14

CYBER LAW

Deepa Kharb[*]

I INTRODUCTION

THE PAST YEARS, 2024 have brought many important judgments in the field of cyber laws. Cyber law in India is exhibiting a phenomenal growth. What began in the year 2000 with the Information Technology Act as a framework to recognize electronic records and combat basic cyber-crimes has expanded into a constitutional, regulatory and technological ecosystem that impacts nearly every aspect of modern life. The judiciary has played a very decisive role in this process. While *Shreya Singhal* in 2015 defined the scope of restrictions on regulation of online speech, *Puttaswamy* laid the foundation for data protection jurisprudence in the absence of a statutory framework, elevating informational privacy to a fundamental right under Art.21. The regulatory framework has also expanded with the coming of Digital Personal Data Protection Act, 2023, criminal law reforms, sector specific cyber security regulations like SEBI's Cyber security and Cyber-Resilience Framework 2024, Telecom Cyber Security Rules,2024 *etc.,* and upcoming digital- governance deliberations and proposals. With new threats looming and rising cybercrimes, the focus has shifted towards a more structured and rights-conscious approach to digital regulation. State surveillance has also increased, particularly after COVID-19. In essence, Indian cyber law is steadily shifting from a narrow, IT-centric model to a broader digital governance architecture grounded in constitutional rights and technological realities.

This segment of the survey reviews important court decisions that impacted online privacy, free speech responsibility of social media platforms, and government surveillance. It also tracks trends in cybercrimes and how delays and lacunae in enforcement were addressed by the courts. Overall, this edition attempts to present a clear picture of how India is trying to keep up with the recent technological advancements while protecting people's statutory and constitutional rights and strengthening digital security.

II CYBER OBSCENITY

Sexual offences against children have recently received renewed attention following a decision of the High Court of Madras, which held that merely watching or downloading child sexual abuse material amounts to an inchoate offence.

* Associate Professor, Faculty of Law, University of Delhi.

The matter in *Just Rights for Children Alliance* v. *S. Harish*[1] arose from a complaint filed by an NGO collective and the consequential apprehension of S. Harish. He was found in possession of Child Sexual Exploitation Material (CSEM) along with other pornographic material on his mobile phone, downloaded and saved, and the same was confirmed by forensic analysis of the phone. He was charged under section 67B of the Information Technology Act, 2000(IT Act hereinafter) and section 14(1) initially and 15(1) of the Protection of Children from Sexual Offences Act, 2015 (POCSO hereinafter) later for committing a cognizable offence under section 67B (IT Act) and s.15(1) (POCSO). The High Court of Madras quashed the criminal proceedings against the accused on three grounds:

(i) mere watching and downloading would not amount to an offence under section 14(1) for which a child must have been used for pornographic purposes;

(ii) To constitute an offence under section 67B, IT Act, the accused must have published, transmitted or created material depicting children in a sexually explicit act or conduct. Mere watching and downloading would not constitute an offence under the said Act in the absence of any transmission or publication

(iii) For attracting section 15(1) POCSO, the storage of pornographic material involving a child shall be for a commercial purpose.

In the absence of any material to indicate any transmission or publication of pornographic content involving children, no offence could be said to have been committed under the POCSO or IT Act as per the High Court of Madras.The central questions for consideration before the Supreme Court were: whether mere viewing, possessing or storing of any child pornographic material is punishable under the POCSO, and what is the scope of Section 67B of the IT Act and Section 15(1) of POCSO?

Court's attention was drawn to decisions like *Akash Vijay* v *State of Kerala* (2024 Ker 42626) and *Shantheeshlal T.* v. *State of Kerala* (2024 Ker 35968) where the Kerala High Court bench held that mere storage or possession of any pornographic material involving a child will not constitute an offence under Section(s) 15 of the POCSO or 67B of the IT Act in the absence of any material to show that the accused person either intentionally downloaded or browsed the said material or that he shared or transmitted the same. High Court of Bombay, however, refused to quash the charges in *Lakshya* v. *State of Maharashtra*[2] and even when the accused was not the creator of the pornographic material, the act of storage and failure on his part to delete or report would fall under section15(1) and (2) of POCSO Act and section 67B of IT Act.

However, the Supreme Court, resolving previously divergent views across different high courts regarding the scope of possession under section 15(1), held

1 [2024] INSC 716, decided on Sep. 23, 2024.

2 2023(1) BomCR (Cri) 512.

that possession includes constructive or digital possession, broadening the liability beyond physical possession to cover digital storage and cached files. Mere possession, viewing or storing of Child Sexual Exploitation and Abuse Material (CSEAM) constitutes an offence under section 15 POCSO and section 67B of the IT Act, even without an intent to publish, transmit or distribute for commercial purposes. Broadening the interpretation of the term' possession' to cover 'constructive' and 'immediate control'. The Supreme Court also made a strong suggestion for the replacement of the term pornography with Child Sexual Exploitation and Abuse Material (CSEAM) to more correctly reflect the nature of the crime and the victimization of the child.

The Supreme Court further observed that the term 'child pornography' is misleading, as it may suggest consensual adult activity. To reflect the true nature of the offence, the Court recommended the use of the term "Child Sexual Exploitative and Abuse Material (CSEAM)". This term better captures the reality that such content records the sexual exploitation or abuse of children, including self-generated material involving minors. Supreme Court directed that the term 'child pornography' should no longer be used in judicial orders or judgments, and instead, the term CSEAM must be adopted. The Union Government was also advised to consider amending the POCSO Act to formally replace the outdated terminology.

The court also held that 'online intermediaries cannot claim safe harbour under section 79 of the IT Act unless they strictly comply with the POCSO Act. Mere compliance with IT Act guidelines or internal policies is insufficient. Intermediaries must exercise due diligence by promptly removing CSEAM content and 'reporting it to the appropriate authorities', as mandated under sections 19 and 20 of the POCSO Act read with Rule 11 of the POCSO Rules. Failure to comply disentitles intermediaries from immunity. The court highlighted the crucial role of social media intermediaries, expert bodies, and educational institutions in preventing the spread of CSEAM. It stressed the need for 'age-appropriate sex education', promotion of lawful content, and proactive steps by all stakeholders to ensure a safer digital environment for children.

In a matter related to an FIR filed against the makers and creators of web series 'College Romance in *Apoorva Arora* v. *State Govt. of NCT of Delhi*[3], the Supreme Court quashed the FIR, holding that vulgarity is not equivalent to obscenity and mere use of profanities, expletives, or vulgar language in creative work does not by itself constitute obscenity under s. 292, 294 and 509 IPC and Sections 67 and 67A Information Technology Act,2000.

