11

CYBER LAW

Deepa Kharb[*]

I INTRODUCTION

THIS SURVEY explores the changing landscape of cyber law by examining key judicial decisions by the apex court and various high courts for the year 2022. It focuses on important topics like intermediary liability, online privacy and right to be forgotten, admissibility of electronic evidences and regulation of obscenity in cyber space offering valuable insights into how cyber law is evolving in India. It highlights several important principles that have been added to the existing body of knowledge.

Serving as a practical guide, the survey helps navigate the complex challenges of the digital world. It also evaluates the courts' reasoning, highlighting areas that may spark further discussion. Overall, the survey emphasises the dynamic nature of cyber law and its significant influence on the legal system, showcasing the judiciary's efforts to keep pace with the challenges of the digital age.

II ADMISSIBILITY OF ELECTRONIC EVIDENCE: SECTION 65B IEA

In today's digital world we are witnessing technological transformations in every field, revolutionizing communication, business operations as well as personal interactions. Electronic devicesare becoming more sophisticated and increasingly being used and relied upon as electronic evidences these days. At the same time the technological advancement has facilitated the tempering of electronic records, raising concerns regarding their integrity.

Reliability of electronic record always pose challenge before the courts of law especially in the context of their admissibility as evidence. Time and again the Supreme Court in last few years has made important strides in clarifying and establishing rules through *Anvar P.V.* v. *P.K. Basheer,*[1]thereafter in *Shafhi Mohammad* v. *State of H.P*[2] and recently in *Arjun Panditrao Khotkar* v. *Kailash Kushanrao Gorantyal*[3] especially around the requirement of certificate under section 65B of Indian Evidence Act,1872 (IEA hereafter)for the admissibility of

* Assistant Professor (SS), Indian Law Institute.

1 (2014) 10 SCC 473.

2 (2018) 2 SCC 801.

3 (2020) 7 SCC 1 at 62.

electronic evidence. However, this uncertainty continue to fuel the debate around the issue in the courts and academia.

In the case of *Ambika Roy* v. *Speaker, West Bengal Legislative Assembly and Suvendu Adhikari* v. *Speaker, West Bengal Legislative Assembly,*[4] the petitioner alleged defection by Mukul Roy, providing electronic evidence such as newspaper reports and video recordings, accompanied by a section 65B certificate. Despite this, the Speaker dismissed the certificate and the electronic evidence without a proper explanation. The court stressed that the speaker had a duty to consider such certificates and provide reasons for acceptance or rejection. The speaker's order, particularly para 79, rejected the electronic evidence citing the absence of a certificate on the terms of section 65B.

The court suggested a different conclusion may result if electronic evidence is deemed admissible and thoroughly examined. The IEA, section 65B, mandates a certification process for the admissibility of electronic records, ensuring that the electronic data is reliable and authenticated.

In the notable judgment of *Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal,*[5] the court ruled that while section 65B(4) certification is mandatory, there are exceptions, such as when a certificate is unattainable from a third party:[6]

> On an application of the aforesaid maxims to the present case, it is clear that though s. 65-B (4) is mandatory, yet, on the facts of this case, the respondents, having done everything possible to obtain the necessary certificate, which was to be given by a third party over whom the respondents had no control, must be relieved of the mandatory obligation contained in the said sub-s. 52. We may hasten to add that s. 65-B does not speak of the stage at which such a certificate must be furnished to the Court. In *Anvar P.V*., this Court did observe that such a certificate must accompany the electronic record when the same is produced in evidence. We may only add that this is so in cases where such a certificate could be procured by the person seeking to rely upon an electronic record. However, in cases where either a defective certificate is given or in cases where such certificate has been demanded and is not given by the person concerned, the Judge conducting the trial must summon the person/ persons referred to in s. 65-B(4) of the IEA, and require that such certificate be given by such person/persons. This is what the trial Judge ought to do when the electronic record is produced in evidence before him without the requisite certificate in the aforementioned circumstances. This is, of course, subject to discretion being exercised in civil cases in accordance with law and in accordance with the requirements of justice on the facts of each case. When it

4 2022 SCC OnLine Cal 732(Decided on April 11, 2022).

5 *Arjun Panditrao* Khotkar v. *Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.

6 *Id.*at 51.

> comes to criminal trials, it is important to keep in mind the general principle that the accused must be supplied all documents that the prosecution seeks to rely upon before commencement of the trial, under the relevant sections of the Cr PC.

The court observed that section 65B does not expressly specify at what stage the certificate must be submitted before the court and *Anwar* ruling only required such certificate to accompany the electronic evidence when submitted. Where a tribunal or courtinfers that the certificate is flawed or defective, it may on its discretion in a civil matter, call upon and seek clarification from the individuals mentioned under s.65Band require that such certificate be given by such person/ persons.Though, in criminal matters, the prosecution is required to supply all documents to the accused before commencement of trial as a general principle.

In the present case, speaker's failure to properly acknowledge and evaluate the section 65-B certificate provided by the petitioner led to the dismissal of crucial electronic evidence, which in turn flawed the speaker's decision, calling for a judicial review on account of perversity.

Hence, the court held that the certificate needs to be reappreciated by the Speaker as per legal procedures instead of having the court examine it for the first time during writ jurisdiction. By doing so, the speaker could reconsider the electronic evidence within the appropriate legal framework, ensuring a more thorough and just assessment. This approach, according to the High Court of Calcutta, better upholds the principles of law.

In another landmark case, *Sudesh Kaushik* v. *CBI*,[7] the appellant challenged the non-production of original electronic devices and the lack of a 65B certificate for CDRs in a corruption case. The absence of the certification for electronic evidence led to a debate about whether the evidence was admissible,given the strict mandate set by *Anvar P.V.* v. *P.K. Basheer,*[8] where non-compliance with section 65B renders electronic evidence inadmissible. Section 65B prevails over general provisions for secondary evidence, and non-compliance renders electronic records unacceptable. Thus, CDs presented without a section 65B certificate cannot be admitted as evidence, leading to the dismissal of the case related to corrupt practices involving songs, announcements, and speeches.

