12

CYBER LAW

*Deepa Kharb**

I INTRODUCTION

YEAR 2023 witnessed some landmark developments in the cyber lawmaking sector with the enactment of the Digital Personal Data Protection Act and the three criminal laws replacing the outdated penal laws. This survey delves into the evolving realm of cyber law, analysing landmark judicial rulings by the Supreme Court and various High Courts in 2023. It covers critical issues such as intermediary liability, government regulation of cyberspace, the admissibility of electronic evidence, and the regulation of obscenity in cyberspace. The aim is to provide a comprehensive overview of how Indian courts are addressing the complex legal challenges presented by the digital age.

By examining these key decisions, the survey offers valuable insights into the principles that are shaping the future of cyber law in India. It serves as both a practical reference and a critical analysis of the judicial reasoning behind these rulings. Furthermore, the survey identifies areas that could prompt further legal discourse, reflecting the dynamic and ever-changing nature of cyber law. Through this exploration, the survey highlights the judiciary's ongoing efforts to adapt the legal framework to meet the demands of a rapidly digitalising society.

II PRIVACY AND RIGHT TO BE FORGOTTEN

"I give the fight up: let there be an end,
A privacy, an obscure nook for me.
I want to be forgotten even by God."

- Robert Browning[1]

The Supreme Court, in its landmark judgment in *K.S. Puttaswamy* v. *Union of India*[2] recognized privacy as a fundamental right, which includes both decisional autonomy and informational control. It was emphasized that individuals must retain control over their personal data, including their presence on the internet. This right is closely tied to an individual's dignity and includes the right to control who accesses their personal information and for what purposes.

* Associate Professor(SS), Faculty of Law, University of Delhi.

1 19th Century English Poet and Playwright Robert Browning in his book Paracelus.

2 2019 (1) SCC 1.

In *Karmanya Singh Sareen* v. *Union of India* (SLP(C) 804 of 2017), the Supreme Court Constitution Bench considered the privacy implications of WhatsApp's 2021 policy. In its judgment dated September 23, 2016, the High Court of Delhi granted partial relief in a case challenging WhatsApp's privacy policy. Recognizing that the Supreme Court was still deliberating on the right to privacy in *K. Puttaswamy,*[3] the court ordered that user data be protected only until September 25, 2016.

The petitioners challenged this decision, arguing that it created an artificial distinction between users who deleted the app before September 25 and those who continued using it afterward, thereby compromising the data and rights of millions.The petitioners raised concerns about WhatsApp's new privacy policy (2016), arguing that it was implemented unilaterally, with users pressured to consent by simply clicking an "Accept" button on the opening screen, which discouraged thorough review of the policy. They contended that this process was deceptive, particularly for users who cannot read or understand the policy. The petitioners demanded the inclusion of an "Opt Out" or "Don't Share" option to give users control over their data, emphasizing that consent should only be obtained from users who clearly understand the policy.

The petitioners further argued that the policy wrongfully grants WhatsApp a license to all content shared by users, including minors, who are incapable of legally granting such a license. Additionally, the petitioners claimed that WhatsApp's policy violated section 72 of the Information Technology Act, which mandates penalties for breaches of confidentiality, and the 2011 Rules, which require full and transparent disclosure of privacy policy consequences. As a result, they argued that WhatsApp's actions violated the right to privacy under Article 21 of the Indian Constitution, as users' private data was shared without adequate consent or disclosure. The key issues for the consideration of the court in this 2017 SLP were:

i. Whether WhatsApp's Privacy policy of August 2016 violates the Right to Privacy of its users?

ii. Whether a privacy policy should have specific 'opt-out' provisions without the user having to 'opt-out' of the application in totality? In this case, whether WhatsApp is obligated to provide a specific option of 'Not to share data' with Facebook?

iii. Whether the manner of seeking 'consent' from users who are unable to read and understand the new privacy policy amounts to deception?

In May 2021 WhatsApp introduced a revised privacy policy allegedly violating Article 21 of the Constitution by collecting sensitive user data, including financial information. Users faced a choice till February 28, 2021(extended till May 15, 2021): accept the policy or stop using WhatsApp. Soon after the policy was announced, a writ petition challenged it before the High Court of Delhi. It claimed

3 *Supra* note 2.

that the new privacy policy violated the fundamental right to privacy and allowed WhatsApp to profile users' data without any government regulation.

On February 15, 2021 an application was filed challenging the new privacy policy. The application claimed that WhatsApp was offering lower privacy protections for Indian users as compared to European users. The three-judge bench led by CJI Bodbe issued notice and asked all the parties to file their replies.

The petitioner contended that Indian users were treated unfairly compared to European users, who could refuse data sharing.The petitioners requested interim relief, including a stay on WhatsApp's new privacy policy and equal privacy standards for Indian users, mirroring those in Europe.The court, through its order dated February 1, 2023, declined interim relief but directed WhatsApp to widely publicize that Indian users were not required to accept the new policy to continue using the app. This interim order ensured that WhatsApp's functionality would remain unaffected until the Data Protection Bill was enacted as submitted by the Government of India.

The Bench noted that WhatsApp had assured the government that users who had not accepted the new policy would face no disruptions. The court directed WhatsApp to publicize this assurance through full-page advertisements in five national newspapers.The court recorded WhatsApp's undertaking and reserved further consideration of the petitions for subsequent hearings.

In *WhatsApp LLC* v. *Union of India,*[4] WhatsApp filed a writ petition in the High Court of Tripura challenging the constitutionality of the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (Intermediary Guidelines). It also challenged an order under Rule 4(2) of the Intermediary Guidelines from a Judicial Magistrate First Class requiring WhatsApp to disclose the originator of a fake resignation letter of the Chief Minister of Tripura.

The Intermediary Guidelines 2021 require intermediaries to comply with judicial orders in specific cases involving national security, public order, or sovereignty. The petitioner argued that Rule 4(2) of the IT Rules allows such disclosure only for serious offenses involving public order, sovereignty, or security, with the court required to assess tangible threats before issuing such an order. The petitioner contended that neither the investigating officer's application nor the judicial order demonstrated such grounds. They sought interim protection, arguing that the directive lacked proper justification.

The State opposed the plea, asserting that WhatsApp being an intermediary under the IT Act and 2021 Rules lack the standing to object to the disclosure of the first originator of the message as per the directions of the trial court. The court, after reviewing the submissions and relevant rules, found that the trial court failed to assess the threat to public order adequately. Citing *K.S. Puttaswamy* v. *Union of India*[5] on the right to privacy, the court granted interim relief, staying the

4 W.P. (Crl.) No. 02 of 2023.

5 *Supra* note 2.

impugned order while allowing the investigation to continue.This matter highlights the ongoing tension between privacy rights and regulatory oversight.The case has now been transferred to the High Court of Delhi along with other cases relating to the IT Act 2021.

The High Court of Karnataka in *The Deputy Director General* v. *P. Lavanya,*[6] has issued a significant ruling on privacy in matrimonial disputes, overturning a single judge's order that instructed the Unique Identification Authority of India (UIDAI) to disclose a husband's Aadhaar details to his wife. The wife, involved in a matrimonial dispute and unable to enforce a maintenance order due to her husband's unknown whereabouts, had sought his Aadhaar information under the Right to Information (RTI) Act.

The petitioner (wife) had filed the RTI application to obtain her husband's address for enforcing a family court order in *Crl. Misc. No. 312/2012*, which directed her husband to pay monthly maintenance.The said application was rejected by UIDAI, citing section 33 of the Aadhaar Act, which prohibits disclosure of Aadhaar details without approval from a high court judge. The rejection was upheld on appeal, prompting the petitioner to file a writ petition. The Single Judge set aside UIDAI's rejection, remitted the matter to UIDAI, and directed it to issue notice to the husband, hear him, and reconsider the application.

The respondents (UIDAI officials) argued that the Single Judge's order contravenes section 33 of the Aadhaar Act, amended following the Supreme Court's judgment in *K.S. Puttaswamy* v. *Union of India*.[7] They contended that disclosure of Aadhaar information requires strict compliance with procedural safeguards, including a hearing before a high court judge.

Conversely, the petitioner's counsel contended that Aadhaar restrictions do not apply in marital relationships, as the identities of spouses are intertwined. They argue that the single judge's order adheres to statutory mandates by requiring the husband's hearing and does not prejudice him. Moreover, the petitioner's inability to locate her absconding husband impedes enforcement of the maintenance order, necessitating access to his Aadhaar details.The appeal thus questioned whether Aadhaar information can be disclosed under RTI for enforcing legal rights while balancing procedural safeguards under the Aadhaar Act.

The appeal addresses the constitutional validity of section 33 of the Aadhaar Act, as interpreted in *K.S. Puttaswamy* v. *Union of India*[8] *(supra)*, and challenged a single judge's order that directed UIDAI to reconsider an RTI request from a wife seeking her husband's Aadhaar details to enforce a maintenance order.

The Supreme Court in *Puttaswamy*[9] had clarified that section 33(1) is an exception to the confidentiality provisions under section 28 and 29 of the Aadhaar Act. It permits disclosure of Aadhaar information only through a judicial order,

6 2023:KHC-D:13177-DB; MANU/KA/3883/2023 (decided on Nov.10,2023).

7 *Supra* note 2.

