12 October 2018 and 31 October 2018, or any extracts/or excerpts thereof, as also modified versions thereof, on any print or digital/electronic platform shall stand restrained during the pendency of the present suit.
>
> 10. The Plaintiff is permitted to communicate this order to any print or electronic platform including various search engines in order to ensure that the articles or any excerpts/search results thereof are not republished in any manner whatsoever. The Plaintiff is permitted to approach the grievance officers of the electronic platforms and portals to ensure immediate compliance of this order.

The court opined that the petitioner may face irreversible harm to his social life and career prospects, despite being acquitted in a case. The court held that the petitioner is entitled to interim protection while the legal issues are pending and accordingly directed Google and Google LLC to remove the judgment titled *Custom* v. *Jorawar Singh Mundy*[53] from their search results and India Kanoon to block access to the said judgment through search engines.

In *X* v. *YouTube,*[54] the plaintiff, a popular Bengali film actor, was promised the lead role in a web series by Ram Gopal Verma Studios. She participated in a demonstration video which included explicit scenes of complete nudity, but the project was later shelved. However, the producer uploaded the video to his YouTube channel and website, and although he removed it upon the plaintiff's request, others uploaded it to different websites without her consent. The plaintiff applied to the court seeking interim protection and a takedown of the video due to the violation of her privacy,

53 *Id.* Cited at para 9 in *Jorawer Singh Mundy v. Union of India*

54 Crl.A. No. 14/2013.

damage to her reputation, and harassment she faced as a result. The defendants included websites, internet service providers, and search engines.

The plaintiff argued that the right to privacy includes the right to be forgotten, which has been recognized by the Indian Supreme Court and several high courts. She also cited Rule 3(2)(b) of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which requires intermediaries to remove or disable access to content that exposes an individual's private areas within 24 hours of receiving a complaint. The defendants, including websites, ISPs, and search engines, were thus obliged to take measures to remove the suit videos. The plaintiff also cited a High Court of Delhi decision where Google was directed to remove URLs/websites under an interim order. The plaintiff argued that the three-part test for an interim injunction was satisfied, and the court should issue such an order against the defendants.

Defendants Google relying on *Karthick Theodre* v. *Registrar General,*[55] and *Subhranshu Rout* v. *State of Odisha*[56] argued that they were not under any obligation to prevent the republication of the Suit Videos since they were unaware of any agreement permitting the broadcast. They also argued that the plaintiff had no valid statutory protection to enforce the right to be forgotten and that the plaintiff should have approached the publishing platforms instead of the search engine defendant. They relied on case law showing that courts had rejected the disabling of search results in the manner sought by the plaintiff. Lastly, they argued that the plaintiff had consented to the filming of the videos, and Rule 3(2)(b) of the Rules 2021 required the victim or an authorised representative to complain to the intermediary, which was not satisfied in the present case. They further submitted that Rule 3(3)(b) should be read alongside Sections 67 and 67A of the Information Technology Act, 2000, which excluded material published in the interest of science, literature, art or learning or other objects of general concern.

The Court found that the explicit nature of the Suit Videos fell under Rule (3)(2)(b) of the Rules 2021, and rejected the defendants' argument that the plaintiff's consent to filming barred her from legal recourse. The Court drew parallels between this case and *Zulfiqar Ahman Khan* v. *Quintillion Business Media (P) Ltd*.,[57] which illustrated the severe impact of publication on personal and professional life. The court found that the plaintiff's right to privacy should be protected, given the explicit nature of the videos and the impact on her reputation. While neighbouring high courts had found no statutory right to be forgotten, the court endorsed the right to be forgotten and the right to be left alone as inherent aspects of the right to privacy.

Court granted interim relief to the plaintiff, finding that the suit videos were of an explicit nature and that their circulation had a clear and immediate impact on the plaintiff's reputation. The court rejected the defendants' arguments that the plaintiff had consented to the filming of the videos and that she had no valid statutory protection

55 2021 SCC OnLine Del 4193(Decided on Aug. 23, 2021).

56 2021 SCC OnLine Mad 2755.

57 (2020) SCC Online Ori 878).

to enforce her right to be forgotten. The court found her consent to have since been expressly withdrawn, as the producer of the series had also removed the videos upon her request and held that the plaintiff's right to privacy should be protected. It therefore passed an interim order directing the defendants to take down all the suit videos from their websites, channels, digital platforms, and search engines and to stop uploading, publishing, streaming, transmitting, broadcasting, or communicating the videos to the public. The defendants were given 36 hours to comply with the order, and the plaintiff was given the right to communicate the order to any other platforms found to be publishing, streaming, or transmitting the suit videos.

V INTERMEDIARY LIABILITY-SECTION 79

The issue of intermediary liability has been a subject of uncertainty since the introduction of the Information Technology Act in 2000. In recent years, intermediaries have become increasingly significant due to the widespread use of social media platforms for communication and information sharing. The emergence of digital media has also made it a mainstream concern, leading the government to focus on regulating these platforms. The 2021 Rules represent an initial effort to regulate such platforms.