The Supreme Court, in its ruling in *Arjun Panditrao Khotkar,*[9] reinforced that sections 65A and 65B of the IEA dictate the admissibility of electronic evidence. Specifically, a certificate under section 65B(4) is mandatory for admitting secondary electronic evidence. However, where the witness produces the original electronic device which recorded the information or communication, the need for this certificate becomes redundant. The court acknowledged that these legal precedents were set after the events of the case in question. The court pointed out that the trial court failed to properly consider the admissibility of the electronic evidence despite the

7 2022 SCC OnLine Del 4300(Decided on Dec. 8, 2022).

8 (2014) 10 SCC 473.

9 *Arjun Panditrao* Khotkar v. *Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.

clear statutory requirements. The unclear methods by which data was transferred between devices and the investigative agency's inadequate handling of evidence cast serious doubts on the reliability of the transcripts from various recorders and cassettes.

The judgment was further influenced by multiple flaws in the prosecution's case, such as irregularities in obtaining prosecution sanctions, contradictory witness statements, the absence of key witnesses, and unreliable electronic evidence. The culmination of these issues, along with the failure to conclusively prove the bribery allegations beyond a reasonable doubt, led to the acquittal of the appellant. As a result, the court overturned both the conviction and the sentencing orders.

In *M. Sudheer* v. *M. Kamaraj,*[10] the petitioner sought to introduce a pen drive containing key evidence during the trial, asserting that the section 65B certificate could be produced later. The court accepted the argument based on *Union of India* v. *CDR Ravindra V. Desai,*[11] which held that non-production of the certificate is a curable defect. The respondent raised objection against admitting the pen drive, claiming it was not presented earlier in the trial. The respondent countered, alleging delay tactics. The court heard both sides' arguments but stressed the importance of raising objections related to the method of proof at the time when the document is marked as an exhibit.

In *Arjun Panditrao Khotkar* v. *Kailash Kushanrao Gorantyal,*[12] the court clarified that s. 65B of the IEA does not specify when the certificate for electronic evidence must be submitted. If the certificate is missing, the trial judge has the authority to summon the relevant person to produce it when the electronic record is introduced. Additionally, the court emphasised that under section 207 of the Criminal Procedure Code (CrPC), the prosecution must ensure that all documents are fully disclosed to the accused before the trial begins.

The court also acknowledged that while the prosecution cannot generally correct gaps in evidence during the trial, it may be allowed to submit additional documents if they were initially omitted by mistake. Therefore, failing to provide a section 65-B certificate at the charge-sheet stage does not automatically weaken the prosecution's case. This legal framework serves the dual purpose of ensuring procedural fairness and allowing for the correction of mistakes, thereby upholding the accused's right to a fair trial. By allowing the submission of a section 65-B certificate at any stage during the trial, the Court provides flexibility in the handling of digital records, acknowledging the potential complexities involved in gathering such evidence. At the same time, it categorises the need for the prosecution to follow proper procedures and avoid tactical delays, ensuring transparency and fairness in the trial process.

10 2022 SCC OnLine Mad 6809 : (2023) 1 Mad LJ 444(decided on Oct. 20, 2022).

11 (2018) 16 SCC 273.

12 *Arjun Panditrao* Khotkar v. *Kailash Kushanrao Gorantyal* (2020) 7 SCC 1.

A similar issue arose in *Ravichandra Gounder* v. *State Rep. by the Deputy Superintendent of Police,*[13] where the court emphasised the necessity of the section 65B(4) certificate for admissibility, yet the trial proceeded without this crucial certification. The incident involved a disagreement over political banners, leading to a community resolution affecting grocery sales to SC/ST individuals. The charges rely heavily on the electronic record from the respondent's mobile phone, requiring proper certification under section 65-B(4) for admissibility. Referring to the Supreme Court ruling in *Ravinder Singh* v. *State of Punjab*[14] highlights that oral evidence cannot replace the mandatory certificate under s. 65-B, as the law strictly demands such certification for electronic records. The judgment clarifies that the certificate is only unnecessary when the original device on which the information is stored is produced by its owner. However, when it is not feasible to physically present the computer system or network, compliance with section 65-B(1) and the accompanying certificate under section 65-B(4) becomes obligatory.

The judgment further emphasised that electronic evidence must meet statutory certification requirements to be admissible in court. In the present case, the petitioner argued that the trial court took cognisance of offences under the IPC and the SC/ST (Prevention of Atrocities) Act against the petitioners without fulfilling the necessary conditions under section 65-B(4). This failure to comply renders the electronic evidence inadmissible.

In summary, the petition highlighted the importance of procedural compliance with section 65-B(4) for the admissibility of electronic evidence. It referred to the Supreme Court's ruling on the necessity of proper certification and challenges the trial court's decision to proceed without fulfilling these conditions. The petition asserted that without proper certification, electronic evidence cannot be considered valid, and it questioned the trial's fairness in light of these lapses. The petition further contended that the complaint lacks specific allegations to substantiate the charges against the petitioners, suggesting that the complaint was retaliatory due to a prior dispute resolved by the Tahsildar. It criticised the charge sheet, which was allegedly based entirely on electronic evidence, for failing to comply with section 65-B(4), rendering the evidence inadmissible. The defence argued that the absence of certification undermines the trial's fairness, stressing the mandatory requirement for section 65-B(4) certification.

In essence, the petition insisted on strict adherence to procedural rules under section 65-B(4) for electronic evidence admissibility, challenging the trial court's decision to proceed without the required certification. It asserted that such evidence is invalid without compliance with statutory provisions. The petition referenced previous rulings to strengthen its position.