8 *Ibid.*

9 *Ibid.*

provided the Aadhaar holder is granted an opportunity to be heard. The court underscored privacy rights, emphasizing that the procedural safeguards in section 33 protect the autonomy of individuals, even in a spousal relationship.

The appellants argued that privacy rights under section 33 are non-delegable and require strict compliance. The single judge erred in remitting the case to UIDAI, as only a high court judge has the authority to decide on disclosure. The principle that an act prescribed by law must be done in the prescribed manner or not at all was invoked to assert that UIDAI cannot independently decide such cases. The court acknowledged that privacy rights are fundamental and that marriage does not override these protections. Therefore, the matter was remitted to the single judge with instructions to include the husband as a respondent and ensure procedural compliance under section 33. The Single Judge was asked to reconsider the case, respecting the Aadhaar Act's statutory framework and privacy safeguards.

The appeal was disposed of with directions to facilitate proper judicial procedure, ensuring that any disclosure of Aadhaar information adheres to the statutory requirement of high court oversight. This ruling reinforces the primacy of privacy rights even in family law disputes, establishing a key precedent for how personal information should be handled in such cases.

India's first Digital Personal Data Protection Act, 2023 (DPDP Act) enshrines the Right to be Forgotten (RTBF), enabling individuals to request the deletion oftheir personal data under specific conditions. This right helps individuals managetheir digital identity and avoid undue judgment based on past actions. Originatingfrom French law and gaining global recognition through frameworks like the European Union's General Data Protection Regulation (GDPR), RTBF reflects agrowing commitment to safeguarding privacy and promoting human dignity. Section 12 of the DPDP Act allows data principals to request data erasure whenthe purpose of collection is fulfilled, consent is withdrawn, or retention is nolonger required by law.

The RTBF acknowledges the intrinsic link between personal data and humandignity, ensuring that individuals can reclaim control over their online existence.At the same time, this right also raises concerns about freedom of expression and accessto information. Courts and policymakers must continually balance these competinginterests.In India, the claim to right to be forgotten draws enforceability from right to privacy which was recognized as a fundamental right under Article 21 of the Constitution in *K. Puttaswamy* v. *Union of India*.[10] However, in the absence of explicit legal provisions recognizing RTBF, various high courts have interpreted its scope differently. In their deliberations, courts have sought to harmonize this right with broader constitutional values such as transparency, free speech, and individual autonomy.

10 *Supra* note 2.

In the case of *SK* v. *Union of India,*[11] the petitioner approached High Court of Delhi seeking masking of his name in a judgment dated July 4, 2018 of the Court of the ASJ, Rohini Courts, titled '*State* v. *SK*'. The single judge bench observed that no case under section 376/506 of the Indian Penal Code, 1860 was made against the petitioner beyond reasonable doubt and the testimony of the prosecutrix was held to be not trustworthy, the Petitioner was acquitted of all charges by the trial court. The petitioner contended that he had suffered immensely due to the existence of the said judgment on the internet. Even a mere search on the web reflected the name of the petitioner and the same was also affecting his personal life and family life.

Hence, the court directed Indian Kanoon to mask the name of the petitioner from the judgment within a week. The court further directed Indian Kanoon to place on record an affidavit stating its policy in respect of the right to be forgotten and of masking of names in such cases including in judgments of this court and in orders and decisions passed by the trial courts.

In *Vysakh K.G.* v. *Union of India*[12] the High Court of Kerala disposed of nine different petitions dealing with removing judgements in the public domain on the grounds of the right to be forgotten filed under various sections. In all these petitioners, the petitioners sought removal of the published judgements on Indian Kanoon and de-indexing of those search results from Google submitting that the right to be forgotten is a part of the right to privacy.The counsel(s) argued for petitioner's right to seek erasure of contents that are unnecessary, irrelevant, inadequate, or no longer relevant. Additionally, the counsel(s) relied on the Supreme Court's judgement in the case of *Justice KS Puttaswamy (Retd)* v. *UOI.*[13] The petitioner's counsel submitted that the judgement puts the petitioner's identity in the public domain. As a result, this causes substantial prejudice to the petitioner The petitioner's counsel submitted that the publication of these judgements has infringed his right to privacy. There are no guidelines regarding the publication of details of individuals in cases involving the settlement between the parties. The petitioner's counsel submitted that the publication of the judgment contravenes the Supreme Court e-Committee's directions which direct all the high courts to refrain from uploading case-related information except case numbers and status on the internet in matrimonial matters.

The court observed that the problem of the present nature of the right to privacy has arisen as an impact of technology in our lives. In light of the *Puttaswamy*[14] judgement, the court leaned in favour of defining privacy in relation to court data to include parties' names and causes.Anonymity is the subject of privacy in a courtroom. A subtle distinction exists between anonymity and privacy in relation to the contents of judicial proceedings.The courts have not formed any

11 2023 SCC OnLine Del 3544, Order dated May 29, 2023.

12 2023(1)KLT83.

13 *Supra* note 2.

14 *Supra* note 2.

policy on open data. However, the larger public interest compels the judiciary to share data with the public.This right developed as a consequence of the dignity of an individual. It aims to help individuals forget the past and live in the present.

Although the European Union's Data Protection Directive of 1995 contained no express right to be forgotten, the Grand Chamber of the Court of Justice of the European Union (CJEU) held that an implied right existed in the Directive in the case of *Google Spain* v. *AEPD.*[15] In the digital context, the right to delisting and the right to oblivion are two facets of this right. Under GDPR, article17 provides individuals with a right to seek erasure of their personal data if it is no longer necessary for the purpose of its collection. However, the right to erasure is the right to be forgotten in the European context. This right relates to the past, and a party cannot claim it as a *right in presentium*. As per the bench, a claim to protect personal information based on privacy cannot co-exist in an open justice system. A party cannot claim this right in current proceedings or proceedings of recent origin. The Legislature can fix grounds for the invocation of such a right. At the same time, a court may consider facts and circumstances to permit a party to invoke this right. The court cautioned that the court's Registry should not publish the parties' personal information in family and matrimonial cases. Further, the Registry shall not allow any form of publication containing the identity of the parties. The High Court Registry should publish privacy notices on its website in English and vernacular languages. The court held that in matters of criminal cases, the petitioners cannot invoke the right to delete past records. Also, there is no reason to grant the removal of personal information in a habeas corpus petition rejecting the writ petition. However, in matters falling under matrimonial and family matters, court granted the relief sought to the petitioners and mandated Google to de-index the names of parties from the search results. Moreover, the Registry was directed to ensure that the Indian Kanoon website hides the personal information of the parties online.

In the case of *X* v. *Union of India,*[16] the court addresses the issue of privacy violation in relation to the uploading of Non-Consensual Intimate Images (NCII) and its connection to various legal provisions, including the IT Act and the Constitution of India. The court reiterated that any order passed by the appropriate government or agency must be in pursuance of the infringement of any prevailing law, in this case, a violation of the IT Act, IT Rules, and the fundamental right to privacy under Article 21 of the Constitution.

Furthermore, the right to privacy also encompasses the concept of the right to be forgotten. This right empowers individuals to request the removal of personal data from public view, acknowledging that people should have control over their digital presence and how their data is shared. This principle aligns with section 66E of the IT Act, which ensures that individuals have a reasonable expectation of privacy, even in cases where intimate images are shared in a private context.

15 ECLI:EU:C:2014:317 (Neutral Citation).

16 2023:DHC:2806, MANU/DE/2685/2023 (Decided on Apr. 26, 2023).

The High Court of Kerala, in the case of *Vysakh K.G.* v. *Union of India* [MANU/KE/3657/2022],[17] also emphasized the importance of informational autonomy in the digital era. Referring to the right to be forgotten, the court linked it to the right to delisting and oblivion, which are necessary for protecting an individual's privacy on the internet. This aligns with the idea that individuals should have the power to control the information about themselves that is accessible online.

The court also rejected the argument made by the respondent intermediaries (search engines), who claimed they were not responsible for the content they host. The court pointed out that intermediaries must respect the constitutional rights of citizens, including the right to privacy, and that the continued existence of NCII content online does not serve any public interest and is punishable under the IT Act. Therefore, the court emphasized that intermediaries must take responsibility for ensuring that privacy rights are not violated. The court reinforced that privacy is a fundamental right and extended this protection to individuals' digital lives, ruling that intermediaries must respect individuals' rights and take actions to remove harmful content.

III BLOCKING OF WEBSITES BY GOVERNMENT UNDER SECTION 69A OF IT ACT

Section 69A of the Information Technology Act, 2000 ("IT Act") confers upon the Union Government the authority to block online content in the interest of national security, sovereignty, public order, or relations with foreign states. The exercise of this power, however, is subject to adherence to the procedural safeguards specified in the Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 ("Blocking Rules"). These safeguards include the requirement to issue a 48-hour notice to the content originator or intermediary, and, in most instances, provide an opportunity for a hearing before a blocking order is made. In cases deemed urgent, Rule 9 permits the government to bypass the notice and hearing requirements, although such actions are subject to post facto review by a designated review committee. Additionally, Rule 16 mandates strict confidentiality regarding the details of the blocking process.

In *Shreya Singhal* v. *Union of India,*[18] the Supreme Court upheld the constitutionality of s. 69A, interpreting the provision in the context of permissible restrictions on free speech under article 19(2) of the Constitution. The court acknowledged that the provision aligned with legitimate grounds for curtailing speech, such as national security and public order, while confirming that the blocking rules provided adequate safeguards, including the requirement for written orders subject to judicial review.