The 2021 IT Rules

In February 2021, the Indian government introduced new regulations for social media platforms, digital news media, and other online content providers called the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (IT Rules 2021). These rules aim to hold intermediaries more accountable to both internet users and the Indian government. They require social media platforms and messaging apps to appoint Indian residents as grievance officers, compliance officers, and nodal officers and to remove content within 36 hours of receiving a legal order or court directive and maintaining records of all removed content for a minimum of 180 days.

There are also specific rules for publishers of news and current affairs content and online curated content. Significant Social Media Intermediaries (SSMI) in comparison to Social Media Intermediaries (SMI) need to observe additional due diligence requirements and comply with stringent residency requirements for compliance officers and nodal contact persons. The rules empower the government to direct intermediaries and publishers to delete, modify, or block content, either through a grievance procedure or through emergency blocking orders passed without a hearing.

However, the rules have faced criticism from human rights groups and digital rights advocates who argue that they could be used to suppress free speech and expression. The rules have also been challenged in petitions filed in different high courts including the High Court of Bombay, Kerala, Delhi, and Madras.

Rule 4(2) of the IT Rules 2021 requires SSMI providing messaging services to enable the identification of the first originator of information on their computer. This provision has been challenged by companies like WhatsApp on the grounds that it infringes upon users' fundamental right to privacy and freedom of speech. Rule 4(4), which requires the use of technology-based measures to proactively identify certain

types of content, raises concerns about the accuracy and consequences of fully automated tools.

In the case of *Live Law Media Pvt. Ltd.* v. *Union of India,*[58] the High Court of Kerala has passed an interim order directing that no coercive action be taken against Live Law, under Part III of the IT Rules 2021 (dealing with digital media), as Live Law is a publisher of law reports and legal literature.

In *Foundation for Independent Journalism* v. *Union of India*[59] and *Sanjay Kumar Singh* v. *Union of India,*[60] High Court of Delhi directed Central Government to file a reply. In another petition before High Court of Kerala titled *Praveen Arimbrathodiyil* v. *Union of India*[61] where a free and open source software (FOSS) developer who filed a petition against India's IT Rules 2021 has claimed that the regulations unfairly burden small-scale FOSS developers and communities. The petitioner has argued that the rules' content moderation requirements could weaken data security and privacy measures, ultimately infringing on the right to freedom of trade and profession under article 19(1)(g) of India's constitution. The government filed a transfer petition under article 139A(1) of the Constitution, seeking a transfer of the four petitions mentioned above, on the ground that they are substantially similar to justice for rights foundation, initiated long before the government notified IT Rules, 2021.[62]

Two petitions *Agij Promotion of Nineteenonea Media Pvt. Ltd.* v. *Union of India*[63] and *Nikhil Mangesh Wagle* v. *Union of India*[64] were filed in High Court of Bombay to challenge the IT Rules 2021 on the ground that they are *ultra vires* the Information Technology Act, 2000('IT Act') and the provisions of articles 14, 19(1)(a) and 19(1)(g) of the Constitution and go beyond the restrictive ambit of section 69A of the IT Act. 2021 Rules have a terrible chilling effect in their applicability to the internet as they bring about a manifestly unreasonable and an arbitrary regime amounting to an affront to the constitutional guarantee of right of citizens to exercise freedom of free speech and expression. The Central Government justified the Rules by stating that they aimed to create a level playing field between online and offline publishers and combat fake news.

The High Court of Bombay granted an interim stay on Rules 9(1) and 9(3) of the IT Rules 2021, stating that they are *ultra vires* the IT Act. Bench stated that Rule 9 of the IT Rules, 2021 appeared to infringe upon the constitutional guarantee of freedom of speech and expression, as enshrined in article 19(1)(a). This infringement was evident in the fact that the rule subjected publishers of news and current affairs content and online curated content to action under the Press Council Act, 1978 and the Cable TV Networks Regulation Act, 1995 which already had their own independent

58 2019 SCC Online Del 8494.

59 W.P.(C) 6272 of 2021.

60 W.P.(C) 3125 / 2021.

61 W.P.(C) 3483 of 2021.

62 *Praveen Arimbrathodiyil* v. *Union of India* WP (C) 18084/2021).

63 *Union of India* v. *Sudesh Kumar Singh*, Transfer Petition (C) No. 100-105/2021.