In *Ravinder Singh @ Kaku* v. *State of Punjab,*[15] a case involving the kidnapping and murder of two children, call records submitted by the prosecution

13 2022 SCC OnLine Mad 3504 : (2022) 4 Mad LJ (Cri) 42(Decided on July 6, 2022).

14 2022 SCC OnLine SC 541(Decided on May 4, 2022).

15 2022 SCC OnLine SC 541(Decided on May 4, 2022).

were deemed inadmissible due to non-compliance with section 65-B(4). The Supreme Court ruled that oral evidence cannot substitute for the certificate, and the high court erred in inferring a relationship between the accused and inadmissible call records. Additionally, the petition cited *Mohd. Arif* v. *State (NCT of Delhi*),[16] where it was held that proof of electronic records is a special provision introduced by the Information Technology Act, 2000, which amended several provisions of the IEA, further reinforcing the legal necessity of such certifications.

In contrast, *Manik Das* v. *Narcotics Control Bureau*[17] illustrated that the absence of a section 65B certificate might not preclude consideration of electronic evidence at the bail stage, allowing flexibility in specific contexts.

In family court proceedings in *Ritu Saigal* v. *Rakesh Saigal,*[18] the court accepted a CD as evidence under section 65B, emphasising that privileged communication between spouses under section 122 IEA does not apply in family courts as eclipsed by section14 of the Family Court Act, 1984. The court emphasised that since the appellant's wife led no evidence to challenge the correctness of the CD and its transcript, evidence was rightly accepted by the family court for deciding the issue of cruelty. The Family Courts Act allows the court to admit any evidence it deems necessary for resolving disputes.

In *Habu @ Sunil* v. *The State of Madhya Pradesh,*[19] a case involving rape and murder, the High Court of Madhya Pradesh scrutinised the prosecution's failure to present critical electronic evidence, such as CCTV footage and mobile phone records, which a witness mentioned during the trial. The witness claimed to have seen video footage of the events on the night of the incident, but this evidence was neither documented in the case diary nor produced in court. Despite having access to this material, the prosecution failed to submit it, raising concerns about the investigation's integrity.

The court noted that the non-production of CCTV footage and non-collection of crucial electronic evidence such as call records and SIM details from the accused was not a simple case of a flawed investigation but amounted to withholding of the best available evidence. In legal terms, this withholding could lead to an adverse inference against the prosecution under section 114(g) of the IEA, which permits the court to assume that evidence not produced would be unfavourable to the party responsible for its omission. The absence of this electronic evidence, especially when the prosecution's case was primarily built on circumstantial evidence, weakened its stance considerably.

The court also referred to sections 65A and 65B of the IEA, which lay down the requirements for the admissibility of electronic records as evidence. These sections demand proper certification under section 65B(4) when electronic records are used as secondary evidence. The high court emphasised that this procedural

16 2022 SCC OnLine SC 1509 (Decided on Nov. 3, 2022).

17 2022 SCC OnLine Cal 195.

18 FAO-4720-2017 (O and M) Punjab-Haryana High Court (Decided on March 4,2022).

19 2022 SCC OnLine MP 2017.

requirement is not a mere formality but a crucial safeguard to ensure the authenticity and reliability of digital evidence. Referring to the landmark case of *Anwar* v. *Bashir,*[20] the court reiterated that electronic documents must be proven in strict compliance with these provisions to be considered admissible in court. Failure to adhere to this procedure results in the exclusion of the electronic record, which could be crucial in determining the outcome of a case based on circumstantial evidence.

Across all these cases, the importance of Section 65B certification has become evident. The courts have oscillated between strict adherence to this requirement and providing some leeway where the evidence could still hold probative value despite procedural lapses.

III OBSCENITY

Section 67 punishes a person who publishes or transmits or causes to be published or transmitted in the electronic form, any material which is lascivious or appeals to the prurient interest or if its effect is such as to tend to deprave and corrupt persons on being exposed to it. After s.66A was declared unconstitutional in 2015,[21] section 67 is becoming the new section 66A due to unavailability of any specific provision under IT Act to cover cases of all kinds of objectionable and offending posts whether defamatory, hateful or distasteful. Further, the vague interpretation of the term "obscenity" ambiguous terms like "lascivious" and a lack of clarity regarding consent[22] have also contributed to unrelated cases being filed under section 67 every year. Section 67 and 67A of the IT Act were originally enacted with the intent of regulating explicit content in the digital era, seeking to protect individuals from offensive, obscene, or harmful material on the internet. However, with time, their misuse has brought to light a range of significant concerns that warrant in-depth consideration.

In *Niyaz Ahmad Khan* v. *State of U.P,*[23] the applicant shared two morphed objectionable posts regarding the Prime Minister and Home Minister leading to an FIR under section 67 of the IT Act. The applicant filed an application under section 482 Cr PC for quashing the criminal proceedings being abuse of process of law. The High Court of Allahabad observed that freedom of speech and expression is not absolute and is subject to reasonable restrictions to protect reputation of people and public interest. Indecent, false or defamatory statements which cause inconvenience, especially if persistent, can be deemed an offence. The right to freedom of expression on social media comes with responsibility and does not

20 (2014) 10 SCC 473.

21 *Shreya Singhal* v. *Union of India* (2015) 2 KLT 1 (SC).

22 S. 67 criminalises all acts depicting "obscene" activities without considering consent. This broad application can lead to wrongful cases that not only criminalise the portrayal of the human body but also misguide the identification of actual crimes and negatively impact the regulation of genuine obscene content. The presence or absence of consent should be a crucial factor in Section 67, as it impacts the government's role in regulating private consensual activities.