However, with the expanding scope of government blocking powers in the digital age, concerns have been raised regarding the balance between curbing

17 *Id.* at para 44.

18 2015 (5) SCC 1.

harmful online content, such as misinformation and hate speech, and preserving the right to free expression. This tension underscores the need for content regulation to be transparent, accountable, and consistent with constitutional principles.

A recent case, *Tanul Thakur* v. *Union of India,*[19] underscores these concerns. In this matter, the petitioner, Tanul Thakur, alleged that his satirical website "Dowry Calculator" was blocked under section 69A without being provided with prior notice or an opportunity to be heard, thereby highlighting a critical issue regarding the application of procedural safeguards. The case raises important questions about whether the government's use of blocking powers aligns with the due process requirements established under the Blocking Rules, emphasising the need for a balanced approach to content regulation that respects both public order and fundamental rights.

The protection afforded to intermediaries under section 79(1) of the Information Technology Act, 2000 ("IT Act"), commonly referred to as the 'safe harbour' provision, is not absolute. One key condition for the applicability of this immunity is the intermediary's compliance with orders issued under section 69A of the Act. Failure to comply with such orders can result in the forfeiture of the safe harbour protection. Section 69A confers upon the government the authority to direct intermediaries or relevant government agencies to block access to any information generated, transmitted, received, stored, or hosted on computer resources, provided the information falls within the specific grounds enumerated in the section (which are discussed in detail below).

Exercising its powers under section 69A, the government routinely issues directives to block or remove content on various intermediary platforms. In a significant development, Twitter approached the High Court of Karnataka under its writ jurisdiction in *X Corp* v. *Union of India*[20] on June 30, 2023, challenging multiple blocking orders issued by the Ministry of Electronics and Information Technology (MeitY), Government of India.

This case is emblematic of the complex intersection of free speech, national sovereignty, and intermediary safe harbour protections in India. It has been heard by both the High Court of Delhi and the High Court of Karnataka. The government's blocking orders, issued under section 69A, targeted 1,474 Twitter accounts and 175 tweets during the period from February 2021 to February 2022, raising important questions about the balance between content regulation and fundamental rights.

Twitter approached the High Court of Karnataka under article 226 and 227 of the Constitution of India seeking quashing of the blocking orders on the following grounds: (i) procedural and substantive non-compliance of section 69A of the Act in light of *Shreya Singhal* v. *Union of India;*[21] (ii) power to issue blocking orders

19 W.P.(C) 788/2023.

20 MANU/KA/2230/2023

21 *Supra* note 18.

is information specific; (iii) blocking of anticipatory information is not authorised; (iv) absence of notice to the account users, which is mandatory; (v) failure to provide reasoning; the reasons cannot be outsourced from the file; (vi) impugned blocking orders are not speaking orders; (vii) non-communication of reasons renders the actions void; (viii) directions are disproportionate as "least intrusive means" not employed; (ix) violation of article 14, 19 and 21 of the Constitution of India; and (x) violation of principles of natural justice as no opportunity of hearing before the review committee given.

This writ petition was filed under article 226 by the petitioner claiming to be an intermediary against the blocking order issued by the Government of India on February 2, 2021 requiring the petitioner to block access to specific information and suspend some twitter accounts. The petition challenged the blocking orders on account of substantive and procedural non-compliance with section 69A specifically according to the mandate of *Shreya Singhal* case.[22] The power to issue blocking orders is information-specific, and blocking anticipatory information is not authorised under the law.

It was also argued that blocking anticipatory information is unauthorised, and that there was no prior notice to the originators of the content. Additionally, the blocking order lacks proper reasons, making it legally flawed, and the action is disproportionate, violating art.14, 19, and 21 of the Constitution. The petition also highlights the lack of a hearing before the Review Committee, violating natural justice principles.

The high court framed eight questions of law for consideration. The ratio laid down in the case is summarily captured below:

i. Whether Twitter being a foreign entity could invoke the writ jurisdiction?

Although certain fundamental rights, such as those under Articles 19 and 21 of the Constitution, are restricted to citizens and natural persons, the court clarified that its powers under article 226 extend beyond fundamental rights to include matters pursued "for any other purpose." The court reasoned that Twitter, facing the potential loss of immunity under section 79(1) of the IT Act, had sufficient locus standi to invoke the writ jurisdiction. It emphasised that article 226 could be employed to address statutory violations independent of fundamental rights. Recognising that constitutional questions were secondary, with Twitter's claims primarily based on alleged statutory breaches, the court, relying on both domestic and foreign jurisprudence, affirmed Twitter's entitlement to seek judicial review.

ii Whether the power under section 69A of the Act read with Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009 ("Website Blocking Rules") allows blocking of entire accounts or is only specific to individual Tweets?

The court held that the text of the legislation could not be read in a manner that would defeat the intent of the statute; legislative logic and realities of the

22 *Ibid.*

cyber world required that blocking of accounts would also be allowed. The court further opined that a ban on the account would serve as a better deterrent for a user, than a ban on a specific tweet. This was found to be in keeping with the intent of section 69A, which was held to be not merely penal and curative, but also preventive.

iii Is communication of reasons required while issuing blocking orders, and whether absence of the same in the present case made the orders void?

The court emphasised that, as a general principle, statutory provisions requiring the recording of reasons must be complied with, and principles of natural justice mandate transparency in decision-making. However, it acknowledged that in exceptional cases, reasons may be withheld for valid grounds. In the present matter, the court found the blocking orders to be sufficiently reasoned.

The court noted that the orders referenced instances of spreading fake news and misinformation about the farmers' protest through specific Twitter URLs and hashtags, which had the potential to disrupt public order. Additionally, the use of objectionable terms likely to provoke farmers was highlighted, justifying the necessity of the takedown measures.

Addressing Twitter's contention that the takedown orders lacked proper reasoning, contrary to the Supreme Court's ruling in *Shreya Singhal* v. *Union of India*[23], the high court clarified that literal adherence to the requirement of issuing "reasons in writing" was not mandatory in every instance. It held that as long as the rationale for State action and an overarching sense of fairness were discernible, procedural deviations would not invalidate the orders. The court observed that the tweets identified by MeitY fell within the grounds stipulated in section 69A of the IT Act, making the reasons for their blocking evident. Consequently, the procedural non-compliance with the *Shreya Singhal*[24] directives was deemed insufficient to invalidate the blocking orders.

iv Whether the impugned blocking orders were bad in law for not being founded on discernible reasons relatable to objectionable content?

Based on the material placed before it, the court took the view that there existed a thick nexus between the orders and the reasons assigned.

v Whether notice to the users is mandatory in terms of Rule 8 (1) of the Website Blocking Rules?

Rule 8 of the Website Blocking Rules outlines the procedure to be followed when a request for blocking is made. Rule 8(1) requires the concerned authority to issue a notice to the person or intermediary controlling the computer resource, requesting a reply and clarification. The court observed that Rule 8(1) only mandates the authority to identify either the person or the intermediary, not both, thereby giving discretion to the authority regarding whom to issue the notice. Consequently, the court ruled that issuing a notice to the user was not obligatory.

23 *Ibid.*
24 *Ibid.*

In challenging the blocking orders, Twitter argued that Rule 8 required MeitY to identify the person or intermediary and issue a notice before taking any action. Twitter further relied on the Supreme Court's observations in *Shreya Singhal,*[25] where it was stated that if the originator was identified, they must be heard before a blocking order is passed. The court, however, clarified that judicial observations do not carry the weight of statutory provisions. Since *Shreya Singhal*[26]did not involve "reading down" Rule 8 to necessitate a hearing, its remarks could not be construed as altering the statutory requirement from an "or" to an "and."

The court also upheld the non-issuance of notice to originators in this case, as the content was deemed "anti-India" and "seditious." Moreover, the court noted that even if a hearing were offered to the originators, Twitter could not assert their rights on their behalf, and since no originator had complained of rights infringement, the argument against non-compliance with Rule 8 was rejected.

vi Whether the blocking orders were violative of doctrine of proportionality?

The court rejected Twitter's argument that blocking orders should apply solely to specific tweets rather than entire user accounts, deeming such an approach impractical. It affirmed that account-wide blocking could be justified in exceptional cases, referencing Twitter's own user agreement, which permits account suspension in extreme circumstances. This further supported the proportionality of the blocking orders.

In doing so, the court revisited the principles established in *Shreya Singhal* v. *Union of India,*[27] where the doctrine of proportionality was scrutinised. In that case, section 66A of the IT Act was struck down for its disproportionate impact on the right to free speech. However, section 69A was upheld, with the court finding it constitutionally valid and narrowly tailored to address the specific grounds under article 19(2).

Twitter's primary legal challenge concerned the scope of section 69A, arguing that it only permitted tweet-specific blocking and not the blocking of entire accounts. The court dismissed this interpretation, stating that a narrow reading would undermine the legislative intent of section 69A. It emphasised the preventive purpose of the provision, aiming to curb the spread of harmful content as per the grounds outlined in article 19(2). The court clarified that the provision extended beyond penalising the originator of specific tweets and allowed for the preemptive blocking of content, including potential future posts. Consequently, the court upheld the Union Government's authority to issue blocking orders that applied to entire accounts under section 69A.