64 2021 SCC OnLine Bom 2938.

mechanisms for dealing with violations, and a subordinate legislation like Rule 9 could not disrupt or override the powers granted by those laws.[65]

The court also noted that Rule 14, which deals with the formation of an inter-departmental committee, and Rule 16, which deals with blocking information during emergencies, do not require immediate action. However, Rule 9 imposes an obligation on publishers to adhere to a Code of Ethics that is not part of the IT Act and may preclude them from criticizing public figures, which the court found problematic as it goes beyond the powers laid down in section 69A of the IT Act:[66]

> 28. "Dissent in democracy is vital. It is, however, the checks and balances that make a democracy work. There can be no two opinions that a healthy democracy is one which has developed on criticism and acceptance of contra views. Opinion based on criticism reinforces its acceptance in a democratic society. For proper administration of the State, it is healthy to invite criticism of all those who are in public service for the nation to have a structured growth but with the 2021 Rules in place, one would have to think twice before criticizing any such personality, even if the writer/editor/publisher may have good reasons to do so without resorting to defamation and without inviting action under any other provision of law. Allowing the operation of the 2021 Rules in its form and substance to operate would result in the writer/editor/publisher standing the risk of being punished and sanctioned, should the inter-departmental committee be not in favour of criticism of any public figure. It is, therefore, quite possible that the writer/editor/publisher on contravention of the provisions of clause (1) of Rule 9 of 2021 Rules, but without even transgressing the boundaries set by clause (2) of Article 19 of the Constitution, may expose himself/itself to punishment/sanction under the 2021 Rules. The indeterminate and wide terms of the Rules bring about a chilling effect *qua* the ight of freedom of speech and expression of writers/ editors/publishers because they can be hauled up for anything if such committee so wishes. The 2021 Rules are, thus, manifestly unreasonable and go beyond the IT Act, its aims and provisions.
>
> 29. A democracy would thrive only if the people of India regulate their conduct in accordance with the preambular promise that they took while giving to themselves the Constitution. Liberty of thought is one of such promises. Exercising this liberty, expressions take shape. Should at least a part of Rule 9 of the 2021 Rules be not interdicted even at the interim stage, it would generate a pernicious effect. As it is, the constant fear of being hauled up for contravention of the Code of Ethics is a distinct possibility now. People would be starved of the liberty of thought and feel suffocated to exercise their right of freedom of speech

65 Public Interest Litigation (L) No. 14204 of 2021.

66 *Agij Promotion of Nineteenonea Media Pvt. Ltd. v. Union of India, supra* note 63 at para 31.

> and expression, if they are made to live in present times of content regulation on the internet with the Code of Ethics hanging over their head as the Sword of Damocles. This regime would run clearly contrary to the well-recognized Constitutional ethos and principles."[67]

The High Court of Bombay therefore, stayed the operation of sub-rules (1) and (3) of Rule 9. However, the court did not stay Rule 7 of the 2001 Rules as the petitioner had not demonstrated that they were an intermediary as defined under section 2(w) of the IT Act. The court emphasized that Rule 9 was an exception to the general presumption of subordinate legislation's constitutionality and did not comply with the IT Act's provisions or the constitutional rights guaranteed under article 19(1)(a). Finally, the court emphasized that subordinate legislation could not transgress the powers occupied by different statutes.[68]

In yet another petition titled *Digital News Publishers Assn.* v. *Union of India*[69] before High Court of Madras filed by TM Krishna and Digital News Publishers Association (DNPA) against the IT Rules 2021, which is similar to the High Court of Bombay case.[70] The court noted that the sub-rules (1) and (3) of Rule 9 of the IT Rules 2021 have already been stayed by the High Court of Bombay, and this stay order should have a pan-India effect, so there was no need for an independent order. However, the petitioners argued that they had received notices requiring them to comply with the IT Rules and Rule 9. The digital news platforms expressed concern over the three-tier grievance redressal mechanism, which gives excessive power to government officials to punish them. This mechanism involves self-regulation by publishers in the first level, self-regulating bodies established by publishers in the second level, and oversight by the Central Government in the third level. The petitioners were specifically concerned about sub-clause (x) of Rule 3(1)(b) which states that:[71]

> "(x) is patently false and untrue, and is written or published in any form, with the intent to mislead or harass a person, entity or agency for financial gain or to cause any injury to any person;"
>
> The petitioners argued that this provision, along with the requirement for intermediaries to terminate access or usage rights for non-compliance[72], and the strict grievance redressal mechanism, creates undue pressure on intermediaries. Additionally, Rule 7 makes intermediaries liable for punishment if they fail to comply with the aforementioned rules.

Section 79 of the Information Technology Act provides protection to intermediaries from liability in certain cases. However, this exemption would not apply if the intermediary does not observe the guidelines prescribed by the Central

67 *Ibid.* at para 28

68 *Ibid.*

69 *Id* . at para 31.

70 2021 SCC OnLine Mad 16337(Decided on Aug. 14, 2021).

71 *Agij Promotion of Nineteenonea Media Pvt. Ltd.* v. *Union of India, supra* note 63.

72 R. 3(1)(b).

Government. In *Shreya Singhal* v. *Union of India,*[73] it was observed that any unlawful acts beyond what is laid down in article 19(2) of the Constitution cannot form any part of section 79 of the Act. The Supreme Court has acknowledged in the judgment that it would be challenging for intermediaries such as Google and Facebook to determine the legitimacy of the millions of requests they receive.