23 2022 SCC OnLine All 105.

permit irresponsible or abusive behaviour. Misuse of these platforms by travestying key-figures holding highest office in country individuals or spreading harmful content, damages reputations and harms society. There is an urgent need for stronger regulation to control such misuse. The government is directed to take action to prevent and address these issues, ensuring a respectful and healthy online environment.

Before assessing section 294 IPC, the court observed, it's crucial to consider section 67 of the IT Act, which deals with obscenity in electronic form. Referring to the Supreme Court ruling in *Sharat Babu Digumarti* v. *Government of Delhi (NCT)*[24] as quoted by Madhya Pradesh High Court in *Ekta Kapoor* v. *State of M.P.*,[25] that section 67 of the IT Act, being a special provision for dealing with obscenity in the electronic content, takes precedence over general provisions under section 292 IPC. The court went further elaborating that section 67 does not require knowledge of the content; thus, even without knowledge, publishing or transmitting obscene material falls under the said provision. Section 67 also does not exempt individuals from liability through a disclaimer. The applicability of section 67A depends upon whether the content is sexually explicit. To do that, it is necessary to first determine what sexually explicit acts actually mean, *i.e.,* whether an explicit act is limited to graphic depictions or if a simulated act of copulation can also trigger this provision.

The court held that there was enough justification to move forward given the facts, circumstances, and nature of the allegations, and a prima facie case is established. Reflecting on the applicability of the said provision the court held that it is for the prosecution to prove that the material is lascivious or appeals to prurient interest.It would be more appropriate for the trial court to address the contested question of facts and the accused's defence at the proper time rather than at this pre-trial stage.

However, in another case, *Alex Sine* v. *The State Represented by Inspector of Police, Kanyakumari District,*[26] the Madurai bench of the High Court of Madras went on to examine and decide on the question - whether the alleged act would constitute an offence under s.67 of the IT Act. The charge sheet filed under section 505(1)(b) of the IPC and section 67 of the IT Actalleged that the accused made vulgar and undesirable comments about the complainant and his private area on Facebook. The court was of the opinion that it would not fall within the definition of the word "lascivious" or the expression "appeals to the prurient interest" of the - readers. It cannot be said, as per the bench, that it tends to deprave and corrupt the persons as well. The act in order to be classified as obscene must arouse the sexual desire or provoke lustful thoughts of persons reading or seeing the publication. In the instant case, however, the court observed, there was no such allegation.

24 (2017) 2 SCC 18.

25 (2020) SCC OnLine MP 4581.

26 Crl.O.P.(MD)No.2316 of 2020.

To constitute an offense under section 67 of the IT Act, the material must be obscene by arousing sexual desire or provoking lustful thoughts, judged by contemporary community standards. A nude or semi-nude image alone does not qualify as obscene unless it is intended to excite sexual passion. The comments in question do not appear to meet these criteria and are not deemed to corrupt or deprave. Therefore, the court concludes that an offence under sectin 67 of the IT Act is not established.

In *Sri Shivanand Kalyani* v. *The State of Karnataka,*[27] the Youth Congress Committee head, Timmanagouda, filed a complaint against a defendant for offences under section 67 of the IT Act and sections 504 and 509 of the I.P.C. The complaint was based on an incident where the petitioner made a derogatory comment on the video of speech posted on MLA's facebook account reading "he is rowdy MLA". This comment, as per High Court of Karnataka, does not imply that obscene material is posted and transmitted by the petitioner and the section 67 is being erroneously applied.

In *Herold* v. *State of Tamil Nadu,*[28] petitioner posted on his facebook account a morphed photograph of the Chief Minister of Tamil Nadu and highly offensive remarks against the Hon'ble Minister of Public Works Department attracting charges under section 505(2) of I.P.C. and section 67 of the IT Act.

The Madurai bench of High Court of Madras observed that if the aforementioned clause(s) is carefully examined, it becomes clear that the legislator's only goal was to forbid the publication or transmission of pornographic material. The 1965 Constitution Bench in *Ranjit D. Udeshi* [*Ranjit D. Udeshi* v. *State of Maharashtra*, AIR 1965 SC 881] noted that the concept of obscenity changes over time, and the world can now tolerate more than formerly.[29] The principle of contemporary community standards and social values was reiterated in *S. Khushboo* v. *Kanniammal.*[30] The Indian Penal Code and IT Act uses the expression "lascivious and prurient interests" to determine obscenity, but the "community standard test" rather than "Hicklin test" is used instead.

According to section 292's sub-section (1), describes pornographic material as something which is lascivious, appealing to the prurient interest, and likely to deprave and corrupt those who see or hear it. Anything that provokes feelings of sexual desire or exposes an overt mentality is deemed offensive. A sex-related piece of content's obscenity is assessed using current social norms and the viewpoint of the average person.Applying the aforesaid test, the offending picture cannot be said to arouse any feeling of lust in any one. Therefore, the court held that the said offence was also not attracted. The FIR was hence quashed because the offending picture did not arouse feelings of lust.

27 CRL.P NO 102124 of 2018.

28 CRL.O.P.(MD)NO.18612 of 2021.

29 *Id* at para 11.

30 AIR 2010 SC 3196.

Sharing sexually explicit content- section 67A

Section 67A relates to the penalties for sharing explicit content in electronic format. In simpler terms, it addresses the act of publishing or transmitting material through digital means that involves sexual acts or behaviour.This section prescribes stricter penalties for sexually suggestive material when compared to section 67 hence its abuse is also noticed in last few years.