The complaint was filed in respect of Season 1, episode 5 of the web series, which contained some vulgar, profane, obscene and sexually explicit language and title (Happily F****d Up) using strong expletives. The central issue was whether the use of expletives and profane language in the title and content of the episodes of the web series constitutes an offence of publication and transmission

3 [2024] INSC 223.

of obscene and sexually explicit content under section 67 and 67A of the IT Act. The two-judge bench observed that the high court posed the wrong question and hence arrived atthe wrong answer. The inquiry under section 292 IPC or Sections 67, 67A of the IT Act does not specify whether the language or words are decent. Rather, it is to determine whether the content is 'lascivious' or 'appeals to prurient interests' or 'tends to deprave and corrupt' the minds of those in whose hands it is likely to fall. Obscenity under law cannot be equated to vulgarity. Mere words cannot amount to obscenity. Obscenity involves material that tends to arouse sexual or lustful thoughts, which is different from profane or abusive language that may elicit disgust, revulsion or shock. Hence, the high court departed from the statutory requirement under section 67. The court referred to a judgment of the apexcourt in *Samaresh Bose* v. *Amal Mitra* case[4] where it was held that regard must be given to contemporary morals and national standards in judging whether content is obscene. The high court erred in adopting a literal interpretation; the expressions used in the web series are sexual in a literal sense, their contextual use does not arouse sexual or lustful feelings and lack any sexual connotation.

Further, the court opined that applying the courtroom decorum standard for judging the obscenity of content unduly curtails freedom of speech and expression and artistic creativity. The judgment highlights that law is shaped by normative parameters chosen by judges and, at times, marginalizes other ways of speaking, living and viewing. The threshold of actual obscenity is no doubt raised, making it harder for the law enforcement agencies to initiate or sustain prosecutions under section 67.

The IT Act was enacted to address the growing misuse of technology for unlawful purposes, including the transmission of obscene and sexually explicit content. With the rise of social media and encrypted communication platforms like WhatsApp, the application of sections 67, 67A, and 67B have gained significance. These provisions distinguish between obscene content, sexually explicit content, and child pornography. However, in practice, investigative agencies often invoke these provisions mechanically without precise classification of the content, thereby diluting the intent of the Act. The present case illustrates this recurring problem, while also raising questions on bail jurisprudence in cybercrime offences.

In *Jai Prakash Kanwar* v. *State of Chhattisgarh,* the applicant, Jai Prakash Kanwar, aged 25, was accused of uploading obscene photographs on WhatsApp using his mobile phone. Based on this allegation, Crime No. 101 of 2024 was registered at Katghora Police Station, District Korba, under Sections 67 and 67B of the IT Act. He was arrested on 14 February 2024 and remained in custody while the charge sheet was filed. He moved the High Court of Chhattisgarh under Section 439 of the Cr PC seeking bail.

The prosecution argued that the alleged act of uploading obscene images was a serious offence under the IT Act, while the applicant contended that he was falsely implicated, had no criminal antecedents, and that the trial would take

4 [(1985) 4 SCC 289, 1985 INSC 205].

considerable time to conclude. The court noted that the charge-sheet was already filed, the applicant had spent months in custody, and the trial was unlikely to finish soon. Accordingly, the court granted bail with conditions to ensure that the applicant would not misuse his liberty. The legal issue at stake was whether the allegations warranted continued pre-trial incarceration under Sections 67 and 67B of the IT Act. Section 67 penalizes publishing or transmitting obscene content in electronic form, while section 67B specifically criminalizes material involving children. The FIR and submissions did not make it clear whether the alleged photographs involved child pornography. This imprecision reflects a systemic issue -the police often invoke multiple provisions of the IT Act without carefully classifying the nature of content. The Supreme Court in *Sharat Babu Digumarti* v. *Government*[5] underscored the importance of precise digital evidence and the need to establish a clear nexus between the accused and the transmission of prohibited material.

In the present case, the high court refrained from entering into the merits of whether the content fell under section 67 or 67B, as this was a bail application. Nevertheless, the order indirectly highlights the challenges in enforcing cyber laws: the absence of forensic analysis, metadata, or server logs in most investigations undermines the robustness of prosecution under the IT Act. Without such evidence, mere assertions that "obscene photographs were uploaded" are insufficient to sustain a conviction. The court's reasoning is pragmatic, aligning with the principle that bail, not jail, is the norm, especially when the accused has no prior record, and the trial is delayed. Yet, the case exposes the limitations of cybercrime investigation in India, where evidentiary requirements under the IT Act are often overlooked. These risks transform the Act into a tool of arbitrary prosecution rather than a safeguard against genuine cyber abuse.

The decision thus serves a dual function: while granting bail in a cybercrime case, it underscores the urgent need for improved investigative capacity and evidentiary rigour under the IT Act. Only with such measures can the Act achieve its legislative objective of curbing digital obscenity and child exploitation without compromising individual rights. The Juvenile Justice (Care and Protection of Children) Act, 2015 ("JJ Act") embodies the principle that children in conflict with the law deserve reformative measures rather than punitive incarceration. Section 12 of the JJ Act mandates that "a person who is apparently a child and is alleged to have committed an offence … shall … be released on bail" except where the exception-conditions apply. This decision of the High Court of Chhattisgarh deals with the bail of a juvenile accused of sexual offences as well as the dissemination of digital/obscene material in electronic form.

The applicant in *A Child in Conflict with Law* v. *State of Chhattisgarh* was approximately 17 years 8 months old at the time of the alleged offence (thus a "child in conflict with law"). The prosecution alleged that he sexually exploited a minor (or young person) from March 2023 to April 2024 and further disseminated

5 (NCT of Delhi) [(2017) 2 SCC 18].

her obscene videos via mobile phones. The charge sheet included provisions under the Protection of Children from Sexual Offences Act, 2012 (POCSO) and the IPC (sections 376(2)(n), 506, 450). The FIR also invoked the Information Technology Act, 2000 ("IT Act") for transmission of obscene material electronically.

The Juvenile Justice Board refused bail, and the appellate court upheld that decision. The applicant then approached the high court by revision petition. The issue that required consideration here was whether the invocation of the IT Act provisions (in respect of dissemination of electronic obscene material) changes the approach towards bail for a child in conflict with law and how the relationship of juvenility, digital evidence and the public interest in offences involving sexual exploitation and electronic dissemination are to be balanced. The court emphasized that under section 12(1) JJ Act, the bail presumption applies to a child unless there are reasonable grounds to believe that (i) release would lead to association with known criminals; (ii) release would expose the child to moral/physical/psychological danger; or (iii) release would defeat the ends of justice. The court noted that the applicant had no prior criminal antecedents, had been detained for a significant period (about five months in an observation home), and the Social Investigation Report was favorable. Although the offence involved allegations of sexual exploitation and dissemination of material via electronic form, the court found that the facts did not show that releasing the juvenile would expose him to the risks listed in the proviso of section 12. Hence, bail was granted under conditions (parental custody/surety).