The High Court of Madras noted that there is a "substantial basis" for assertions that Rule 9 violates article 19(1)(a) of the Constitution and may be applied to intermediaries coercively. In accordance with this, the Madras High Court on 16th September 2021 issued an interim order that any action under Rules 3 and 7 would be subject to the outcome of the challenge of constitutional validity as the main matter was likely to be taken up by the Supreme Court in coming days. Pursuant to requests from the Central Government, the Supreme Court has transferred cases for regulation of content on OTT Platforms pending in different high courts to the Supreme Court, and has passed orders prohibiting the relevant high courts from hearing these cases while they are pending before the Supreme Court.[74]

In the case of *Omanakuttan K.G.* v. *Union of India,*[75] the petitioner filed a writ petition in the public interest, seeking various reliefs, including mandamus or other appropriate writs to compel WhatsApp to comply with the IT Rules, 2021 and to prohibit the reliance on WhatsApp contents by investigating agencies and courts. The petitioner raised concerns about user manipulations, lack of security, traceability of messages, and compliance with the IT Rules, 2021, citing the right to privacy. WhatsApp argued that it is not bound by the IT Rules, 2021 due to end-to-end encryption and that the Rules infringe upon the right to privacy.

The court, considering the provisions of the Rules, observed that the petitioner made vague allegations without providing supporting evidence. It noted that the government has already made provisions in the Rules to regulate and control the platform in question. The fact that the Rules are being challenged in the High Court of Delhi does not automatically entitle the petitioner to the mandamus requested in prayer.

The court refused to grant the petitioner's requests for directions to investigating agencies or courts to not rely on WhatsApp contents in their functioning, as it would interfere with the statutory framework of the criminal justice system, and the registrar general does not possess supervisory powers in this regard.

The court found that the petitioner disregarded core judicial aspects and sought directions that exceeded the comprehension of the Constitution and laws concerning the issue of end-to-end encryption. It deemed it premature to issue the mandamus as sought by the petitioner and concluded that the petitioner failed to demonstrate any arbitrariness or illegality on the part of the respondents, justifying judicial review. Accordingly, the court dismissed the writ petition, and the petitioner's request for a writ of prohibition was deemed unwarranted.

73 R. 3(1)(c), 2021 IT Rules.

74 (2015) 5 SCC 1.

75 *Union of India* v. *Sudesh Kumar Singh*, Transfer Petition (C) No. 100-105/2021).

Removal of content posted unlawfully from pornographic websites and de-indexing from search engine results

The High Court of Delhi in *X* v. *Union of India*[76] heard a case involving a woman (referred to as X) whose photos were posted on a pornographic website without her consent. Despite court orders to remove the content, it continued to resurface on the internet. The court appointed an advocate as amicus curiae to address the issue. The Delhi Police requested directions to intermediaries, under sections 79(3)(a) and (b) of the IT Act, to remove and prevent the posting of unlawful content and to share actual unlawful content, metadata, data dump, and basic subscriber information for investigation purposes. Google argued that search engines are not publishers but only index existing information, and they should only remove specific URLs upon request. They emphasized the need to consider context and avoid pre-emptive banning of content as it would jeopardize free speech and be contrary to the law quoting para 62 and 66 from *Myspace.*[77] ISPAI stated that blocking content at the sub-page level is technically challenging due to encryption mechanisms and suggested global source blocking at the content provider level. The Ministry of Electronics and Information Technology suggested granting petitioners the right to request content removal. The court discussed the extraterritorial jurisdiction of the IT Act, the responsibilities of intermediaries, and the exemptions (as outlined in section 79(1) and Rule 10 of the 2009 Rules) and liabilities (sections 67, 67A, and 67B) outlined in the Act and the 2021 IT Rules. The court emphasized the need for intermediaries to expeditiously remove or disable access to offending content upon receiving 'actual knowledge' as held in *Shreya Singhal* case.

The court appointed *amicus curiae*[78] highlighted the relevant provisions of the Information Technology Act, 2000, as amended, and the associated rules, including the 2021 Rules, which have increased the liabilities and obligations of intermediaries in dealing with unlawful content. The 2021 Rules have set a shorter timeframe of 24 hours for removing or disabling access to such content. Failure to comply with these rules can result in the revocation of the intermediary's liability exemption. The *amicus curiae* also referenced legal precedents from both Indian and foreign jurisdictions that address intermediary liability and the responsibility to remove unlawful content.

The court proposed directions to ensure the effective removal of unlawful content while balancing the obligations of intermediaries and the rights of victims.[79] These directions include immediate content removal within 24 hours of a court order, preservation of information related to the content, de-indexing by search engines, proactive monitoring by intermediaries, information sharing with law enforcement, removal from other platforms upon request, filing complaints on the National Cyber-Crime Reporting Portal, and potential liability for non-compliance with court orders. These measures aim to strike a fair balance and facilitate meaningful compliance without placing undue burden on intermediaries.

76 2021 SCC OnLine Ker 2758(decided on June 28, 2021).