In *Archana Vijaykumar Baheti* v. *The State of Maharashtra*[31]theapplicant invoked the inherent jurisdiction of the Court under section 482 of the Code of Criminal Procedure to quash FIR along with the associated charge-sheet for offences under s. 509 of the IPC and s. 67-A of the IT Act. The informant (respondent no. 2) alleges that her father has an inappropriate relationship with the applicant, despite her and her mother's objections. She claims the applicant is harassing her by filing various complaints and forwarded a photo of her father kissing her, which she asserts has outraged her modesty, leading her to file a police report. The High Court of Bombay bench took observation that section 67-A of the IT Act pertains to the publication, transmission, or facilitation of materials that contain "sexually explicit acts or conduct" in electronic form. However, the Act does not define what constitutes a *'sexually explicit'* act or conduct. Generally, *"sexually explicit material"* refers to audio or visual content that predominantly depicts nudity or sexual acts in a lascivious manner. Upon examining the material in question, which allegedly outraged the informant's modesty, it was observed that the content in dispute is merely a photograph showing the informant's father kissing the applicant on the cheek. This image does not meet the threshold of being 'sexually explicit' as defined above. Prima facie essential ingredients for attracting either section 509 of IPC or section 67-A of the IT Act were not available hence dismissed the application.

Transmitting nude video of a person is an offence under the section 67A of the Information Technology Act

The High Court of Bombay denied anticipatory bail to a man accused of forwarding a married woman's nude video in *Esrar Nazrul Ahemad* v. *State of Maharashtra,*[32] determining that such conduct falls within the definition of "sexually explicit" as outlined in section 67A of the IT Act, 2000.

Bharati Dangre J., in her order asserted that "sexually explicit" encompasses not only sexual intercourse but also nude imagery. The court emphasised that the legislature's intent behind s. 67 was to address the publication and transmission of obscene material in electronic form, and this definition should not be narrowly construed. Referring to the case of *Pramod Anand Dhumal* v. *State of Maharashtra*[33] where the judge had an opportunity to deal with the similar situation *i.e.*, section 67-A and while construing the effect of section 67, the judge assigned definite meaning to the terms used therein and has also referred to the expression

31 CRI.APPLN-1505-2020.odt.

32 Anticipatory Bail Application No.1459 of 2022.

33 2021 SCC OnLine Bom 34 referred in para 8 of *Esrar Nazrul Ahemad* v. *State of Maharashtra(Ibid)*.

'explicit' as defined in Black's Law Dictionary as, '*Physical sexual activity or both persons engaged in sexual relations.'* Since the depiction of a woman in a nude form would definitely attract and would amount to obscene material and this being transmitted in electronic form, the argument of the accused's counsel that section 67-A *prima facie* does not attract does not hold the water at this stage.

IV INTERMEDIARY LIABILITY-SECTION 79

Intermediary liability in India is governed primarily by section 79 of the IT Act, which provides a framework for the liability of intermediaries concerning third-party content. Section 79 offers a "safe harbour" provision, shielding intermediaries from liability for third-party content as long as they follow due diligence. The jurisprudence surrounding this section has evolved significantly in the last decade, especially in the context of online platforms and the complexities of digital communication. The distinction between active and passive intermediaries has been a critical aspect of the jurisprudence. Courts have held that while intermediaries should not be required to monitor all user-generated content, they must act upon receiving specific complaints about unlawful content.

In *Neetu Singh* v. *Telegram FZ LLC,*[34] the petitioner, Neetu Singh, alongside K.D. Campus Pvt. Ltd., sought a permanent injunction, damages, and other reliefs against Telegram for the unauthorised dissemination of their copyrighted materials, including videos, lectures, and books. Singh, an author of competitive exam preparation books, and K.D. Campus, which operates coaching centres, alleged that their works were being shared without permission on various Telegram channels. Despite notifying Telegram and requesting the removal of infringing channels, some persisted, leading to the lawsuit.

Drawing from the *Myspace*[35] precedent, the court highlighted the safe harbour principle for intermediaries, emphasising compliance with legal requirements. Swift action against infringement is essential to prevent proliferation of unauthorised content channels, relieving courts of the burden of continuously issuing injunctions. Tracing the origin of infringing material and holding responsible parties accountable, including for damages, aligns with Telegram's role as an intermediary facilitating information exchange, without implicating its liability or safe harbour status.

Under section 79(3)(b) of the IT Act, Telegram was required to promptly remove unlawful material while preserving evidence. Rule 3 of the IT Guidelines mandates intermediaries to advise against copyright violations. Disclosing details of infringing channels or operators under a court order does not violate privacy or freedom of speech. Section 81 of the IT Act supplements the Copyright Act, requiring compliance with trademark laws outlined in the Intermediary Guidelines 2011. Provisions of the Trademark Act, such as sections 29, 101, and 102, aid in interpreting actions constituting trademark rights infringement, ensuring intermediaries are not immune from liability.

34 2022 SCC OnLine Del 2637: (2023) 93 PTC 515(Decided on Aug. 30, 2022).
35 CS (COMM) 282/2020.

Intermediaries, the court observed, are required to comply with copyright and trademark laws. While legitimate trademark use on genuine goods is allowed, services related to counterfeit goods may infringe on rights. The court noted that Telegram's server location in Singapore does not exempt it from liability, ensuring copyright owners can seek remedies within Indian jurisdiction. As technology evolves, legal frameworks must adapt to effectively address copyright and intellectual property violations. It highlighted that territorial boundaries should not impede justice, maintaining that Indian courts retain jurisdiction over such disputes, regardless of where the servers are located. As a result, Telegram (defendant no. 1) was directed to disclose information about the channels and devices involved in the distribution of infringing content, including mobile numbers, IP addresses, and email addresses, within a specified timeframe in a sealed cover. Any additional infringing channels identified must also be reported. Court reserved its right to review the information and issue further directions after hearing all parties involved.

In *Flipkart Internet Private Limited* v. *State of U.P*[36] a practicing lawyer from Ghaziabad, the fourth respondent (R4), filed an application under section 156(3) of the Code of Criminal Procedure (Cr PC) after receiving a laptop that did not match his order specifications. Following the seller's refusal to replace or refund the product, R4 lodged a criminal complaint with the Senior Superintendent of Police. When no action was taken, he sought the Magistrate's intervention, resulting in an order on January 14, 2019, directing the police to register a case regarding the product mismatch.