While evaluating the blocking orders' adherence to proportionality, the court noted that the least rights-restrictive measure must be employed. Twitter argued that account-wide blocking, without first addressing individual tweets, was

25 *Supra* note 18.
26 *Ibid.*
27 *Ibid.*

disproportionate. The court found that blocking entire accounts was an effective measure to prevent the dissemination of harmful content, and that limiting the blocking to specific tweets would render the content-takedown regime ineffective. The court also declined to set a time limit for the duration of the blocking orders, citing the principle of separation of powers.

vii Whether the conduct of Twitter disentitled it to relief?

The court observed that Twitter delayed in complying with the orders under section 69A (in some cases of more than a year), and only complied shortly before coming to court. It was held that Twitter was not entitled to any relief due to its culpable conduct.

viii Whether the conduct of Twitter made it liable for levy of exemplary costs?

The court, finding Twitter's willful non-compliance with MeitY's blocking orders, imposed exemplary costs amounting to INR 50,00,000 (Fifty Lakhs). The Court observed that some blocking orders remained uncomplied with for over a year, with Twitter adopting a tactical approach to delay compliance, demonstrating an intent to remain non-compliant with Indian law. The court emphasised that constitutional courts do not support litigants who act in bad faith or with indolence, and it deemed Twitter's conduct an offence under s. 69A(3) of the IT Act, which also had broader societal harm. Consequently, the court directed Twitter to deposit the exemplary costs with the Karnataka Legal Services Authority.

While section 69A was upheld as constitutionally valid in the *Shreya* Singhal[28]case, the court ensured that its powers are used judiciously, emphasising that restrictions on internet access must comply with the test of proportionality under Article 19(2). The Supreme Court in *Anuradha Bhasin* v. *Union of India* had reiterated that internet shutdowns should be used only when necessary and unavoidable. In this case, the High Court of Karnataka found that MeitY's blocking orders were in compliance with the principles laid down in *Shreya Singhal.*[29]

The High Court's of Karnataka ruling on the interpretation of section 69A of the Information Technology Act (IT Act) significantly expanded the scope of the government's power to block online content, including entire user accounts, rather than just specific tweets or posts. This broad interpretation contradicts the Supreme Court's decision in *Shreya Singhal,*[30] where the court emphasised that any ambiguity in statutes related to freedom of speech must be interpreted narrowly to avoid a chilling effect. The high court's decision to allow blocking of entire accounts is criticised as disproportionate and a violation of the user's right to free speech under article 19(1)(a), as it prevents future speech from being posted, regardless of its content.

By allowing account-wide blocking without a clear threshold or guidelines for its application, the judgment is said to have opened the door to excessive

28 *Ibid.*
29 *Ibid.*
30 *Ibid.*

governmental control over online discourse. This interpretation also assumes the future speech of the user will always fall within the grounds for blocking, which is both speculative and restrictive.

On procedural matters, the court upheld the non-requirement for the government to provide reasons for blocking orders, provided that the intermediary is notified, contradicting the procedural safeguards established in *Shreya Singhal.*[31] The Supreme Court had previously held that a reasoned order is crucial for judicial review and challenges against blocking orders under article 226. By not mandating notice to both the intermediary and the originator of the content, the high court is said to have undermined the principles of natural justice, which require transparency and fairness in governmental actions that affect fundamental rights.

The court also disregarded the necessity for issuing notice to the originator of the content, which had been upheld by the Supreme Court in *Shreya Singhal.*[32] While Rule 8 of the Blocking Rules allows flexibility in identifying the person or intermediary, the court's interpretation raises concerns about the adequacy of "reasonable efforts" to identify the originator, especially when it is easier to identify intermediaries rather than users. This could result in an erosion of the originator's rights and their ability to challenge the blocking orders effectively.

In conclusion, the high court's reading of section 69A—allowing entire user accounts to be blocked—and its lack of attention to proper procedural safeguards raise serious concerns about free speech and fair process. This ruling potentially undermines the constitutional protections offered by article 19(1)(a) and the procedural principles established by the Supreme Court in *Shreya Singhal.*[33] The expansive powers granted to the government under this decision may be subjected to scrutiny, particularly regarding the practical implications for users' rights to free expression and access to justice, in future decisions.

IV CYBER OBSCENITY

The proliferation of digital technology and the internet has raised significant concerns regarding the dissemination of obscene and harmful content, particularly in relation to cyber obscenity. The IT Act addresses this issue through various provisions aimed at curbing the transmission and publication of obscene and sexually explicit material in electronic form. Sections 66E, 67, 67A, and 67B of the IT Act establish penalties for the publication or transmission of such material, with varying degrees of imprisonment and fines, depending on the nature of the offence. Specifically, section 67 criminalises the publishing of obscene material, while s. 67A addresses sexually explicit content, and section 67B provides stricter punishment for material depicting children in sexually explicit acts. These offences are classified as cognizable under section 77B, allowing law enforcement to take immediate action.

31 *Ibid.*
32 *Ibid.*
33 *Ibid.*

In addition to the IT Act, the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 impose additional responsibilities on intermediaries such as social media platforms and online service providers. These rules mandate that intermediaries must ensure that users do not engage in the hosting, sharing, or transmission of content that is obscene, pornographic, pedophilic, or harmful to minors. Rule 3(2)(b) specifically requires that intermediaries remove, within 24 hours, any content that infringes on an individual's privacy by exposing private areas, depicting nudity or sexual acts, or involving impersonation or morphed images. Together, these legal frameworks reflect a robust attempt to combat cyber obscenity and protect individuals from online harm, particularly in the age of rapid digital communication and media sharing.

In *Gautam Kumar Vishwakarma* v. *State of U.P,*[34] an FIR dated June11, 2022 was lodged by the prosecutrix under section 363, 366, 376, 506, 323 IPC, s. 3/4 POCSO Act, section 66 and 67 of the IT Act, and section 3(2)(V) of the SC/ST Act at Gagaha Police Station, Gorakhpur. The FIR named four accused, including Gautam Vishwakarma, alleging kidnapping, rape, creation of obscene videos, and threats. However, the FIR lacked specific details regarding dates, times, and locations of the alleged incidents. It mentioned an incident three years prior and another on January 5, 2022, claiming that the obscene videos were made viral.

The applicant's counsel argued that there was no medical evidence supporting the charges against him and highlighted that the obscene video was allegedly made viral by co-accused Gyanendra Gaur, not the applicant. The delay in lodging the FIR, which remained unexplained, rendered the case weak as per the Supreme Court's ruling in *P. Rajagopal* v. *State of Tamil Nadu*[35](AIR 2019 SC 2866 (para 8).

The court noted that the allegations under section 66 and 67 of the IT Act, related to transmitting obscene material electronically, primarily implicated co-accused Gyanendra Gaur. The applicant's role in creating or circulating such content was not clearly established. Given the applicant's lack of prior criminal history, the absence of medical corroboration, and the delay in filing the FIR, the court found his custodial detention unnecessary.

The court granted bail, emphasizing that the evidence against the applicant had been gathered, and his case differed from that of co-accused Gyanendra Gaur, who faced direct charges under the IT Act for making the video viral.

In another case *Anil Kumar vs The State of Bihar,*[36] the matter related to the offence of gang rape of two sisters one aged nearly 16 years and her younger sister aged nearly 14 years by eight boys on gun point where one of the boys had video-graphed the occurrence. The charge of commission of offence punishable under s. 67-B of the IT Act was based on the accusation that after having video

34 2023:AHC:158171(decided on Aug. 7, 2023).

35 *Ibid.*

36 MANU/BH/0700/2023(decided on June 28, 2023).

graphed the occurrence of rape, the same was made viral and video was sent by accused Kamlesh through WhatsApp to PW-3. The witness (PW3) had given his mobile phone to the police at the police station and the police had taken print-outs of the video and photo from his mobile phone. However, the court ruled that they didn't find any admissible evidence adduced at the trial that PW-3 had received any electronic message from the mobile phone of the appellant Kamlesh. The mobile phone of PW-3 was not seized nor the contents of electronic record were proved at the trial in accordance with the requirement of s.65B of the Evidence Act. The prosecution relied on the print-outs taken out by the police from the mobile phone of PW-3. PW-11, who is said to have accompanied PW-3 to the police station for handing over the video and photo-stat copies of the photographs, deposed that PW-3 had come with a prepared video.

The court said that as per*Anwar P.V* v. *P.K.Basheer,*[37] an electronic record is admissible as evidence only when it is duly produced in terms of section 65B of the Evidence Act *i.e.,* either the recording device itself is produced or the copy of recording as secondary evidence along with a 65B certificate is produced and that the requirement of the same cannot be substituted or satisfied by oral evidence. In the present case, the mobile phone of PW-3, from which, according to the prosecution's case, print-outs were taken, was neither seized nor produced at the trial. There was no evidence to substantiate that the said video, of which photocopies were said to have been taken from mobile phone of PW-3, was actually sent by the appellant Kamlesh.[38]

The court observed that since the electronic evidence was inadmissible due to non-compliance with section 65-B of the Evidence Act, it rendered the digital evidence inadmissible. Additionally, the prosecution failed to establish a clear link between the accused and the alleged creation or dissemination of the obscene material. These shortcomings in handling the electronic evidence significantly weakened the charges under the IT Act, contributing to the acquittal of the appellants. In view of the aforesaid discussion, the appellants' conviction for the offence punishable under section 67-B of the IT Act was not upheld.