Kamala v. *The State*[6] case demonstrates both the utility and the interpretive challenges of the IT Act when invoked in cases of sexual exploitation. The prosecution alleged that the petitioner, A. Kamala, played an active role in the sexual exploitation of minors by aiding the primary accused in recording acts of abuse and transmitting the same through electronic platforms. The charges invoked provisions of IPC, POCSO, and crucially Sections 67 and 67A of the IT Act, criminalizing the publication and transmission of obscene or sexually explicit content in electronic form. The petitioner sought quashing of proceedings, contending that her alleged involvement did not amount to "publication" or "transmission" within the meaning of the IT Act, and highlighting contradictions in witness statements.

Before the high court, it was argued that the provisions of the IT Act could not apply to the petitioner since she had neither authored nor directly transmitted the content. The defense urged that her alleged role amounted at best to passive presence or peripheral knowledge, which, if criminalized, would stretch the scope of section 67 and 67A beyond legislative intent. The prosecution, however, countered that the IT Act provisions were meant to capture not only direct producers or distributors but also those complicit in the circulation and perpetuation of such material, particularly when minors are involved.

6 [2024] H.C.P.No.1163 of 2024.

The court refused to quash the charges, holding that the allegations, supported by material records and witness statements, prima facie disclosed offences under the IT Act. It was observed that the terms "publication" and "transmission" cannot be read narrowly, since even forwarding, sharing, or enabling access to such material constitutes transmission in cyberspace. The court emphasized that the IT Act was enacted precisely to deal with such forms of digital complicity, which aggravate the trauma of victims by multiplying the reach and permanence of exploitative content. The reasoning of the court merits scrutiny. By equating facilitation with active transmission, the court adopts a purposive interpretation that seeks to ensure no digital abettor escapes liability. However, this broad reading risks blurring the line between active participation and mere presence, unless carefully tethered to evidentiary standards. The court's insistence that the trial court must strictly verify device seizure, forensic analysis, and chain of custody before convicting reflects an awareness of this danger. Without such rigour, digital allegations could too easily be weaponised.

The present case highlights both the strengths and limitations of the IT Act. While sections 67 and 67A are essential tools against cyber-enabled sexual offences, their breadth demands cautious application. Unlike IPC offences, which deal with tangible acts, the IT Act criminalises conduct tied to technology's unique ability to amplify harm. This amplificatory effect justifies harsher liability but also requires courts to exercise vigilance in distinguishing culpable complicity from incidental contact. The Information Technology Act, 2000, which was enacted to address the challenges posed by the digital age, has steadily expanded into domains beyond e-commerce and cyber fraud, now covering offences that intersect with privacy, sexuality, and child protection. Section 67-A of the Act, which criminalises the publication and transmission of sexually explicit content in electronic form, is one of its most stringent provisions, particularly when read alongside the Protection of Children from Sexual Offences Act, 2012 (POCSO). The present case, *Jeet Kumar* v. *Union Territory of Jand K*,[7] illustrates the growing tendency of prosecuting authorities to invoke the IT, Act in tandem with sexual offence statutes. At the same time, it exposes the danger of over-criminalisation and misuse of successive FIRs to aggravate charges.

Jeet Kumar, a resident of Jammu and Kashmir, was first implicated in March 2024 under section 363 of the Indian Penal Code, 1860 after a minor girl failed to return from school. The police filed a challan in May 2024, restricting the charge to kidnapping. However, in November 2024, months after the first FIR, a second FIR was registered against him, alleging not only physical offences under Sections 341, 354, 354-D, 506 IPC and provisions of POCSO, but also offences under Section 67-A of the IT, Act. The new allegations suggested that the petitioner had sexually harassed the minor and transmitted sexually explicit content electronically. This second FIR, coming so soon after the trial in the first case commenced, raised serious doubts about its bona fides.

7 [2024] HC J&K 99690500.

Before the high court, the petitioner argued that the second FIR was false, frivolous, and designed to ruin his life. He stressed that it was filed after the challan in the earlier case, thereby amounting to an abuse of process. The high court, while refraining from quashing the FIR outright, recognized the need for judicial scrutiny. It stayed the operation of the second FIR, thereby preventing the continuation of proceedings pending further examination. The reasoning of the court must be situated in a broader jurisprudential framework. The Supreme Court in *T.T. Antony* v. *State of Kerala*[8] had held that multiple FIRs on the same incident were impermissible, as they result in harassment and double jeopardy. The present case falls within this matrix, while the second FIR was not identical in content; its proximity to the first and its expansive addition of serious cyber charges indicated an attempt to escalate the matter without fresh substantive evidence.

Particularly significant is the invocation of section 67-A of the IT, Act. This provision requires strict proof of electronic transmission of sexually explicit content. At the stage of registration, however, there was no indication of any seized device, forensic analysis, or digital trail linking the petitioner to the alleged conduct. The mechanical addition of such a grave cyber offence risks diluting the credibility of prosecutions under the I.T. Act, which already suffers from evidentiary challenges. Courts have repeatedly emphasised that cybercrime allegations cannot rest merely on oral statements; they demand robust technological corroboration. What emerges is the delicate balance between protecting children from sexual exploitation, both offline and online and safeguarding accused persons from inflated charges lodged with mala fide intent. By staying the second FIR, the high court acted as a check against prosecutorial overreach while keeping open the possibility of trial if credible digital evidence is later produced.

The case thus underscores the expanding reach of the IT, Act into matters of sexual morality and child protection, but also cautions against its overuse without technological rigour. Unless courts insist on a high evidentiary threshold for offences under section 67-A, there is a real risk that the statute will become a convenient tool of harassment rather than a meaningful safeguard in the digital age.

The prosecutrix in *State of Karnataka* v. *Kusumadhara*[9] alleged that the accused established physical relations with her under the pretext of marriage and without her consent, secretly recording intimate acts and later posting her nude photographs and videos on Facebook. He allegedly demanded 5,00,000, threatening further exposure. The trial court acquitted him of charges under sections 376, 417, 384, 506, and 511 IPC due to inconsistencies in testimony and lack of corroboration, but convicted him under section 292(2)(a) IPC (sale/obscenity) and Section 67A IT Act (publishing or transmitting sexually explicit material). He was sentenced to six months' imprisonment with a fine under the IPC and one year with a fine under the IT Act. The State filed appeals- one challenging the acquittals (Cr.A. No. 678/2018)

8 AIR 2001 SCC 2637.

9 [2024] KHC 15108-DB.

and the other seeking sentence enhancement (Cr.A. No. 677/2018). The High Court of Karnataka upheld acquittals under IPC, holding that the prosecutrix's testimony regarding rape and extortion lacked credibility as she admitted she would not have complained had the images not been posted. Delay in reporting and absence of evidence on the alleged extortion further weakened the case.