The petitioner-company approached the High Court of Allahabad seeking the quashing of the FIR, contending that it functions exclusively as an e-commerce platform that facilitates transactions between buyers and sellers on its website, *www.flipkart.com*. The petitioner emphasised its status as a non-party to these transactions, which are governed by terms mutually agreed upon by the users. It asserted that all commercial terms, including pricing and product specifications, are solely determined by the sellers, with the company making no representations regarding the quality of the products sold.

Claiming the status of an "intermediary" as defined under section 2(1)(w) of the Information Technology Act, 2000, the petitioner argued that it is exempt from criminal liability in relation to the transactions conducted on its platform. This assertion underscores the petitioner's role as a facilitator of sales rather than a direct participant in the commercial exchanges between buyers and sellers. The petitioner's position rests on the premise that, as an intermediary, it is insulated from liability for third-party actions, thereby reinforcing its claim for relief from the allegations set forth in the FIR.

The court observed that the petitioner clearly identifies as a marketplace intermediary rather than an inventory-based model, acting as a neutral platform without control over transactions or ownership of goods. The petitioner claims

36 2022 SCC OnLine All 706.

compliance with due diligence requirements under section 79 of the IT Act and the Intermediaries Guidelines Rules, informing sellers of their legal obligations.

Additionally, the court acknowledged the petitioner's argument that, under the Consumer Protection (E-Commerce) Rules, 2020, it qualifies for legal protections as long as it adheres to section 79. It maintained that any liability for violations rests with the sellers, while claims against its directors would be vicarious and unjust.

The court noted that, according to section 79(3)(b), an intermediary's only obligation is to remove third-party content upon receiving a court order or notice, which the petitioner asserts it has fulfilled. It concluded that there is no distinction between passive and active intermediaries concerning safe harbour provisions and found that the FIR did not adequately establish the necessary elements of the alleged offences against the petitioner-Company, therefore quashed.

In *Star India Pvt. Ltd.* v. *Aapkeaajanese.Net*[37] the Plaintiff, a leading entertainment and media Company in India and the owner of various television channels, filed an application before Delhi High Court seeking permanent injunction against unlawful and unauthorised distribution, broadcasting, rebroadcasting, transmission, and streaming of their original content by defendant nos. 1 to 67, collectively referred to as 'Rogue Websites',constituting infringement of their copyright. To substantiate their claims, the Plaintiffs engaged an independent investigator, Anurag Kashyap, whose findings revealed that the Rogue Websites have infringed their copyright by streaming, hosting, or facilitating the downloading and streaming of the Plaintiffs' original works.

Legal notices were dispatched to the Rogue Websites consequently demanding cessation of their infringing activities; however, the infringements persisted unabated. The Plaintiffs' counsel sought specific relief, referring to the ruling in *UTV Software Communication Ltd.* v. *1337X.,*[38] wherein the court similarly found the implicated websites culpable of copyright infringement under section 51 of the Copyright Act,1957. The court found the present case virtually similar to *UTV Software* and held that the websites were not entitled to exemptions under section 52(1)(c) of the Copyright Act or section 79 of the IT Act.

The court identified several illustrative factors to ascertain whether a website qualifies as a "rogue website." These factors include: the primary purpose of the website in facilitating copyright infringement; the severity of the infringement; the masking of registrant details, which obstructs identification; the website's silence or inaction in response to takedown notices; the existence of directories or indexes facilitating infringement; a general disregard for copyright by the website's operator; any court orders disabling access to the website due to copyright violations; guides or instructions that circumvent legal restrictions; the traffic volume or frequency of access to the website; and any other pertinent considerations.

37 2022 SCC OnLine Del 2663.
38 2019 SCC OnLine Del 8002.

Based on the evidence submitted and the aforementioned factors established in *UTV Software,*[39] it was concluded that there are sufficient grounds to categorise the websites of defendants nos. 1-67 as "rogue websites." The affidavit of Anurag Kashyap, also substantiated that the principal aim of these websites was to disseminate unauthorised and infringing content to the public. Additionally, the court observed that the registrant details for each website were masked, impeding the identification of either the registrants or the users.

Moreover, despite receiving legal notices, the defendants failed to comply with requests for the removal of infringing content. The presence of directories or indexes that facilitate copyright infringement is also noted. Evidence, including screenshots submitted with the Plaintiffs' documentation, corroborated the illegal availability of copyrighted content on these websites.

The court, based upon the evidence submitted and factors mentioned above , was convinced that there were sufficient grounds to categorise websites of defendants 1-67 as 'rouge websites' like in *UTV Software*, and to the issue of dynamic injunctions to the Plaintiffs for subsequent inclusion of mirror/ redirect/ or alphanumeric websites that provide access to the rogue websites by filing an application under Order I Rule 10 of the CPC, along with an affidavit providing evidence to effectuate such injunctions.

In *Kunal Bahl* v. *State of Karnataka*[40]the Directors of the Snapdeal Private Ltd., were accused of facilitating the sale of a drug, Suhagra 100mg, from their website without the necessary drug licenses in violation of the Drugs and Cosmetics Act, 1949. The petitioners asserted their immunity from liability for actions of third-party sellers on their platform under section 79 as intermediaries and contended exercise of due diligence on their part as mandated by IT Act and compliance with the applicable laws. The court reiterated that intermediaries cannot be held criminally liable for actions of vendors unless they are directly involved in the manufacturing and distribution of products. The court also took serious note of the five-year delay in filing the suit and warned that delays can lead to doubts about the legitimacy of the complaints and weaken the prosecution case as was explained by the Supreme Court in *State of Andhra Pradesh* v. *M. Madhusudhan Rao*.[41] Hence the court dismissed the proceedings against the petitioners aligning with prior decisions on similar issues.