77 2021 SCC OnLine Del 1788.

78 *Myspace Inc* v. *Super Cassettes Industries*, 2017 (69) PTC 1 (Del) (DB).

The court ordered the petitioner to provide information to the Investigating Officer within 24 hours. The Delhi Police/CyPAD Cell was instructed to remove/ disable access to the content within 24 hours. Search engines were directed to de-index the content globally and disable access to identical content on other platforms within 24 hours. The investigating officer was tasked with sharing relevant URLs with other entities. The Delhi Police was instructed to obtain necessary information from websites and search engines. The petitioner can request removal of similar content from other platforms, with corresponding directions to the investigating officer. Non-compliance will result in loss of exemption and liability under the IT Act. Parties can seek clarification from the court if needed.

Intermediary liability on e-marketplaces

The central issue in *Kunal Bahl* v. *State of Karnataka*[80] case was whether an intermediary (the online marketplace www.snapdeal.com here) would be held liable for the sale of drugs that did not comply with the requirements under the Drugs and Cosmetics Act, 1949. The complaint was filed by the Inspector of Drugs based on information received from the Deputy Drugs Controller, Mysore. It alleged that a seller on Snapdeal's platform had sold SuHAGRA-10P tablets. Since Snapdeal did not possess a license to sell drugs, it was accused of violating section 18(c) of the Drugs and Cosmetics Act, 1940, which is punishable under section 27(b)(ii).

Snapdeal argued that it has fulfilled its obligations as an intermediary under the Information Technology Act, 2000 and the Intermediaries Guidelines Rules, 2011. It claimed exemption from liability under section 79 of the Act for the following reasons:

i. Snapdeal had no involvement in the specific transaction in question.
ii. Snapdeal merely provides a platform for communication and information sharing between sellers and buyers. The information about the products offered for sale by the accused seller was made available on Snapdeal's online marketplace.
iii. As an intermediary, Snapdeal does not have control over the content posted by users on its platform.
iv. Snapdeal has exercised "due diligence" as required by Section 79(2)(c) of the Information Technology Act, 2000, along with the Intermediaries Guidelines Rules, 2011.

Snapdeal argues that as an intermediary, its liability under section 79(3)(b) of the Information Technology Act, 2000 is limited to the removal of third-party content upon receipt of a court order or notice from a government authority. It cannot be held responsible for the listing and sale of products by independent third-party sellers on its marketplace. Snapdeal cited the decisions in *Sharat Babu Digumarti* v. *Govt. (NCT of Delhi)*[81] and *Shreya Singhal* v. *Union of India*[82] to support its position.

79 *Supra* note 76.

80 *X* v. *Union of India supra* note 76 at para 90

81 2021 SCC OnLine Kar 15706(decided on Jan. 7, 2021).

82 (2017) 2 SCC 18.

Snapdeal also pointed out that the Consumer Protection (E-Commerce) Rules, 2020 have introduced a distinction between marketplace e-commerce websites (like Snapdeal, Amazon, and Flipkart) and inventory e-commerce websites (such as Lifestyle and Decathlon). Rule 5(1) of the Consumer Protection (E-Commerce) Rules, 2020[83] states that in order to claim exemption under section 79 of the Information Technology Act, 2000, marketplace e-commerce entities like Snapdeal must comply with the requirements of subsections (2) and (3) of section 79, as well as the Information Technology (Intermediaries Guidelines) Rules, 2011.[84]

The High Court of Karnataka ruled that an intermediary, as defined in section 2(w) of the IT Act, along with its directors and officers, cannot be held responsible for any action or inaction taken by a vendor or seller utilizing the services provided by the intermediary through a website or marketplace.

Court extensively discussed various provisions of the Cr PC, Information Technology Act, and Drugs and Cosmetics Act. In the context of Section 18(1)(c) of the Drugs and Cosmetics Act, 1940, it is essential for an individual to engage in activities such as manufacturing, distributing, stocking, exhibiting, or offering for sale without possessing a valid license issued under the Act. Therefore, neither Snapdeal nor its directors can be held liable for an offense punishable under section 27(b)(ii) of the Act.

It concluded that no offense was established against the accused, leading to the allowance of the petitions and the quashing of the criminal proceedings initiated against the accused in question.

Snapdeal/accused no.2 cannot be held responsible for the sale of non-compliant items under the Drugs and Cosmetics Act, 1940. The court found no offense and quashed the criminal proceedings against Snapdeal and its directors.

In *Sanatan Sanastha* v. *Union of India,*[85] a registered public charitable trust, claiming to be a Non-Governmental Organization (NGO), had filed a petition against Facebook (respondents no. 3 and 4). The petitioner alleged that their Facebook pages, which were used to spread spiritual teachings, had been blocked by the respondents without providing any reasons or government orders. The petitioner argued that this action was arbitrary, violated their constitutional rights, and constituted an unauthorized exercise of power. During the proceedings, the petitioner received a communication from the respondents, citing their right to permanently disable accounts that breached Facebook's community standards. The petitioner amended the petition to include this communication and referred to a civil suit in the High Court of Delhi (CS (OS) 510 of

83 (2015) 5 SCC 1.