The high court, however, found adequate proof of transmission of obscene content *via* Facebook through the accused's mobile phone, corroborated by witnesses, nodal officer records, and forensic analysis. Importantly, the court clarified that a conviction under both section 292(2)(a) IPC and section 67A IT Act amounted to duplication since both provisions addressed the same mischief. Recognizing the IT Act as a special law designed to address cyber-specific obscenity, the Court set aside the sentence under IPC, maintaining the conviction solely under section 67A IT Act. By prioritizing the IT Act over IPC, *Kusumadhara* reinforces the principle *generalia specialibus non derogate* (the general law does not derogate from the specific).The Protection of Children from Sexual Offences Act, 2012 (POCSO Act) was designed as a special legislation to protect children from sexual abuse and exploitation, with stringent provisions that prioritise child safety over the rights of the accused. At the same time, the IT Act, 2000, has increasingly been invoked in cases of the circulation of sexual content on digital platforms. In *Pratheek H.J.* v. *State of Karnataka,*[10] before the High Court of Karnataka, raises a difficult question: how should courts balance the rehabilitative interests of a young adult accused with the seriousness of allegations under the POCSO and IT Acts, especially when the victims themselves were minors at the time of their statements?

The case arose from a complaint filed by a member of a local organization who claimed to have discovered video clips on social media depicting the petitioner engaged in sexual activity with college girls. It was alleged that the petitioner and his associates had not only recorded such acts but also blackmailed girls by threatening to circulate the videos. The petitioner, a 21-year- old BCA student, was arrested in June 2023, and a charge sheet was later filed for offences under sections 4 and 8 of the POCSO Act, Sections 386, 366, and 34IPC, and Sections 66(E) and 67(A) of the IT Act.

Before the high court, the defense argued that the victim girls were adults when their statements were recorded by the police, and the allegation of their being minors at the time of the alleged acts was only introduced to attract the POCSO provisions. The medical evidence did not confirm sexual assault, and the petitioner's continued incarceration would jeopardize his academic career. The prosecution, on the other hand, opposed bail, emphasizing the seriousness of the allegations and warning that release might enable the petitioner to tamper with witnesses or repeat the offence.

The court, while acknowledging the gravity of the allegations, placed significant weight on the factual context: the victims were majors when they

10 [2024] KHC 13652.

deposed, and the alleged incidents had surfaced only after the videos were circulated on social media in June 2023. The court stressed that whether the petitioner had indeed committed sexual assault when the victims were minors was a matter for trial. Importantly, the court recognized that prolonged pre-trial detention of a 21-year-old student could irreparably harm his prospects. Therefore, the court allowed bail subject to stringent conditions, including surety, appearance before trial, non-tampering with witnesses, and restrictions on travel.

The reasoning of the court is instructive. By granting bail, it reaffirmed that bail remains the rule and jail the exception, even in cases involving special legislation like POCSO and the IT Act, provided safeguards can be ensured. However, this pragmatic approach also raises concerns. The POCSO Act was enacted precisely to guard against the exploitation of minors, and the Court's emphasis on the victims' age at the time of deposition, rather than at the time of alleged assault, risks diluting the statutory intent. Moreover, allegations of recording and circulating intimate videos strike at the heart of digital safety, an area where courts are expected to take a strict view to deter further misuse. In conclusion, *Pratheek H.J.* v. *State of Karnataka* [11]illustrates the judiciary's struggle to balance the preventive aims of special legislation with the individual rights of young accused persons. While the decision ensures that the petitioner is not condemned to prolonged incarceration without trial, it also leaves open questions about how POCSO is to be applied when the victim's minority at the time of the offence remains disputed. The case reflects both the strengths and limitations of bail jurisprudence in the intersection of sexual offences and cybercrime.

The High Court of Gujarat in *Bhavinbhai Devshankarbhai Modha* v. *State of Gujarat*[12] confronted the delicate balance between the inherent powers of the high court under section 482 Cr PC and the gravity of heinous sexual offences, particularly those intertwined with digital exploitation under the IT Act, 2000. The petitioners sought quashing of an FIR on the ground of settlement, but the court emphatically rejected the plea, underscoring that such offences are not merely private disputes but crimes against society.

The facts reveal a deeply disturbing narrative. The complainant, wife of petitioner no.2, alleged that her husband, father-in-law, and mother-in-law coerced her into allowing the recording of nude images and videos, which were later disseminated on WhatsApp groups and pornographic websites. The father-in-law was further accused of sexual assault, including acts falling within Section 375 IPC. The FIR charged the accused under sections 354A, 354C, 376D, 498A, 506(2), 508, 509, 34 and 114 IPC and sections 66(e) and 67A of the IT Act. After charge-sheeting, the parties purportedly settled, prompting the accused to invoke Section 482 CrPC for quashing.

11 2024 KHC 13652.

12 [2024] SCC OnLineGuj.

The court, however, dismissed the petition. The court relied on *Gian Singh* v. *State of Punjab*[13] and *State of M.P.* v. *Laxmi Narayan*[14], reaffirming that while section 482 provides wide inherent powers, it cannot be exercised to quash proceedings in cases involving heinous crimes like rape, sexual assault, and offences under special statutes. Such offences, the court emphasised, transcend private disputes and directly implicate societal morality, the dignity of women, and public interest.

A significant aspect of the judgment is its treatment of offences under the IT Act. The accused were charged under sections 66(e) (violation of privacy by publishing images of private parts) and 67A (transmission of sexually explicit material). The court stressed that under section 77A IT Act, offences affecting women cannot be compounded. The use of technology to perpetuate sexual violence, the court observed, aggravates the offence by violating bodily autonomy and digitally immortalising the victim's humiliation. Thus, even if the complainant withdraws, the societal harm persists, and quashing cannot be permitted.

The court also clarified the scope of section 482 Cr PC. Citing *CBI* v. *Aryan Singh*[15] it held that the high court cannot conduct a "mini-trial" while deciding quashing petitions. The issue is not whether conviction is likely but whether the allegations disclose a cognizable offence. Given the graphic allegations and supporting digital evidence (CCTV, WhatsApp uploads), the court concluded that a full-fledged trial was necessary. Notably, the court's reasoning reflects an evolving judicial sensitivity towards marital and familial sexual abuse. Referring to *Hrishikesh Sahoo* v. *State of Karnataka*[16], it criticised the regressive marital rape exception, implicitly acknowledging that consent within marriage is not absolute. By recognising the father-in-law's acts under Section 375(b) IPC, the court underscored that familial status cannot shield perpetrators from accountability.

The judgment is significant for three reasons. First, it reaffirms that heinous sexual offences, especially those involving digital exploitation, cannot be trivialised as private disputes capable of settlement. Second, it demonstrates the judiciary's willingness to read the IT Act provisions harmoniously with the IPC to tackle emerging cyber-enabled sexual crimes. Third, it marks a progressive step in addressing intra-familial sexual abuse, challenging patriarchal silences within households.

However, the decision also highlights a recurring tension: while settlements are often invoked in matrimonial disputes, courts must vigilantly distinguish between civil-flavoured conflicts and crimes of mental depravity. The Gujarat High Court's refusal to quash despite the settlement signals a necessary deterrence against the misuse of compromise in cases of sexual violence. In conclusion, *Bhavinbhai Modha* is a robust affirmation of women's dignity and bodily autonomy

13 [(2012) 10 SCC 303].