The appellant-defendant in *Flipkart Internet Private Limited* v. *Indusviva Health Sciences Pvt Ltd*[42] filed an appeal against the order of session judge granting temporary injunction against the appellant prohibiting the appellant-defendant, its associated entities from soliciting, advertising, exhibiting, offering, endorsing, for sale, trade, or resale of current or future products of plaintiff company in print or electronic media, via the internet, or in any other way via these channels.

39 *Supra* note 37.

40 Crl.P. No.4676 of 2020 and Crl.P. No.4712 of 2020. (Decided on Feb. 24, 2022)

41 (2008) 15 SCC 582.

42 WP (Crl) 1376/ 2020 [Decided on July 29, 2022].

The respondent-plaintiff a private limited company and Direct Selling Entity (DSE) engaged in the direct sale of wellness and health products made by the relevant manufacturers filed a suit seeking permanent injunction for restricting appellant, an e-commerce platform, based on claims that it was soliciting, advertising, exhibiting, offering, and endorsing the sale of the plaintiff's products without written or oral consent.

The defendant contended that the suit is not maintainable as it is merely an intermediary, entitled to immunity under section 79 of the IT Act, 2000. Further it argues that the Direct Selling Guidelines (DSG), which the plaintiff relies upon, is only advisory and not binding.

The trial court granted temporary injunction against appellant who were hence constrained to file this appeal. Appellant's counsel, placing reliance on several judicial decisions,[43] argued that the trial court decision contradicted the law settled principles of law and statutory provisions, rules etc., governing intermediaries and as such, the impugned order deserves to be set aside.

The court held that the appellant was not directly selling hence is immune from section 79(2)(a) of the IT Act since its role is limited to mere providing a platform where third party conduct sales and thus not liable for third party infringements. Also, the court was convinced that appellant has observed due diligence as required under section 79(2)(c) of the IT Act and Rules thereunder.

The appellant, as per the court, is eligible for exemption under section 79(2)(a) of the IT Act as the appellant has not initiated transmission, selected receivers, or modified information in the transmission, as it does not create product listings, select buyers, or modify listing content. The plaintiff's claim against the appellant is liable to be rejected. The court also noted that the DSGs, which the trial court relied upon, are not enforceable law until adopted by the state government. Setting aside the trial court temporary injunction order the plaintiff's request for a temporary injunction was dismissed.

The ruling reinforced the legal protections for intermediaries and clarified the limitations of liability regarding user-generated content.

V RIGHT TO BE FORGOTTEN

In *Saleel Raveendran* v. *Union of India,*[44] a chartered accountant with over twenty years of experience challenged the publication of articles by The New Indian Express and India Kanoon, claiming they violated his rights to reputation, dignity, and privacy under articles 21 and 14 of the Indian Constitution. The petitioner, accused of sexual assault and rape—which he denies—argued that these publications sensationalised the allegations and suggested his guilt,

43 The counsel relied upon landmark judgments like *Shreya Singhal* v. *Union of India* (2015) 5 SCC 1; *Google India Private Limited* v. *Visaka Industries* (2020) 4 SCC 162; *Kent RO systems Ltd.* v. *Amit Kotak* 2017 SCC online Del 7201; *Amazon Seller Services Private limited* v. *Amway India Enterprises Private Limited* 2020 SCC Online Del 454; *Facebook Inc.* v. *Surinder Malik* 2019 SCC Online Del 9887 *etc*.

44 MANU/KE/3654/2023.

undermining his presumption of innocence and leading to job loss and family distress.

He sought the court's intervention under articles 226, requesting the removal and anonymisation of his details in connection with the allegations. The petitioner argued for anonymity for the accused during investigations, similar to the protections afforded to victims, citing the need to maintain dignity and privacy.

In response, the counsel for the media contended that press freedom, guaranteed by article 19(1)(a), allows for reporting on court proceedings. The court recognised the tension between media freedom and the rights of the accused, emphasising responsible reporting, especially in sensitive cases.

The court referred to the *Kaushal Kishor* ruling,[45] affirming that no additional restrictions on free speech can be imposed beyond those outlined in article 19(2). It highlighted the need to protect privacy and the right to a fair trial while acknowledging the media's role in public accountability.

The court found that the publication identifying the petitioner violated the Criminal Procedure Code (Cr PC) as it lacked necessary court approval. Consequently, it ordered the removal of the offending article and mandated that any future publications regarding this case adhere to confidentiality requirements.

Ultimately, the court ruled that:

(i) Respondent No. 3 must not publish related information without court permission.

(ii) Respondent No. 4 must anonymise the petitioner's details in the online publication.

In *Mahendra Kumar Jain* v. *State of West Bengal*[46] the petitioner challenged a memo from the Assistant Commissioner of Police that disclosed WhatsApp chats and photographs between his late daughter, Rashika Jain who died under mysterious circumstances in February 2021 and Abhishek Padia. A criminal proceedings was hence going on between the Jain and Agarwal families.

Mahendra Kumar Jain argued that the disclosure violates the Right to Information Act (RTI) because of the ongoing investigation into the Alipore P.S. Case, which requires confidentiality. He cited police regulations protecting witness statements and claims this breach infringes Articles 19 and 21 of the Constitution.

On the other hand, the Agarwal family contended that the information was essential for their defence in the Kalighat P.S. Case related to missing jewellery, by referencing witness statements involving Abhishek Padia, asserting that the RTI Act does not prohibit disclosing necessary evidence. The state's counsel submitted that the disclosed documents are considered public information, losing their private status, and the police maintains impartiality in the investigation.

45 (2023) 4 SCC 1.

46 2022 SCC OnLine Cal 3060.