In *TVF Media Labs Pvt Ltd* v. *State (Govt. of NCT of Delhi)*[39] an FIR was lodged against the appellants under s.292 and s.294 of the IPC and section 67 and section 67A of the IT Act as the vulgar language used in the webseries 'College Romance' is *prima facie* capable of appealing to prurient interests of the audience and is hence obscene by relying on the decision of this court in *Sharat Babu Digumarti* v. *Government (NCT of Delhi).*The appellants on the other hand argued that the allegedly offending portions of Season 1, Episode 5 of the web-series do not meet the threshold for obscenity and that the high court has erred in characterising the material as obscene. Further, these portions do not contain any

37 (2014) 10 SCC 473.

38 *Anil Kumar* v. *The State of Bihar* , *supra* note 17.

39 2023:DHC:1683(decided on June 6, 2023) heard and decided along with *Simarpreet Singh* v. *State of NCT of Delhi*[Case Reversed/Partly Reversed by: *Apoorva Arora.* v. *State (Govt. of NCT of Delhi)*(MANU/SC/0218/2024).

sexually explicit act and as such no offence under section 67 or section 67A of the IT Actis made out.

It was argued that as per *Aveek Sarkar* v. *State of West Bengal* [AIR 2014 SC 1493] the determination of whether some material is obscene or not must be made by the 'community standard test' by considering the work as a whole and then looking at the specific material that has been alleged to be obscene in the context of the whole work: The web-series is a romantic comedy that traces the life of a group of friends who are in college. Its intention is to paint a relatable picture of college life in a cosmopolitan urban setting. Two specific portions that were alleged to be obscene- the first, where the male protagonist, named Bagga, indiscriminately uses expletives that are heard by the female protagonist, named Naira, who objects to the use of such language and points out that the literal meaning of the terms is absurd. Bagga states that these terms are not meant to be taken literally and are a part of common parlance. Naira reiterates her disapproval and threatens Bagga with consequences if he continues to speak in such a manner. Bagga 'inadvertently' uses another expletive, due to which Naira leaves from there. In the second segment, Naira and Bagga are with a wider group of friends where Naira is incensed by the statements of another friend and angrily uses the same expletives as Bagga, at which Bagga is delighted. Learned senior counsel has argued that when these scenes are considered individually and in the context of the web-series as a whole, they are not obscene. They only portray the absurdity of the literal meaning of these terms and show their inevitable presence in common language, including by those who disapprove of their use.

Relying on *Samaresh Bose* v. *Amal Mitra* (MANU/SC/0102/1985),[40] senior counsel argued that while the alleged portions are vulgar, vulgarity does not equate to obscenity. Mere words cannot amount to obscenity unless they involve lascivious elements that arouse sexual thoughts and feelings, which is not the effect of the scenes in the present case. The effect of the words must be tested from the standard of an "*ordinary man of common sense and prudence", "reasonable, strong-minded, firm and courageous"* person and not from the perspective of a hypersensitive person or a weak and vacillating mind. The terms used in the allegedly offending portions do not refer to any sexually explicit act and are not obscene as per the community standard test. Therefore, no offence of obscenity was made out under section 67 of the IT Act. Learned senior counsel has also argued that the scenes do not contain any sexually explicit act or conduct, as is required for an offence under section 67A.

Lastly, the senior counsel argued that a higher threshold of tolerance must apply in the present case as the web-series is a form of "pull media". In pull media, the consumer has more choice in deciding whether or not they wish to view some particular content. Unlike television or radio, where obscene material may be publicly broadcasted and there is little to no choice to the users in terms of what content is made available, the consumption of pull media over the internet gives the viewer

40 *TVF Media Labs Pvt Ltd* v. *State (Govt. of NCT of Delhi)* at para 37.

complete control and decision-making over what they watch. Therefore, the web-series is only available and accessible to those persons who wish to view it, and hence a higher threshold of obscenity must be applied to "pull content".

Sections 292 and 294 IPC cannot exist together with section 67A IT Act, if the content is only confined to the digital media and since the obscenity pertaining to electronic media can be dealt only under section 67 of IT Act and 67A of the IT Act, and not under section 292 and 294 of IPC.The object behind enactment of section 67 of the IT Act is punishing acts of publishing or transmitting obscene material in electronic form. Section 67A lays down that transmission of sexually explicit material circulated through cyber space is punishable. The prosecutor contended that there was no disclaimer or warningthat the content was meant for people above 18 years. The languages used in the web series is such that it will not be used by general public and that section 67A of IT Act makes it clear that sexually explicit content will also include the language used in web series.

The court, upon reviewing the case file, concluded that the content of the web series must be assessed under sections 67 and 67A of the IT Act. The lower courts primarily based their findings on Episode5 of Season 1, where the petitioners allegedly used obscene language throughout. The Additional Sessions Judge (ASJ) determined that the case warranted registration of an FIR under section 67A of the IT Act, instead of section 292 and 294 of the IPC, as previously suggested by the Additional Chief Metropolitan Magistrate (ACMM). The ASJ's conclusion was based on the premise that the petitioners published and transmitted material that was lascivious, appealed to prurient interest, and tended to deprave and corrupt viewers.

The complainant argued that the web series "College Romance" violated the community standards test, as its vulgar language and content could corrupt viewers, particularly impressionable minds, and misrepresent college life. The petitioners however, countered that the series adhered to contemporary societal standards, where vulgarity does not equate to obscenity, and should be judged from the perspective of an ordinary person, not a hypersensitive one.

The court reviewed the episodes, finding excessive use of profane, vulgar, and obscene language, including explicit references to sexual acts. It held that such language was not reflective of commonly spoken language in India and could not be heard without embarrassment, breaching societal norms of decency. The absence of age-appropriate warnings or disclaimers further heightened the risk for young viewers.The court noted that while terms like "obscene" and "lascivious" are not defined in the IT Act or IPC, judicial precedents and dictionary definitions offer guidance. Applying the standard under section 67 of the IT Act, which penalizes transmitting lascivious material likely to corrupt viewers, the Court concluded that the series crossed the threshold of decency. Citing *Samaresh Bose* v. *Amal Mitra* (*supra*), it emphasized the need to judge content against national standards and contemporary morals. The court held that the web series violated section 67 of the IT Act, as its language and explicit content posed a risk of corrupting impressionable minds, thereby justifying legal action.

The court emphasized the need to regulate the use of vulgar language, profanity, and obscene content on social media platforms, especially those accessible to children. It noted that while individuals have the freedom to choose their language, the widespread use of foul language in public domains cannot receive constitutional protection under free speech, as it risks corrupting impressionable minds. The court rejected the argument that such language reflects contemporary societal norms and upheld its duty to act when self-regulatory bodies fail to curb the dissemination of indecent content.

The court held that content like the web series 'College Romance', which excessively employs vulgar and sexually explicit language, does not mirror the real-life behaviour of Indian college students or society. It stressed that the language used in the series violates societal norms of decency and fails the "community standards test." The series, despite claims of representing modern youth culture, cannot legitimize the use of profane language by portraying it as the norm. The court noted that such content risks degrading linguistic and moral standards, impacting the youth and society at large.

The judgment highlighted the influence of media in shaping societal norms and cautioned against allowing unregulated platforms to normalize indecency. It dismissed the notion that societal evolution justifies a decline in linguistic and moral standards, asserting that the foundational values of civility and decency must be preserved.

The court clarified that it does not intend to engage in moral policing but recognizes its duty to ensure that public decency and societal values are upheld. It urged legislative and regulatory bodies to address gaps in the law governing online content. The judgment concluded by reaffirming the judiciary's role in interpreting and applying constitutional values to uphold the rule of law and protect societal welfare, especially in cases where existing laws are silent or ambiguous.

The court faced the challenging task of balancing free speech with the need to regulate obscene and sexually explicit language in the web series *College Romance*. It emphasized the powerful influence of words and their potential to corrupt impressionable minds. The court upheld the application of section 67A of the IT Act for transmitting obscene content while dropping charges under section 67 of the IT Act and section 292 and 294 IPC. It directed the registration of an FIR without arresting the accused and instructed YouTube to take remedial steps if the content remains posted. The court also urged the Ministry of Information and Technology to enforce stricter rules under the IT (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, and consider further regulatory measures to address emerging digital content challenges. The petition was disposed of accordingly.

V ELECTRONIC EVIDENCE AND SECTION 65B INDIAN EVIDENCE ACT

The law governing electronic evidence in India has evolved significantly, with section 65-B of the Indian Evidence Act, 1872(IEA), serving as a pivotal

provision for the admissibility of electronic records. This section requires a certification to authenticate electronic records, leading to extensive litigation and varied interpretations by the Supreme Court regarding the mandatory nature of this requirement.

With the Bharatiya Sakshya Adhiniyam (BSA), 2023 set to replace section 65-B with section 63, several new changes have been introduced. The BSA mandates dual certification: one by the individual responsible for the device and another by an expert, along with the inclusion of a hash value to ensure the authenticity of electronic evidence. However, ambiguity persists regarding the definition of an "expert," with parallels drawn from section 45A of IEA and s. 79A of the IT Act, which recognise court-appointed examiners of electronic evidence.