14 [(2019) 5 SCC 688].

15 (2023 SCC OnLine SC 379).

under article 21. By refusing to condone settlement in offences involving rape, voyeurism, and cyber-pornography, the court not only upheld the rule of law but also reinforced the principle that such acts, though occurring within private homes, constitute crimes against the collective conscience of society.

IV INTERMEDIARY LIABILITY

In the case of *Arijit Singh* v. *Codible Ventures LLP,*[17] the plaintiff, a well-known playback singer, instituted proceedings before the High Court of Bombay seeking protection of his "personality and publicity rights" against unauthorised commercial exploitation by multiple defendants, including content creators, domain registrars, and online platforms. The grievance arose from the unauthorised use of the plaintiff's "name, voice, vocal style, mannerisms, photographs, likeness, signature and persona" in online videos, merchandise, and domain names without his consent.

Several defendants were engaged in hosting, disseminating, or facilitating access to infringing content and merchandise through online platforms and websites. Certain defendants had registered domain names incorporating the plaintiff's name, while others were hosting videos and content that exploited his personality traits. The plaintiff contended that such acts amounted to a violation of his personality and publicity rights and sought an ad-interim injunction restraining continued misuse.The court acknowledged that "digital platforms and intermediaries play a critical role in enabling the dissemination of content", and that technological advancements, if left unchecked, may be misused by unscrupulous individuals for commercial exploitation of celebrity identities. While the primary infringement arose from unauthorised commercial use, the court implicitly recognised the "responsibility of online platforms and intermediaries once they are made aware of infringing content". The directions issued to platform-related defendants to "remove, edit, or disable access to content" demonstrate the court's approach that intermediaries cannot remain passive facilitators when personality rights violations are brought to their notice.

The court held that freedom of speech and expression does not extend to "commercial exploitation of a celebrity's persona", and that platforms hosting such content cannot shield themselves behind neutral conduit arguments when the use is prima facie unlawful. By directing certain defendants to remove references to the plaintiff's name, image, voice, and likeness from hosted content, the court reinforced the principle that "intermediaries have a duty to act expeditiously upon notice. Significantly, the court granted an "ad-interim injunction capable of operating as a dynamic injunction", reflecting judicial recognition of the evolving and repetitive nature of online infringements. Such dynamic relief places a continuing obligation on platforms to ensure that once infringing content is identified, "re-uploads or mirror links are also addressed, thereby strengthening intermediary accountability.

16 2022 SCC 371.

17 [2024] SCC OnLine Bom2445.

The court further directed domain name registrars to "lock and suspend infringing domain names, incorporating the plaintiff's name and restraining their transfer to third parties. This underscores that entities providing technical infrastructure such as domain registration services are also subject to judicial directions to prevent ongoing personality rights violations. Overall, the decision advances the jurisprudence on platform liability by emphasising that intermediaries cannot enable or perpetuate unauthorised commercial exploitation once they are put on notice, particularly where violations of personality and publicity rights are evident.

The petitions in *Kunal Kamra* v. *Union of India,*[18] the Stand-up comedian Kunal Kamra, along with the Editors Guild of India, Association of Indian Magazines, and News Broadcasters and Digital Association, challenged the constitutional validity of the 2023 amendment to the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules ("IT Rules"). These amendments empowered the Central Government to notify a Fact-Checking Unit (FCU) to identify and flag "fake, false or misleading" content related to the business of government on social media platforms.

A Division Bench of the High Court of Bombay delivered the judgment, a split verdict. Justice G.S. Patel held that the challenged amendments (especially the FCU provisions) were unconstitutional because they were vague, lacked procedural safeguards, and had a chilling effect on freedom of speech and expression under Article 19(1)(a) of the Constitution. Justice Neela Gokhale disagreed and upheld the validity of the amendments, viewing the regulatory powers as permissible and within the scope of reasonable restrictions under the Constitution. Hence, the matter was referred to a third judge (Justice A.S. Chandurkar) under the High Court of Bombay Letters Patent to decide the points of difference.Justice Gokhale observed that the amendment introduces the Fact Checking Unit (FCU) only as a mechanism to identify the correctness of information relating to government business. The FCU has no power to direct intermediaries to take down content, and the discretion to act remains with the intermediary. If a user is aggrieved by any action taken by an intermediary, they may approach the grievance redressal mechanism provided under the Intermediary Rules or seek judicial remedies before a competent court. Therefore, the amendment does not amount to censorship or executive overreach.

The court further held that the amendment does not create a chilling effect on freedom of speech and expression. It targets only false and misleading information shared with bad intent and does not cover opinions, criticism, satire, parody, or commentary. The terms "fake," "false," and "misleading" were held to be clear and understandable in their ordinary meaning and not vague. Similarly, the expression "business of the government" was not considered vague, as the government is best placed to clarify facts relating to its own functioning. Relying

18 [2024] BHC-OS:14750-DB.

on Supreme Court judgments such as *Justice K.S. Puttaswamy* v. *Union of India*[19] and *PUCL* v. *Union of India*[20], the court held that the amendment satisfies the test of proportionality and falls within the scope of reasonable restrictions under Article 19(2) of the Constitution. Justice Gokhale emphasized that the spread of disinformation and misinformation weakens an informed citizenry and undermines democratic processes. Since the amendment neither penalizes users nor intermediaries without due process nor removes the role of courts as the final arbiters, it was held to be constitutionally valid and a legitimate measure to protect democratic discourse.

In *Aneesh K. Thankachan* v. *Union of India*[21], the High Court of Kerala examined whether YouTube, as an intermediary, could be compelled to remove a video alleged to be defamatory without a court order declaring it so. Can the government be compelled to block the content under Section 69A of the IT Act aand whether YouTube's refusal to remove the video (Ext. P5 email) was legally valid were considered by the court in this case.A YouTube video allegedly defaming the Marthoma community and its Bishop was uploaded on the platform. The petitioner, a member of the Marthoma community, claimed the video was scandalous, hurt religious sentiments, and could disturb public order. Complaints were filed with YouTube (under the 2021 Intermediary Rules) and with the government (under the 2009 Blocking Rules). YouTube responded that it cannot decide defamation claims and would act only if a court orders removal. The petitioner approached the high court seeking directions to remove the video, block the content, and compel authorities to act.

The petitioner argued that YouTube had failed in its responsibility to regulate harmful content under its own policies and that the video could disturb communal harmony and public order. He relied on section 69A of the IT Act, 2000, claiming that the government had the authority to block such content. YouTube, on the other hand, contended that it was merely an intermediary and could not judge the legality or defamatory nature of user-generated content. Relying on *Shreya Singhal* v. *Union of India*,[22] YouTube argued that it enjoyed safe harbour protection under section 79 and was not required to remove content unless there was a court order or a valid government direction. The court agreed with YouTube and held that intermediaries cannot be directed to remove content solely based on defamation allegations without a judicial finding. The court noted that section 69A is a narrowly framed provision applicable only in cases involving threats to sovereignty, national security, or public order, none of which were established in this case. T. R. Ravi J., emphasised that, in the absence of a court order declaring the video defamatory, YouTube could not be compelled to take it down.