84 5(1) *Liabilities of marketplace e-commerce entities*. -

(1) A marketplace e-commerce entity which seeks to avail the exemption from liability under sub-section (1) of section 79 of the Information Technology Act, 2000 (21 of 2000) shall comply with sub-ss. (2) and (3) of that section, including the provisions of the Information Technology (Intermediary Guidelines) Rules, 2011.

85 *Ibid.*

2016) filed by *Sasikala Pushpa* v. *Facebook*.[86] Additionally, the petitioner challenged the constitutionality of section 79 of the Information Technology Act, 2000, alleging a violation of fundamental rights under articles 14, 19, and 21 of the Constitution.

The relief sought in this petition could not be granted because the constitutional validity of section 79 of the Information Technology Act had already been upheld by the Supreme Court in the case of *Shreya Singhal*. It was well-established that once the Supreme Court upheld the constitutional validity of a provision, the high court generally could not entertain a petition questioning the same provision based on new or rephrased grounds. Therefore, there was no basis for granting relief as requested in prayer clause D-1 of the petition.

The relief sought in prayer clause D-2 of the petition was also unclear. Declaratory relief could not be granted in a vacuum, and there was no ongoing proceeding where the respondents had claimed or been granted immunity based on the provisions of section 79 of the Information Technology Act. If there had been a breach of a contractual relationship between the petitioner and the respondents regarding the blocking of the petitioner's Facebook page, the appropriate course of action would have been for the respondents to seek redress through the appropriate forum. A petition under article 226 of the Constitution of India might not have been the appropriate remedy in such a situation. Therefore, the petition was dismissed with no order as to costs.

V IDENTITY THEFT- SECTION 66C

Section 66C of the IT Act provides for the punishment of identity theft. It stipulates that individuals who intentionally and dishonestly use someone else's electronic signature, password, or other unique identification feature to deceive or defraud others can be sentenced to a maximum imprisonment of three years and may also face a fine of up to 1 lakh Rs/-.

In *Ravari Kirankumar* v. *Home Department*[87] application was filed by the applicant under section 482 of the Cr PC, seeking the quashing of FIR and the subsequent charge-sheet claiming that the applicant has committed offenses punishable under sections 66A and 66C of the IT Act, 2000. However, upon careful examination of the complaint, FIR, and charge-sheet, it is evident that the accusations primarily revolve around the applicant sending objectionable emails from their email ID to various offices. Notably, there are no allegations regarding the use of electronic signatures, passwords, or any other unique identification features of another person. Therefore, there is no valid basis for registering an FIR under section 66C of the IT Act.

Moreover, the court observed that section 66A of the IT Act has been deemed unconstitutional by the Supreme Court in the case of *Shreya Singhal* (supra) therefore, no prosecution can be maintained under section 66A of the IT Act. Therefore, the FIR and charge-sheet invoking section 66A of the IT Act must be quashed and set aside. Considering the absence of any allegations regarding fraudulent or dishonest use of

86 (2021) SCC OnLine Bom 1049.

87 2020 SCC OnLine Del 618 (Decided on June 2, 2020).

electronic signatures, passwords, or unique identification features of another person, it is perplexing how any prosecution can be pursued under section 66C of the IT Act.

Upon examining the complaint, FIR, and charge-sheet, it becomes apparent that the sole allegations against the applicant involve the sending of objectionable emails on November 18, 2010 from their email ID, alert aa@redoffmail.com, to various offices of NSSO (FOD) in India. These allegations were likely made to invoke the provisions of section 66A of the IT Act, which was applicable at the time. However, throughout the entire complaint, FIR, and charge-sheet, there are no accusations pertaining to the use of electronic signatures, passwords, or any other unique identification features of another person. Consequently, there was no justification for registering an FIR under section 66C of the IT Act.

Therefore, it is imperative to quash the FIR and charge-sheet since the allegations in the FIR do not establish the commission of any offense under section 66C of the IT Act. Additionally, even if we assume the allegations to be true, they do not constitute an offense or establish a case against the applicant under section 66C of the IT Act. It is evident that the allegations do not fulfill the requirements for an offense under section 66C of the IT Act. Moreover, considering that section 66A has already been struck down and cannot be invoked, the FIR and charge-sheet must be quashed under these circumstances.

The appellant in *Santosh* v. *State of Madhya Pradesh*[88] case has been convicted under section 66C of the Information Technology Act, 2000. The conviction was based on the appellant's alleged involvement in sending fraudulent emails using a forged email ID. The complainant, G.B. Bamankar, filed a complaint stating that an email was forwarded to him by Ashish Dongare, which was sent from Pankaj Kanthed's email ID. However, Pankaj Kanthed denied sending the email and claimed that his email ID had been fraudulently created by someone else. Based on the complaint, an FIR was registered under various sections of the Indian Penal Code (IPC) and the IT Act. During the investigation, it was discovered that the appellant, Santosh Bharti, was the one who sent the email in question. The appellant was acquitted of some charges but convicted under section 66C of the IT Act. Aggrieved by the conviction, the appellant has filed this appeal.