These changes aim to strengthen the reliability of electronic records but bring significant challenges. Limited infrastructure, a mere 15 certified examiners nationwide, and technological barriers for litigants risk delays, especially in civil cases. Questions also arise about ongoing trials that lack valid certificates under section 65-B. The Supreme Court's judgment in *Arjun Panditrao Khotkar* v. *Kailash Kushanrao Gorantyal*(*supra*) provides some flexibility, allowing fresh certificates in criminal trials without prejudicing the accused.

Further section 170 of the BSA explicitly exempts trials initiated before its enactment from its provisions, ensuring that evidence submitted before July 1, 2024, remains governed by the IEA. In such cases, any new certificates must comply with the provisions of the 1872 Act. Adhering to the BSA's requirements, such as hash value reports and expert certification, may necessitate re-transmission of evidence, rendering earlier submissions obsolete. This introduces procedural complexities, potentially increasing litigation burdens and delaying justice. Courts must address these issues to ensure a seamless transition to the new framework.

The plaintiff in. *Sai Infra Equipment Pvt. Ltd* v. *Geo Foundations and Structures Pvt.*[41] filed this money suit to recover a sum of Rs.1,01,11,084/- from the defendant together with interest @ 24% per annum on the aforesaid amount of Rs.1,01,11,084/- from the date of plaint till date of realisation. The plaintiff has claimed that the aforesaid amount is allegedly due from the defendant for the usage of the construction materials/equipment's of the plaintiff hired by the defendant. The petitioner relied on computer-generated documents, stored securely in the plaintiff's email account, as evidence. These documents, accessible only by the plaintiff, include email communications marked as Ex.P.8 to Ex.P.14 and printed from the plaintiff's computer. However, the Supreme Court in *Anvar P.V.* v. *P.K. Basheer* and *Arjun Panditrao* v. *Kailash Kushanrao Gorantyal* has laid down mandatory requirements under s. 65B of the IEA for the admissibility of electronic records. These include a certificate identifying the electronic record, describing its production method, specifying device details, addressing conditions under section 65B(2), and being signed by a responsible official. The plaintiff's affidavit failed to meet these requirements. Consequently, emails marked as Ex.P.8 to Ex.P.14,

41 C.S. (Comm. Div.) No.10 of 2022 (decided on May 24, 2023).

despite mentioning outstanding dues and related transactions, cannot be admitted as evidence due to procedural deficiencies.

The court held that the ledger marked as Ex.P.2, detailing financial transactions between the plaintiff and defendant for various years, also falls under "electronic records." Since no section 65B certificate accompanied Ex.P.2, the court ruled that it is inadmissible in evidence. Similarly, the bench reasoned that Ex.P.7, a legal notice, refers to Ex.P.8 emails but lacks supporting details of dues and fails to substantiate claims effectively. The outstanding amounts detailed in Ex.P.16 to Ex.P.37, along with tables summarising unpaid balances, also reveal a lack of clear documentation justifying the plaintiff's claims. Interest calculations for delays, spanning 2018 to 2021, aggregate the total outstanding balance with interest to a substantial figure, yet the lack of compliance with procedural requirements undermines the admissibility of evidence, held the court.

VI HACKING,TEMPERING OF SOURCE CODE AND SECTION 65A ITAINTERMEDIARY LIABILITY

In the case of *Suki Sivam* v. *You Tube*[42] the plaintiff, an eminent speaker with a global following, has filed a suit seeking a permanent injunction to prevent unauthorized individuals from uploading or exploiting his audio-visual works on platforms like YouTube, Facebook, and WhatsApp under defamatory captions, damaging his reputation and reducing his revenue. As the first owner of the copyright in his speeches, the plaintiff argues that such unauthorized reproduction constitutes copyright infringement under section 51 of the Copyright Act. The plaintiff contended that these actions infringed his exclusive rights under the Copyright Act, specifically section 14, 17, and 51, and sought an injunction against the defendants to prevent further infringement. Due to the untraceable nature of the offenders, he seeks a court order to restrain such activities and protect his intellectual property rights.

The defendants seek dismissal of the suit, asserting that the plaintiff failed to provide evidence of copyright ownership over the works listed in Annexure "A" and did not identify specific infringing content through URLs. They argue that the suit is defective due to the non-joinder of necessary parties and lacks concrete allegations.The first defendant, a platform provider, claims immunity under section 79(1) of the IT Act, which shields intermediaries from liability unless they fail to act upon actual knowledge of infringement provided through a court or government order. It denies any obligation to proactively monitor or remove content without specific URLs or legal notice.The second defendant, operating WhatsApp, highlights its end-to-end encryption, preventing access to user messages. It denies any responsibility for monitoring content and asserts it requires court or government orders to act.The third and fourth defendants, associated with Facebook, argue they merely provide a platform for third-party uploads and are immune under the IT Act. They claim no obligation to monitor or control content proactively.All defendants contend the plaintiff's claims are unsupported by

42 MANU/TN/4488/2023 (Aug. 9, 2023).

evidence or legal compliance, rendering the suit untenable. They seek its dismissal, emphasizing their limited roles as intermediaries and the absence of actionable legal grounds.

The court formulated the following issues for consideration:

(i) Whether the suit is liable to be dismissed for non-joinder of the alleged infringers?;

(ii) whether the defendants are exempted from liability in terms of s. 79 of the Information Technology Act, 2000?;

(iii) Whether any of the defendants infringed the copyright of the plaintiff?;

(iv) Whether the plaintiff is entitled to the relief prayed for against any of the defendants?;

(v) Whether the parties are entitled to any other relief?

The defendants claimed the plaintiff had not joined the alleged infringers as parties, making the suit bad for non-joinder. They also argued that the plaintiff failed to specify the URLs or phone numbers of the infringing content, making it impossible for them to identify and remove it. Emphasizing that intermediaries could only be held accountable upon being informed through a court order, the court highlighted the impracticality of expecting them to scrutinise every upload and post on their platforms for potential infringing content.

The plaintiff countered that intermediaries are obligated to exercise due diligence and cannot claim immunity in preventive relief cases. However, the defendants contended their roles as intermediaries under section 2(1)(w) of the IT Act, claiming immunity from liability for third-party content under section 79(1). The defendants highlighted their roles as mere facilitators, not creators or owners of the content, and noted that WhatsApp's encryption further limited their access. The defendants, as social media platform owners, argued they were not responsible for content uploaded by users and relied on s. 79(1) of the IT Act, which exempts intermediaries from liability for third-party content. The Supreme Court addressed this in *Shreya Singhal* v. *Union of India,*[43] stating that intermediaries could only be held liable if they had actual knowledge of unlawful content through a court order or a government directive under section 69A. The court clarified that intermediaries are not obligated to monitor user uploads but must act when notified of infringing content *via* formal channels.

The plaintiff's counsel argued that *Shreya Singhal*[44] only absolved the defendants from liability in civil and criminal cases, not in actions for injunctive relief. However, the court, referencing the *Shreya Singhal*[45] judgment, emphasized that the defendants could only be compelled to remove infringing content upon receiving a court or government order. Without identifying specific URLs or phone numbers of the infringing content, the injunction could not be implemented, as the

43 *Supra* note 18.

44 *Ibid.*

45 *Ibid.*

defendants could not be expected to monitor millions of uploads, complicating the plaintiff's claims without detailed evidence.

In similar cases, the court observed, including *Google India Pvt. Ltd.* v. *Visakha Industries* and *Myspace Inc.* v. *Super Cassettes Industries*, courts have consistently held that intermediaries are only responsible for taking down content once they receive actual knowledge *via* a court or government order under section 69 of IT Act and fail to act.The court concluded that while the suit was not bad for non-joinder of infringers, the plaintiff must specify the infringing URLs or phone numbers to enable the defendants to act. The court noted that the plaintiff had failed to provide specific evidence of infringement, such as URLs or identifying details of the alleged infringers. It held that injunctions against intermediaries must target specific content and cannot impose a blanket obligation to monitor all posts. The absence of identified infringers or specific infringing material weakened the plaintiff's case. In conclusion, the court dismissed the suit, reiterating that intermediaries like the defendants are only required to act upon specific notifications and cannot be held accountable for general allegations of copyright infringement.

The controversy in *Google LLC* v. *DRS Logistics (P) Ltd.*[46] centres on Google's Ads Programme, a platform that allows businesses to create and display paid ads on Google's search engine. These ads, labelled "Ads," appear alongside regular search results, and businesses bid on keywords in real time to secure better placement. For example, if a user searches for "Audi," competitors like Lexus or Porsche may display their ads by bidding on the keyword "Audi." Google also provides a tool called "Keyword Planner," which helps advertisers by showing search volumes for specific keywords and suggesting related ones. The issue at hand is whether this practice, particularly Google's use of trademarks as keywords, undermines competition and fairness in search results.

DRS Logistics (P) Ltd. (DRS) filed a grievance against Google, claiming that using its registered trademark "AGGARWAL PACKERS and MOVERS" as a keyword in Google's Ads programme allowed competitors to display ads that diverted internet traffic from DRS's website to rival sites. DRS argued that this practice amounted to trademark infringement and deceived consumers into believing they were engaging with DRS. DRS further argued that Google could not claim "safe harbour" protection under section 79 of the IT Act , as Google profited from these ads and actively suggested keywords through its "Keyword Planner."