19 AIR 2017 SC 4161.
20 AIR 2003 SC 2363.
21 2024/KER/90640.
22 AIR 2015 SC 1523.

The court further observed that expecting intermediaries to assess the legality of every takedown request would be impractical and unfair, given the vast volume of content hosted online. Such an obligation would effectively turn intermediaries into arbiters of speech, contrary to the law laid down in *Shreya Singhal*. Since the petitioner failed to demonstrate that the video fell within the grounds specified under section 69A, the petition was dismissed.In conclusion, the judgment reaffirmed the limited liability of intermediaries under Section 79 of the IT Act and reinforced the *Shreya Singhal* principle that content removal can only be mandated through proper legal channels. The ruling strikes a balance between protecting free speech and regulating harmful content by ensuring that intermediaries are not forced to act without clear judicial or governmental authority.

The IT Act, 2000 was enacted with the object of regulating online activities, ensuring safe use of digital spaces, and balancing freedom of expression with the need to curb misuse of technology. Its intermediary liability provisions, particularly section 79, were framed to prevent the unchecked spread of obscene or inflammatory online content. However, the implementation of these provisions has been marked by judicial hesitation, leaving unresolved tensions between safeguarding free speech and curbing harmful digital conduct. The present case exemplifies this tension, where the court adopted a pragmatic yet restrained approach in dealing with objectionable videos uploaded on YouTube.

The petitioner in *Akshya Kumar Sarangi* v. *State of West Bengal*[23] was aggrieved by a series of objectionable videos uploaded by one Prasanta Roy across multiple URLs. Despite initial State intervention to block certain links, new videos continued to surface. The petitioner sought judicial intervention to ensure comprehensive removal and accountability of both the State authorities and the intermediary, Google/YouTube.Pursuant to earlier court directions, the State initiated a criminal case- Haridevpur Police Station Case No. 311 of 2023 under Sections 153A, 295A, 504, and 505 of the IPC, which address promotion of enmity, deliberate insults to religion, provocation, and circulation of false information. The matter was later transferred to the cyber police station. Simultaneously, a notice under Section 79(3)(b) of the IT Act was issued to Google/YouTube for the removal of the unlawful material. The State contended that the identified URLs were blocked and that further monitoring was underway.

On its part, Google LLC submitted that it had complied with the notice and taken all possible measures to block objectionable content on its platform. However, it pointed out the technological challenge that content once removed could reappear under different URLs,often uploaded by different users.The court noted compliance by both the State and the intermediary. It was observed that the petitioner remained free to notify authorities of freshobjectionable content,who would then be bound to act upon such complaints. Importantly, the court emphasised that the criminal proceedings already initiated must reach their logical conclusion, directing that an

23 [2024] Cal HC; MANU/WB/0996/2021.

investigation be conducted expeditiously. The writ petition was accordingly disposed of.

The reasoning of the court is both cautious and revealing. By accepting the compliance of the intermediary, the court reaffirmed the "notice and takedown" regime embedded in section 79 IT Act, whereby intermediaries enjoy safe harbour until they fail to act upon official notice of unlawful content. This preserves the balance between the right to freedom of expression and the need to prevent the circulation of harmful or inflammatory material. At the same time, by refraining from imposing broader obligations on intermediaries, the court highlighted the limitations of judicial power in addressing systemic digital harms.The judgment, however, leaves critical questions unanswered. The recurring reappearance of harmful content exposes the inadequacy of a purely reactive framework. The absence of preventive obligations on intermediaries' risks normalises the endless cycle of "*block andre- upload*." Furthermore, by limiting its role to ensuring compliance with existing statutes, the court avoided grappling with the deeper challenge of how digital platforms can be made more accountable in real time.

Ultimately, *Akshya Kumar Sarangi* illustrates the judiciary's incremental approach: pragmatic in securing immediate relief, but restrained in shaping broader cyber law jurisprudence. The decision reflects the uneasy compromise between protecting individuals from digital harms and preserving the autonomy of online platforms under the IT Act.

V EXTENT OF OVER-RIDING EFFECT OF THE INFORMATION TECHNOLOGY ACT, 2000, OVER THE INDIAN PENAL CODE, 1860

Two different benches of the High Court of Bombay gave divergent opinions on whether the offences committed using computers/ computer system/ computer resources should be dealt under the I.T Act or also under the Indian Penal Code, 1860 .In *Gagan Harsh Sharma* v. *State of Maharashtra* (2019), the court held that when a dishonest or fraudulent act is committed using a computer, it falls under s. 66 of the IT Act. By virtue of section 81 of the IT Act has an overriding effect; theprovisions of IPC, the Court held, should not apply in such cases.However, the Aurangabad Bench of High Court of Bombay disagreed in *Awadesh Kumar Parasnath Pathak* v. *State of Maharashtra* (2019), holding that offences under the IT Act and the IPC are different in nature, and both laws can apply at the same time. Due to this contradiction, the matter was referred to a three-judge bench.

The appellant's counsel contended that where an offence is specifically covered under the provisions of the IT Act, the provisions of the Indian Penal Code cannot be simultaneously invoked, placing reliance on the apex court ruling in *Sharat Babu Digumarti* v. *Government of NCT of Delhi*, wherein it was held that a special statute would prevail over the general law. Section 43 of the IT Act comprehensively deals with unauthorised access to computer systems, and where such unauthorised access is accompanied by dishonest or fraudulent intention, the offence squarely falls within the ambit of section 66 of the IT Act. According to the applicant's counsel, sections 66 and 72 of the IT Act effectively subsume the

essential ingredients of offences such as cheating, theft, and criminal breach of trust as defined under the IPC. Consequently, prosecuting an accused under both the IT Act and the IPC for the same set of facts would amount to double jeopardy, as it would result in punishing the individual twice for the same offence.The State,however, argued that the two laws create distinct offences. section 43 of the IT Act does not include cheating by inducement, a key element of offences like cheating under the IPC.Section 72 of the IT Act does not cover cases of misuses property for personal gain, butis covered under IPC offences.

The arguments from the State side regarding section 43,66 and 72 IT Act found favour with three judges bench. Since offences such as cheating, criminal breach of trust, inducement, deceit, common intention, and misappropriation for personal use are not fully covered under sections 43, 66, or 72 of the IT Act, prosecution under the IPC remains permissible, the court held. This narrows the scope of section 81 of the IT Act and prevents its blanket application to exclude the IPC.A general law (IPC) can be excluded only if the exact ingredients of the offence are fully covered by the special law (IT Act). Where the elements of a crime under the IPC are not fully covered by the IT Act, both the laws will be applicable, and would not amount to double jeopardy as the ingredients of both offences are different. Hence, the IT Act does not automatically override IPC as per the bench. The judgment reinforces the principle that special law prevails over general law only when there is complete overlap in the elements of the offences.