The appellant's counsel contended that the prosecution's case suffered from a critical flaw: the absence of proper evidence. They argued that the email in question, which formed a crucial part of the prosecution's case, had not been certified in accordance with Section 65-B of the Evidence Act. This section stipulates that electronic records must be supported by a certificate to be admissible as evidence in court. In the absence of such certification, the email (Ex.P/2) could not be considered reliable or valid evidence. Upon careful examination of the record, the court concurred with the appellant's counsel. It observed that the email in question was merely a photocopy of the forwarded email sent to the complainant, and this photocopy (Ex.P/2) was not accompanied by the required certificate under section 65-B. The court emphasized that the absence of certification was fatal to the prosecution's case, as it

88 2021 SCC OnLine Bom 4086.

undermined the authenticity and admissibility of the email as per Supreme Court ruling in *Anwar*.

Furthermore, the court noted that the prosecution's witness, P.W.3 Ritesh Singh, a constable in the cyber cell, did not provide any substantial testimony regarding the email (Ex.P/2). His examination-in-chief remained silent on this crucial document, and although he was not cross-examined on the matter, the court deemed it inconsequential. The primary responsibility of the prosecution was to establish the admissibility and authenticity of the evidence, which they failed to do. The court referred to the Supreme Court's decision in the case of Anvar P.V., which emphasized that a mere printout or photocopy of an electronic record cannot be admitted as evidence without a certificate under section 65-B.

Considering the lack of certification for Ex.P/2, the court concluded that the prosecution had not succeeded in proving the appellant's guilt beyond a reasonable doubt. It further criticized the trial court for failing to address this crucial aspect and proceeding to decide the case on its merits, which was deemed improper.

In light of these findings, the court allowed the appeal, set aside the impugned judgment, and acquitted the appellant. It deemed it unnecessary to delve into the other grounds raised by the appellant, as the lack of certification alone was sufficient to undermine the prosecution's case and warrant the appellant's acquittal.

VII ONLINE PRIVACY

In the case of *Manohar Lal Sharma* v. *Union of India,*[89] the Supreme Court of India ordered an independent investigation into unauthorized surveillance using the Pegasus software. A committee comprising three technical experts[90] was appointed to probe the matter, assess the targeting of Indian citizens' devices, review the software's acquisition, and provide recommendations for strengthening cyber security and privacy protection. Raveendran J., oversaw the committee's functioning, ensuring adherence to procedures and thorough investigations. The court emphasized the importance of privacy, constitutional restrictions, and the balance between national security and individual rights. It expressed concerns about the potential impact on free speech and the need to protect democratic values in the face of emerging technologies and surveillance practices.

The court acknowledged privacy limitations but emphasized that restrictions must align with the constitution. It rejected the government's request for unrestricted immunity in the name of national security. The court expressed concerns about the influence of surveillance on free speech and the potential for self-censorship. It underscored the importance of privacy, constitutional restrictions, and balancing national security with democratic values in the face of emerging technologies and surveillance practices.

89 2021 SCC OnLine MP 686.

90 2021 SCC OnLine SC 985(Decided on Oct. 27, 2021).

V CONCLUSION

Over the past decade, the internet has become widely accessible in India, leading to a significant increase in digital connectivity and the growth of the digital economy. The COVID-19 pandemic further accelerated the use of social media platforms and information sharing. However, this resulted in several challenges like spread of fake news causing riots and mob lynching and the stifling of voices against oppression. Lack of transparency and accountability in dealing with malicious content on social media platforms added to the rising discontent among society. Additionally, the rise of OTT platforms for entertainment has highlighted the need for content regulation.

In 2021, several noteworthy events shaped the landscape of cyber law in India. WhatsApp's privacy policy revision faced backlash for allowing the sharing of sensitive personal data, while the Indian government introduced the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 under section 87 of the Information Technology Act, 2000. These rules aimed to increase accountability for social media platforms, establish a self-regulatory framework, and address concerns regarding digital content and OTT platforms.

The Rules differentiate between social media intermediaries and significant social media intermediaries, aiming to promote innovation and facilitate new platform growth. Significant social media intermediaries have additional due diligence measures and face criminal consequences for non-compliance. These Rules address concerns about digital content on digital media and OTT platforms. The Ministry of Information and Broadcasting oversees these issues, while the Information Technology Act governs the regulatory framework. The Rules establish a self-regulatory framework and a Code of Ethics for news publishers and OTT platforms. A three-tier grievance redressal mechanism is in place. However, concerns have been raised about potential threats to press freedom and media due to the allocation of adjudicatory powers to the executive branch.