Google, on the other hand, defended its actions, stating that the use of keywords in its Ads programme did not amount to trademark use under the Trade Marks Act (TM Act). Google argued that there was no consumer confusion and that it did not infringe on trademarks unless it had actual knowledge of such infringement. The court had to address whether Google's practice of permitting third parties to bid on trademarks, allowing their ads to appear on search result pages, constituted trademark infringement.

46 2023:DHC:5615-DB,MANU/DE/5136/2023 (decided on Aug.10, 2023).

The principal questions the court considered were:

i. Whether the use of trademarks as keywords amounts to "use" under section 29 of the TM Act.

ii. If so, whether the use of trademarks as keywords constitutes infringement by Google, or if it is solely the responsibility of the advertiser.

iii. Whether such use of trademarks amounts to infringement of a trademark under the TM Act.

iv. If so, whether Google can claim immunity under s. 79 of the IT Act, as an intermediary.

The key issue in the case was whether using trademarks as keywords constitutes "use" under the TM Act. Google contended that such use did not qualify as "use" because the keywords are invisible to users and are not physically or visually represented. Google argued that "use" under section 2(2)(b) of the TM Act requires a visible or printed representation. Additionally, Google pointed out that section 2(2)(c) requires the use of trademarks in relation to the availability or performance of services, which keyword use does not fulfil.

The court disagreed with Google's position, stating that section 29(9) of the TM Act extends "use" to spoken words, thereby broadening the scope beyond visual or printed forms. Citing cases such as *Amway India Enterprise* v. *1MG Technologies*[47] and *People Interactive* v. *Gaurav Jerry,*[48] the court held that keyword use could qualify as trademark use, even if the trademark is not visible to the user.

While Google contended that its use of trademarks as keywords was distinct from meta-tags, which are embedded in the website's source code, the court found that both serve a similar function—indexing and associating websites with search queries. The court noted that the use of meta-tags has been considered trademark infringement in cases such as *Amway India v. 1MG Technologies*[49] and *People Interactive* v. *Gaurav Jerry,*[50] where courts found that such practices diverted internet traffic dishonestly.

In the case of *Google LLC* v. *DRS Logistics*, the court ruled that using trademarks as keywords qualifies as trademark use under the TM Act, even if the use is invisible. It emphasized that this interpretation ensures that trademark law remains effective in addressing challenges posed by evolving internet and e-commerce practices. Moreover, the court clarified that using a trademark as a keyword to trigger ads constitutes trademark use in advertising, even though the trademark is not used to identify the origin of goods or services.

The court's analysis extended to whether Google's role as an intermediary could absolve it of liability under section 79 of the IT Act. Section 79 provides a safe harbour to intermediaries, protecting them from liability for user-generated

47 (2019) SCC OnLine Del 9061.

48 MIPR 2014(3) 101.

49 *Supra* note 48.

50 *Supra* note 49.

content. However, the court ruled that Google's active involvement in monetizing the use of trademarks as keywords, including providing keyword suggestions through its Keyword Planner, meant that Google could not claim the protection of section 79. In this case, Google's role was not passive, and it could be held liable for contributory infringement if it knowingly allowed trademark infringement on its platform or failed to act on complaints.

In terms of contributory infringement, the court held that Google could be liable for contributing to trademark infringement by allowing advertisers to use registered trademarks as keywords. The court also examined whether Google's use of trademarks as keywords caused consumer confusion. Although the court acknowledged that not every use of a trademark as a keyword automatically leads to confusion, it noted that if such use leads to a likelihood of confusion or harms the distinctiveness or reputation of the trademark, it could amount to infringement.

The doctrine of "initial interest confusion," which addresses trademark infringement based on confusion at an early stage (even if no confusion persists during a transaction), was also relevant in this case. Courts have applied this doctrine to meta-tags, keywords, and domain names, recognizing that even brief confusion can harm a trademark's goodwill. The court ruled that a real likelihood of confusion, even at the initial stage, could trigger liability under the Trade Marks Act.

The court concluded that Google's use of trademarks as keywords in its Ads programme could amount to trademark infringement, and that Google could be held liable for contributory infringement due to its active involvement in monetizing the use of trademarks. Furthermore, Google's safe harbour protection under section 79 of the IT Act was unavailable, as Google's role went beyond merely facilitating the use of keywords.

The court's judgment highlights the complexities of trademark infringement in the digital age. It emphasized the need to balance trademark protection with the promotion of fair competition in the online advertising ecosystem. The decision also underscores the importance of clear and non-deceptive advertising practices, especially in keyword advertising. Businesses engaged in digital advertising must ensure that their practices comply with trademark law to avoid infringing on the rights of trademark owners.

In *X* v. *Union of India,*[51] a married Indian woman (Mrs. X) met Richesh Manav Singhal online in December 2019, who allegedly assaulted her during a visit to her rented accommodation in Gurugram in July 2020. He transferred explicit photos from her phone, coerced her son into sexual acts, and threatened to leak the photos unless she paid him and gave him her jewellery. Singhal later uploaded her explicit images to pornographic websites and even created a YouTube channel under her name, regularly posting explicit content. In August 2021, X filed a police complaint and sought the help of intermediaries like Google and YouTube to

51 2023:DHC:2806,MANU/DE/2685/2023 (decided on Apr. 26, 2023).

remove the content. Despite repeated requests, the content was re-uploaded. She approached the High Court of Delhi for assistance in blocking access to these websites. The court appointed Senior Advocate Saurabh Kirpal as an *amicus curiae* to assist in balancing victim rights and intermediary responsibilities.

By March 2022, Singhal was arrested, and 83,000 explicit photos, including those of X, were found on his laptop, confirming his involvement in other similar cases. Though Singhal could no longer re-upload the images, the court continued the case to address systemic issues regarding content removal processes, ensuring victims wouldn't have to repeatedly seek help from authorities.The Ministry of Electronics and Information Technology (MeitY) submitted an affidavit highlighting the IT Act and the 2022 Intermediary Guidelines[52], emphasizing grievance redressal, content removal timelines, and the victim's right to request removal. However, the government contested the request to delink X's name from search results, citing concerns about freedom of speech and expression.

Non-Consensual Intimate Images (NCII) are sexually explicit materials shared without the consent of the individuals depicted, often resulting in profound psychological and social harm. While the term "revenge porn" refers to a subset of NCII, the broader category encompasses all types of non-consensual explicit content. Victims of NCII face serious emotional distress, social stigma, and mental health challenges, including suicidal ideation and significant impacts on their personal and professional lives. As the prevalence of NCII grows, driven by widespread internet accessibility, it has become evident that legal and regulatory interventions are needed to both prevent and address the distribution of such content.

While the IT Act and IT Rules do not specifically define NCII, Rule 3(2)(b) of the IT Rules establishes a grievance redressal mechanism for content that violates privacy, including explicit images, nudity, or sexual acts shared without consent, as well as morphed images. This rule mandates that intermediaries remove such content within 24 hours of receiving a complaint. However, the lack of explicit reference to non-consensuality in the definition under Rule 3(2)(b) has led to ambiguity, with violations of privacy governed by section 66E of the IT Act. This section penalizes the non-consensual capture, publication, or transmission of private images, including imprisonment and fines. Additionally, section 67 of the IT Act penalizes the publication or transmission of obscene or sexually explicit materials, with section 67B targeting content depicting children in sexually explicit acts.

Intermediaries, such as search engines, are critical in the distribution and removal of NCII. Under the IT Rules, 2021 (as amended in 2022), they are required to swiftly remove harmful content and cooperate with law enforcement when necessary. S. 69A of the IT Act grants the government authority to block access to

52 Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Amendment Rules, 2022 (passed on Oct. 28, 2022).

harmful content, with penalties for non-compliance. Together, these provisions aim to combat the abuse of NCII and provide protection to victims.

The Intermediary Guidelines under the IT Act govern intermediaries, such as social media platforms, and outline their responsibilities in handling user-generated content. A central provision in the law is section 79, which provides intermediaries with a "safe harbour" from liability for third-party content, as long as they are not aware of its unlawful nature or have not facilitated its transmission. However, this protection is revoked if the intermediary is found to be complicit in unlawful acts or fails to remove harmful content after being notified by the government or a court order.

The IT Rules, 2021 amended in 2022, further specify the due diligence required of intermediaries. Rule 3(1) mandates that intermediaries provide clear information about their rules and policies and take reasonable steps to prevent the publication of illegal content, including obscene or defamatory material. They must act expeditiously to remove such content, within 36 hours if ordered by a court or notified by the government, or within 72 hours for specific content like sexually explicit materials. The grievance redressal mechanism has been strengthened, with intermediaries required to acknowledge complaints within 24 hours and resolve them within 15 days, or within 72 hours for specific cases.

Failure to comply with these guidelines can result in significant penalties. Rule 7 specifies that intermediaries that fail to adhere to the IT Rules lose their safe harbour protection, exposing them to legal action under both the IT Act and the Indian Penal Code. This legal framework underscores the accountability of intermediaries in ensuring the swift and effective removal of illegal content, while also providing a clear process for user complaints and governmental oversight.

The role of intermediaries in regulating online content, especially in handling NCII, is critical. The IT Act and IT Rules define intermediaries broadly to include ISPs, websites hosting third-party content, social media platforms, and search engines. Different types of intermediaries have varying obligations based on their function. ISPs provide internet connectivity and cannot monitor or remove unlawful content unless directed by a government or court order. Websites hosting third-party content can remove harmful material at its source, while social media platforms have heightened obligations to detect and remove such content.