VI ELECTRONIC EVIDENCE

In *Ram Kishan* v. *Emaar MGF Constructions Pvt. Ltd.,*[24] the petitioner, proprietor of ShivAluminum and Glass, executed work for the respondent at the Commonwealth Games Village from 2010 onwards. Although part payments were made, a sum of 12,00,580 remained unpaid after August 2011.After issuing a legal notice in April 2014 and receiving no response, the petitioner filed a recovery suit relying on a computerized Statement of Account but failed to initially file the required section 65B Evidence Act certificate.

An application to place the certificate on record was rejected by the trial court. The petitioner then approached the high court under article 227, which held that non-filing of a Section 65B certificate is a curable procedural defect and allowed it to be filed, subject to costs.

Relying on several Supreme Court judgments, including *Arjun Panditrao Khotkar, Ram Rati* v. *Mange Ram*,[25] and *State of Karnataka* v. *M.R. Hiremath*,[26] the court held that filing a suit. 65B certificate is a procedural requirement, not a substantive one.Failure to file it at the initial stage is a curable defect, and the certificate can be allowed to be filed at a later stage as long as the trial is still ongoing.Rejecting such a request amounts to taking an overly technical and rigid view, which goes against settled legal principles.

24 [2024]DHC:4793.

25 AIR 2016 SCC1343.

26 AIR 2019 SCC 2377.

The court emphasised that if a document is important for deciding the dispute fairly, it should be allowed on record, provided the other party gets an opportunity to challenge it.As a result, the high court set aside the trial court's order dated July 26, 2018, and allowed the petitioner to place the section 65B certificate on record in support of the Statement of Account, subject to payment of 15,000 as costs. The court prioritised justice over technicalities and allowed the missing certificate to be filed so the dispute could be decided fairly on its merits.The court made it clear that cases should be decided based on their real merits and not dismissed because of technical mistakes. It was observed that procedural requirements should not block justice.

VII IDENTITY THEFT, CHEATING BY PERSONATION, CYER TERRORISM, OFFENCE OR CONTRAVENTION COMMITTED OUTSIDE INDIA

The Prevention of Money Laundering Act, 2002 (PMLA) operates in tandem with scheduled offences under other laws, making it a unique legislation where liability under one statute flows from criminality defined in another. The present case, *Adnan Nisar* v. *Directorate of Enforcement,*[27]is a striking example where offences under the IT Act formed the very foundation of PMLA proceedings. Justice Swarana Kanta Sharma of the High Court of Delhi examined how cyber fraud with cross-border dimensions could be treated as a predicate offence under the PMLA framework.

The facts trace back to a US investigation where a Kansas resident's cryptocurrency was siphoned off using malware and routed to Indian accounts through WazirX. Blockchain analysis linked one Vishal Moral and his associates, including Shivang Malkoti and the petitioner, Adnan Nisar. The Enforcement Directorate (ED) alleged that Nisar knowingly facilitated the conversion of the fraudulently obtained cryptocurrency into cash, thereby committing the offence of "money laundering." The scheduled offence was traced to sections 66C, 66D and 66F of the IT Act, relating to identity theft, cheating by personation through computer resources, and cyber terrorism, respectively.

The petitioner argued before the court that since the alleged hacking and misappropriation took place outside India, Indian law could not apply. Moreover, without a registered predicate offence in India, proceedings under PMLA would not survive. He contended that the MLA (Mutual Legal Assistance) request from the U.S. only sought freezing of assets and did not authorise ED to arrest or prosecute. Reliance was placed on *Vijay Madanlal Choudhary* v. *Union of India*[28] (2022), stressing that prosecution under PMLA cannot be notional and must be anchored in a valid domestic scheduled offence.The ED, however, invoked section 75 of the IT Act, which provides for extraterritorial jurisdiction application to offences committed outside India if the computer system or network is located within India. Since the laundered cryptocurrency entered Indian wallets and platforms, the ED argued that the predicate IT Act offences were very much triable

27 [2024]DHC:6779.

28 (2023) 12 SCC 1.

in India. By extension, this satisfied the "proceeds of crime" requirement under Section 2(u) PMLA. The court also noted that the IT Act provisions are explicitly included in the Schedule to the PMLA, thereby validating the ED's prosecution.The court,upholding this reasoning, held that cyber offences under the IT Act, even if initiated abroad, could constitute scheduled offences once their effects were felt inIndia through Indian exchanges and accounts. By applying Sections 66C and 66D of the ITAct as predicate offences, the court found sufficient material linking the petitioner to the laundering process. On the question of bail, the court reiterated that under section 45 PMLA,the accused must demonstrate that he is "not guilty" and "not likely to commit an offence while on bail"- a threshold the petitioner failed to cross. Consequently, bail was denied.

Nevertheless, the court's ruling highlightsIndia's robust response to cyber-enabled money laundering, affirming that IT Act offences are not merely stand-alone cybercrimes but also gateways to the wider anti-money laundering regime.The Information Technology Act, 2000 (IT Act), enacted to address offences in the digital domain, criminalises identity theft and the dishonest use of electronic credentials through provisions like section 66C. Yet, its judicial application often exposes evidentiary lacunae in cybercrime prosecutions. In *Sanjay Kumar Gupta* v. *State of Chhattisgarh*, the high court confronted a complaint alleging attempted misuse of Aadhaar and OTP to reset an IncomeTax e-filing password. The court's dismissal of the writ petition underscores the evidentiary rigor demanded for invoking Section 66C while revealing institutional challenges in responding to emerging cyber-frauds.

The petitioner, a partner in Mahi Polymers, alleged that his chartered accountant and another associate attempted to procure his Aadhaar-linked OTP for gaining access to thefirm's e-filing account. He refused to share the OTP, but argued that the very act of soliciting it amounted to identity theft under section 66C of the IT Act. Complaints were lodged before the police and on the cybercrime portal, but closure reports followed. The Judicial MagistrateFirst Class (JMFC) dismissed his complaint, and the Sessions Judge upheld that order in revision. Aggrieved, he approached the high court by way of writ petitions seeking directions to register offences under the IPC and the IT Act.

The core issue was whether solicitation of an OTP without evidence of its actual use or consequent alteration of digital records satisfies the ingredients of section 66C, which penalizes

fraudulent or dishonest use of another's unique electronic identification. The court noted that the petitioner himself admitted he never shared the OTP and that no access to or manipulation of the e-filing account occurred. In the absence of any *actusreus* beyond solicitation, the charge of identity theft could not be sustained. On this reasoning, the court endorsed the magistrate's and sessions judge's concurrent findings. The alleged conduct, though suspicious, lacked sufficient material to constitute offences of cheating, forgery, or identity theft. The court declined to interfere under its writ jurisdiction, emphasising that the

petitioner had failed to demonstrate either illegality in the investigation or perversity in the lower courts' orders.