In this context, High Court of Calcutta bench observed, it was important to trace the flow of information, specifically the WhatsApp messages and photographs, to determine if they can be considered public and thus lose their private nature. The sequence, the court held, shows that the WhatsApp messages between the petitioner's daughter and Abhishek Padia were not in the public domain prior to their disclosure to authorities. Padia's sharing of the information cannot be seen as a voluntary act since it likely occurred under pressure and may have been motivated by self-preservation.

Moreover, Padia's disclosure lacked the necessary consent from Rashika Jain, the other party in the chat. Therefore, sharing the WhatsApp messages without Jain's consent violated the expectation of privacy that existed between them. The court held that the concept of privacy is foundational to the constitutional guarantee of freedom, encompassing the right to be free from interference and intrusion.

Court in the judgment narrated several characteristics of private information. Firstly, individuals retain full agency over their private space and its boundaries in respect of private information including intimate details such as relationships, sexual preferences, and personal thoughts that one wishes to keep confidential. The creator of this information exercises agency in determining its dissemination, ensuring that sharing is intentional and limited. Furthermore, private information originates from individuals who intend it for restricted sharing, thereby establishing a perimeter around access. This concept also safeguards against external scrutiny, protecting one's identity and beliefs from unwanted observation.

Finally, it embodies the right to be forgotten, asserting that:[47]

(vi) The concept of personal space and information also carries with it the right to be forgotten. Any information shared with another or put in the public domain does not mean that the information of the source must remain in public memory for all times to come. In other words, concomitant to the right of private information, is the right to be erased from public memory.[48]

The right to privacy is exercisable against the world at large; a right in rem. Even if a person ventures into the public, he or she does not relinquish his/her claims to the private sphere This understanding strengthens the right to life and personal liberty under Article 21 of the Indian Constitution and supports the freedoms outlined in article 19, including the freedom to choose our associations and live according to our personal choices without interference.[49]

Hene the court in its final order directed that the police to immediately remove all photographs and WhatsApp messages between the late Rashika Jain and Abhishek Padia, treating them as private information. The authorities were instructed to ensure that these messages and photographs are not shared with

47 *Mahendra Kumar Jain* v. *State of West Bengal* 2022 SCC OnLine Cal 3060.

48 *Ibid.*

49 *Id*., para 13(xi).

anyone, either through RTI requests or by any other means with the following observation:[50]

28(g). The significance of section 8(1)(j) which upholds the right to privacy and ultimately the reputation and dignity of an individual under Article 21 of the Constitution goes against the tide of a free flow of information and remains steadfast in holding on to the private space of an individual. The significance of this provision must not be forgotten or diluted under any circumstances (Ref. *Subramanian Swamy* v. *Union of India, Ministry of Law*; (2016) 7 SCC221).[51]

VI CONCLUSION

In 2022, India made significant advancements in its cyber law framework, particularly with the introduction of the IT Directions 2022 by the Indian Computer Emergency Response Team ("CERT-In") under Section 70B(6) of the Information Technology Act, 2000. These directives are aimed to strengthen cybersecurity in response to a surge in data breaches and ransomware attacks worldwide and in India and mandates all service providers, intermediaries, data centres, body corporates and government organisations report all cyber incidents within 6 hours of becoming aware or being notified of the existence of such cyber incidents. Non-compliance with these new reporting requirements can lead to penalties, including up to one year in prison. This stricter approach builds on earlier regulations, like the 2021 Intermediary Guidelines, which established criminal liability for intermediaries that fail to meet compliance standards.

Effective from June 28, 2022, the IT Directions also mandate increased data retention and require synchronisation of system clocks with CERT-In-approved servers, especially impacting those in the virtual asset sector. In addition to the IT Directions, November 2022 saw the release of a revised Data Protection Bill by the Ministry of Electronics and Information Technology (MeitY). This new bill simplifies rules for cross-border data flow, removes distinctions between sensitive and critical data, and introduces stringent penalties for non-compliance. Looking ahead, the proposed Digital India Act aims to replace the Information Technology Act of 2000, aligning India's digital laws with global standards. This new legislation will address crucial issues such as technology regulation, intermediary liability, and electronic signatures, thereby supporting the government's Digital India Mission. It aims to not only encourage the adoption of the new age technologies but also to ensure that their deployment is in line with ethical-legal principles, data privacy principles and mechanisms for accountability.

The evolving landscape of cyber law in India also reflects the impact of previous judicial decisions. A notable example is the 2019 ruling in *UTV Software Communication Ltd.*, where the High Court of Delhi proactive stance established a 'dynamic' blocking injunction against websites hosting pirated films. This ruling allowed rights holders to update the list of blocked sites as new mirror websites

50 *Id.,* para 29.

51 *Id.*, para 28(g).

emerged, streamlining the process for enforcing copyright protections. In 2022, as online piracy remained rampant, especially among younger audiences, the importance of this decision became even more evident. The judgment and it's principles were heavily referred and relied upon in a number of judgments across country,

Furthermore, discussions around Internet Service Provider (ISP) liability and the admissibility of electronic evidence gained traction. Courts worked to clarify ISPs' responsibilities in preventing copyright infringement and established clearer guidelines for what constitutes admissible electronic evidence in legal proceedings.

Amid these developments, there was also an increased focus on emerging issues such as the right to be forgotten and provisions under sections 67 and 67A of the Information Technology Act. The right to be forgotten gained momentum as individuals sought to remove outdated or harmful information from online platforms. Courts began to navigate the delicate balance between this right and the public's interest in accessing information, leading to richer discussions around privacy and data protection. Overall, 2022 marked a pivotal year in shaping India's cyber law landscape, addressing both longstanding challenges and new developments in the digital age and highlighting the judiciary's ongoing efforts to address the challenges posed by the digital landscape.