In 2020, the government issued several content takedown and blocking orders without providing adequate explanations. The 2021 IT Rules now require reasons for takedowns to be discussed and offer a grievance redressal mechanism to challenge government actions. Intermediaries have greater responsibilities, including due diligence, monitoring, and user education. The Rules aim to foster a culture of self-regulation among social media intermediaries, supported by artificial intelligence tools.

High courts received multiple public interest litigations challenging the constitutionality of certain provisions in the IT Rules, 2021. The High Court of Mumbai granted a stay on the rules related to digital publishers, stating that Rule 9 goes beyond the scope of the IT Act. Specifically, Rule 9(1) and Rule 9(3) were stayed as they were deemed to exceed delegated power and infringe upon the constitutional right to freedom of speech and expression. This decision had a pan India effect, being accepted by other high courts.

The *X* v. *Union of India* judgment is praised for its lucid exposition of the procedure and guidelines for intermediaries and government agencies to remove offensive content from digital platforms in accordance with the IT Rules, 2021. The

judgment addressed concerns of individuals facing victimization through the posting of obscene content about them online. While the victim's photographs taken from her social media accounts were not obscene, their unauthorized posting on a pornographic website made them offensive by association.

The landmark judgment in *Arjun Panditrao Khotkar* v. *Kailash Kushanrao* by the Supreme Court was believed to have settled the jurisprudence on the admissibility of electronic evidence, restoring *Anwar* ruling. However, the current stance of the Supreme Court suggests that WhatsApp messages may not be considered admissible evidence due to concerns about their authenticity and potential tampering. The court has expressed reservations about the evidential value of such messages, considering that they can be easily created, modified, or deleted by anyone. Nevertheless, with the existence of the Information Technology Act, 2000 and the continuous advancements in the field, it is anticipated that there will be significant progress in the regulatory framework regarding electronic evidence in the future.

In the ongoing process of finalizing the long-awaited data protection legislation, progress has been made with the submission of the Joint Parliamentary Committee's report on the Personal Data Protection Bill, 2019 to both Houses of Parliament. The committee has endorsed the bill with certain observations, suggesting the need to broaden its scope to include non-personal data. It has also supported exemptions for certain government agencies from the applicability of the data protection law on specified grounds, despite dissenting opinions expressing concerns about constitutional violations and the potential creation of separate ecosystems. The report is currently in the hands of the Indian government, and it remains to be seen how the government will incorporate the committee's recommendations into a revised version of the Data Protection Bill.[91]

The Pegasus controversy of 2021 sparked substantial attention and legal discourse in Indian cyberspace. The Supreme Court's response,[92] which recognized the right to privacy as a fundamental right and called for independent investigations, elicited contrasting viewpoints. Critics argue that the court's actions may encroach upon the executive's authority over national security and surveillance. They raise concerns about the court's lack of technical expertise in appointing an investigative committee and the potential ramifications for counterterrorism efforts, including operational challenges and delays. Nonetheless, this judicial decision empowered the courts to scrutinize matters of national security and public interest, thereby contributing to the ongoing development of cyber legal jurisprudence in India.

While the Pegasus controversy did generate significant attention and legal discussions in Indian cyberspace in 2021, it is important to note that the response from the Supreme Court and acknowledgement of the right to privacy as a fundamental

91 The committee consisted of three technical experts: Naveen Kumar Chaudhary(Dean of National Forensic Sciences University,Gujarat) , Prabaharan P (Professor at Amrita Vishwa Vidyapeetham, Kollam, Kerala) and Ashwin Anil Gumaste(Associate Professor at the Indian Institute of Technology, Bombay).

92 Pawan Duggal.

right and its order for independent investigations[93] could be seen as encroachment upon the executive's domain of national security and surveillance. Concerns could be raised about the court's lack of technical expertise in appointing a committee to investigate the Pegasus software and the possible implications for counterterrorism efforts, including delays and operational challenges. However, this decision empowered the courts to examine matters of national security and public interest but also contributed to the ongoing development of cyber legal jurisprudence in India.

In 2021, a significant development emerged with the introduction of the crypto currency and Regulation of Official Digital Currency Bill, 2021. The primary aim of this bill is to establish a comprehensive framework for the official digital currency issued by the Reserve Bank of India. Additionally, the bill seeks to prohibit the use of private crypto currencies in India, while allowing certain exceptions to support crypto currency technology. Its overall objective is to bring consistency and regulation to the crypto currency market, replacing private crypto currencies with an official digital currency and enforcing stringent penalties for non-compliance. The implementation of effective regulation would not only facilitate taxation of crypto currency revenue but also generate advantages for both the government and investors. These advancements set the stage for future changes and progress in the dynamic field of cyber law, warranting careful observation.

93 *Manohar Lal Sharma* v. *Union of India* Civil/Criminal Jurisdiction Writ Petition No. 314 of 2021

94 *Manohar Lal Sharma* v. *Union of India* Civil/Criminal Jurisdiction Writ Petition No. 314 of 2021