The ruling reflects a strict evidentiary approach to the IT Act's penal provisions. While section 66C aims to safeguard citizens against digital impersonation and fraud; its invocation demands verifiable proof of dishonest use, such as server logs showing unauthorized access, records of OTP validation, or altered filings. A mere attempt to obtain credentials, unless substantiated by digital footprints of misuse, does not suffice. This insistence preserves the balance between criminalising cyber-misconduct and preventing overreach on the basis of uncorroborated suspicion. However, the case also indicates bare systemic shortcomings. The closure of the complaint without a detailed forensic investigation, such as requisitioning audit logs from the Income Tax portal or call-data records,highlights the inadequacies of current policing of cyber offences. Victims often perceive solicitation of OTPs as a precursor to identity theft, but unless investigative agencies preserve and present technical evidence, prosecutions falter. While thestatutory thresholds of proof can't be diluted by the courts, the necessity of upgrading cyber-forensic capacities of law enforcement is signalled here.In a sextortion case in *Kisan Kumar @ Krishna Kumar* v. *State of Chhattisgarh*,[29] the high court at the stage of bail hearing adopted a cautious approach and refused bail, citing the seriousness of the offence, the organised nature of the cybercrime, and the need to continue investigating digital evidence leaving the final determination of intent to be decided based on digital forensic evidence at trial.

The complainant in the present case was blackmailed after receiving an obscene WhatsApp video call and, out of fear, transferred over 31 lakh rupees to multiple bank accounts. Investigation revealed that these accounts were operated by the accused, including the applicants. The case was registered under Section 420 IPC and section 66(c) of the IT Act.The applicants claimed false implication,claiming that they allowed their bank accounts to be used without knowledge of the fraud. The prosecution, however, opposing bail, contended that the applicants were key facilitators in an organised cyber-extortion racket,with the main accused still absconding.

The high court refused bail, citing the seriousness of the offence, the organised nature of the cybercrime, and the need to continue investigating digital evidence. The case highlights that while s. 66(c) requires proof of dishonest intent, courts may adopt a cautious approach at the bail stage in large-scale cyber fraud cases, leaving the final determination of intent to be decided on the basis of digital forensic evidence at trial.

VIII RIGHT TO BE FORGOTTEN

Right to Be Forgotten (RTBF) is explicitly recognised under article 17 of the GDPR. Individuals can seek erasure of personal data when data is no longer

29 (2021)06 CHH CKK 0051.

necessary, when the consent is withdrawn or when the data processing lacks a legal basis.The RTBF in India represents a constitutional response to the permanence of digital memory. Rooted in *K.S. Puttaswamy*,it reflects the idea that privacy, dignity, and autonomy must protect individuals not only from state intrusion but also from perpetual reputational harm. Indian law, however, does not clearly recognise RTBF. The IT Act, 2000, mainly deals with public order and decency, not personal reputation. The Digital Personal Data Protection Act, 2023 (DPDPA) takes a small step by allowing people to ask for the deletion of personal data once it is no longer needed, but this applies only to private entities, not court records or judicial websites. As a result, harmful or outdated information especially about criminal cases often remains online even after a person is acquitted. Because of this legal gap, courts have become the main decision-makers on RTBF, resulting in fragmented and uncertain outcomes.

The controversy arising from *Karthick Theodore* v. *Registrar General*[30] presented a constitutional challenge before the Supreme Court- to decide whether, and to what extent, RTBF can be enforced against judicial archives in a constitutional system founded on transparency and open justice. The petitioner, Karthick Theodore, had been convicted of rape and cheating under ss. 376 and 417 IPC, and was sentenced to imprisonment by the trial court *vide*in 2011, but was subsequently acquitted of all criminal charges by the High Court of Madras in a criminal appeal. Despite the acquittal, his name and case details continued to remain publicly accessible through online court databases and legal research platforms. He claimed that perpetual online availability caused serious reputational harm, violating his dignity and right to privacy under article 21.

The High Court of Madras granted limited anonymisation, holding that continued identification of an acquitted individual served no legitimate public interest and caused disproportionate harm. The court attempted to balance open justice with digital-era privacy concerns.The order was stayed after a challenge by an online legal database, raising concerns that anonymisation undermines transparency, precedentvalue, and public access to justice.The issue for consideration for the court was whether RTBF apply to judicial records without eroding the principle of open justice.After the High Court of Madras Division Bench judgment in *Karthick Theodore* (2024), Ikanoon Software Development Pvt. Ltd. challenged the decision before the Supreme Court through a Special Leave Petition. Finally, on 24 July 2024, the matter was referred to the Supreme Court, wherein the Bench led by the Chief Justice stayed the High Court of Madras judgment and linked the case with *Alka Malhotra* v. *Union of India*, which raises similar issues about the Right to Be Forgotten (RTBF) and the continued online availability of court judgments.

The Supreme Court now has to decide whether, and how far, the Right to Be Forgotten can apply to judicial records.In *Rakesh Jagdish Kalra* v. *India Today*

30 W.P.(MD) No.12015 of 2021.

Group[31], the High Court of Delhi examined the continuing harm caused by online media reports that linked the plaintiff to criminal allegations even after his acquittal. Although the criminal proceedings had conclusively ended in his favour, several media houses continued to host articles referring to the accusations, which remained readily accessible on the internet and perpetuated an impression of guilt.

The court noted that an acquittal restores not only the legal presumption of innocence but also the individual's right to live with dignity. Continued publication of content connecting an acquitted person to past allegations was held to amount to a continuing invasion of privacy and reputation, particularly when such content does not adequately reflect the outcome of the case or its finality.

Addressing the balance between freedom of speech under article 19(1)(a) and the right to privacy and dignity under article 21, the court reiterated that freedom of expression is not absolute. While the media plays a vital role in reporting criminal proceedings, this role does not extend to indefinitely preserving and circulating accusations once they have lost relevance and no longer serve any legitimate public interest.The High Court of Delhi drew a clear distinction between public interest and public curiosity, holding that post-acquittal dissemination of prejudicial material caters only to the latter. Where the individual has been legally exonerated, continued online association with criminal allegations serves no meaningful societal purpose and results in disproportionate harm to personal reputation.

Accordingly, the court directed the immediate removal of the impugned content, emphasising that the right to privacy of an acquitted person must prevail over freedom of expression when the expression in question has no ongoing public value. The judgment is an important contribution to India's evolving jurisprudence on the Right to Be Forgotten, reinforcing the principle that digital permanence cannot be allowed to impose a lifelong penalty on those who have been cleared by the law.

IX CONCLUSION

The year 2024 marked a decisive phase in the evolution of Indian cyber law, reflecting the law's ongoing struggle to keep pace with rapid technological change.Courts dealt with important issues like online privacy, free speech, platform responsibility, and the lasting impact of digital records, especially through debates around the Right to Be Forgotten. At the same time, new rules and policies reflected the State's growing role in regulating the online space, raising questions about fairness and accountability.

31 SCC OnLine Del 5113.