Search engines, which index web pages to help users find content, are distinct because they do not host content. They cannot remove unlawful content from websites directly, but they can de-index URLs, effectively making such content harder to locate. As intermediaries, search engines must comply with Rule 3 of the IT Rules, which requires due diligence to prevent the display or transmission of unlawful content. This includes removing NCII or content violating privacy within 36 hours upon receiving a court order or government notification, or within 72 hours if reported by users.

However, the protections under section 79 (safe harbour) for intermediaries are not absolute. Intermediaries, including search engines, must meet their

obligations to maintain this protection from liability. Failure to do so can result in the loss of safe harbour protection, which would expose them to legal consequences for hosting third-party content.

Saurabh Kirpal, the *amicus curiae*, submitted a short note emphasizing the legal obligations of intermediaries to remove unlawful content, particularly NCII. His submissions included the following points:

i. Broad Obligation to Remove Content: S.79(3)(b) of the IT Act mandates intermediaries to remove not just specific URLs but all offending content once it is deemed unlawful, as per judicial orders. This ensures intermediaries fulfill their legal duties to prevent unlawful content from remaining on their platforms.

ii. Rule 3 of IT Rules: This rule obligates intermediaries to remove unlawful content, including material that infringes privacy or is harmful, within 36 hours of receiving actual knowledge of it through a court order or government notification, or within 24 hours when notified through a grievance mechanism.

iii. Grievance Redressal: The case differs from *Shreya Singhal v. Union of* India[53]in that the Court had already ruled on the unlawfulness of the content, making the grievance redressal mechanism pivotal for swift action.

iv. Technology for Removal: Kirpal highlighted that large companies like Google and YouTube possess technological tools like Content ID and AI, which can be repurposed to detect and remove unlawful content, including NCII.

v. Global Reach of Intermediaries: He argued that content removal must be global in scope to be truly effective, citing previous court orders enforcing global content removal.

vi. Search Engine Policies: Google uses keyword search filters and continuously updates its algorithms to block harmful content, such as CSAM, and these tools could be adapted to tackle NCII.

In conclusion, intermediaries must leverage their technological resources to swiftly and comprehensively remove unlawful content, ensuring compliance with Indian law and protecting user privacy and safety.

In the case of *Sabu Mathew George* v. *Union of India,*[54] the Supreme Court introduced the "auto-block" mechanism, directing intermediaries like Google and other search engines to proactively block search results containing prohibited content. This measure is triggered when specific keywords are searched, displaying a warning before blocking the content. The court emphasized that intermediaries must act quickly when notified about prohibited content, implementing internal procedures for this purpose.

Google, represented by Senior Counsel Arvind Nigam, argued that its search engine does not control or host content, merely indexing third-party websites. Google contended that it should only act upon receiving court orders or

53 *Supra* note 18.

54 (2018) 3SCC 229.

notifications from authorities, as proactive content policing would undermine its safe harbour protection under section 79 of the IT Act. Google highlighted its existing mechanisms for content removal, such as user reporting tools for flagging non-consensual explicit images, but argued that proactive monitoring could infringe upon free speech and privacy rights.

Microsoft, represented by Jayant Mehta, similarly highlighted that Bing does not have the technology to automatically detect or remove NCII, removing such content only upon receiving notice from affected individuals or relevant parties. He noted that while technologies for image scanning exist, they are still under development with industry collaboration.The court acknowledged the difficulty in managing the spread of harmful content online but stressed the importance of intermediaries fulfilling their duties to prevent unlawful content from circulating. It balanced the need to protect privacy and user safety with the protection of free speech.

The court issued several recommendations for effective content removal processes, including the creation of a trusted third-party encrypted platform to streamline removals and multilingual support for accessibility. It emphasized privacy protection, transparency, and the development of a status tracker for the Online Cybercrime Reporting Portal.

The case reinforced the need for intermediaries to take proactive steps in ensuring the swift removal of harmful content, balancing privacy, free expression, and public safety. The court directed further action if necessary, ensuring compliance with the IT Act and the IT Rules.

VI COMPUTER RELATED OFFENCES: TEMPERING WITH COMPUTER SOURCE DOCUMENTS/CODE AND HACKING

Over the past decade, the rise of technology and electronic commerce has led to a surge in cybercrimes and data related offences in India.The Indian judiciary has been playing a proactive role in addressing computer-related offences, contributing to the development of cyber law jurisprudence in the country.

The petition in *SwapnilBhatt* v. *Central Bureau of Investigation*[55] concerns a dispute involving a company, initially named A.U. Commodities Pvt. Ltd. and later Moneyhouse Commodities Pvt. Ltd., which was authorised for future trading by the Multi Commodity Exchange (MCX). The company was founded by petitioner Amit Soni, his brother Anurag Soni, and complainant Lokesh Sharma. Over time, multiple individuals, including Amit, Anurag, Hemant Soni, and others, assumed roles in the company, with Hemant Soni managing its operations from 2011.

In 2013, several complainants filed a complaint, alleging that Amit and Anurag Soni had induced them to invest in commodities trading using a software called Meta Trade-5 (MT-5). The complainants claimed they were provided with login IDs and passwords to trade on a fake commodity exchange operated by the petitioners, resulting in financial losses. Further investigations revealed that the

55 MISC. CRIMINAL CASE No. 33356 of 2022 (Decided on Mar. 14, 2023).

MCX platform was not involved, and the software was allegedly used for unauthorised trading. The investigation, led by the CID and later the CBI, uncovered illegal trading practices and financial discrepancies, including the operation of a parallel exchange. It was found that the accused had invested large sums in unauthorised trading activities, leading to substantial profits, which were concealed.

Petitioners, particularly Amit and Anurag Soni, argued that the complaints stem from personal conflicts with family members and disputes over the company's management. They claimed that financial mismanagement by the complainants led to sour relations, and the complaints filed against them are retaliatory. The charge sheet accuses the petitioners of various offences under the IPC, the IT Act, and other related laws. The petitioners challenge these allegations and the charge sheet on the grounds of personal grievances and conflicts within the family and business.The petitioners sought to quash FIRs and subsequent proceedings, citing a lack of credible evidence. Investigating agencies failed to establish a direct connection between the petitioners and the alleged activities, as they could not trace IP addresses, verify the creation or access of disputed data, or link email accounts and server data to the petitioners' devices.

The CBI relied on the CFSL report and FMC expert opinion, alleging 'Dabba Trading' through the petitioners' company, Moneyhouse Commodities. However, the company's legitimate forward trading activities since 2010, with a turnover of 22,635.37 crores, overshadow the prosecution's claim of unauthorised trading worth 72 crores over just 41 days. Charges under IPC s. 467, 468, 471, and 474 lack evidence of forgery or fabrication. Allegations of misappropriation (s. 409 IPC) are unsupported, as there is no proof of financial transactions involving the petitioners. This petition under section 482 of Cr.PC. challenges the jurisdiction and validity of FIR registered by CBI. The petitioners are accused of violations under various laws, including the IPC, IT Act, FCRA, and SCRA, based on allegations of unauthorised trading outside the MCX platform using MetaTrader-5 software.

The investigation revealed significant gaps, including the absence of evidence linking the petitioners to the alleged devices or data. Complainants failed to produce mobile devices, SIM details, or server data, rendering the key evidence unavailable. No proof established that the petitioners used MetaTrader-5 software for illegal activities. The cited provisions of FCRA and SCRA were found irrelevant due to a lack of allegations or evidence concerning securities or regulated contracts.Sections of the IT Act cited in the chargesheet, such as 43(b), 65, and 66D, also lacked corroborative evidence of unauthorised access, data tampering, or fraudulent electronic transactions by the petitioners. In the absence of credible and substantive proof, the case fails to establish culpability, making the charges unsustainable and the prosecution an abuse of the legal process.Given the absence of substantive and corroborative evidence, the charges appear unsubstantiated, making the prosecution an abuse of legal process.

The case revolve around allegations that the petitioners were running an illegal parallel trading exchange using Meta Trader 5 (MT-5) software, resulting in losses for the complainants. However, the investigation revealed several

discrepancies and procedural lapses that undermined the prosecution's case. The data retrieved from the allegedly seized server did not contain the complainants' names, and the seizure process itself was marred by irregularities. The specifications of the seized server did not match the invoiced records, suggesting possible tampering or planting of evidence. Furthermore, the DVD analysed by the Forward Market Commission (FMC), which formed the basis of the report alleging illegal activities, lacked certification under s.65B of the Evidence Act, rendering it inadmissible.

The FMC's opinion indicated illegal "Dabba Trading" worth 72 crores outside the MCX platform. However, no evidence linked the petitioners to the server, devices, or the MT-5 software allegedly used for the illegal transactions. Investigations revealed that MT-5 was neither purchased nor licensed by the petitioners or any Indian entity, and attempts to connect the petitioners with Cyber Futuristics Pvt. Ltd. or Skytel Services, the purported leaseholder of the server, were unsuccessful. The complainants claimed they paid 2 lakhs each in cash to the petitioners without receipts or records, further casting doubt on the veracity of their allegations, especially given their identical statements and lack of credible evidence.

Legally, the charges under various sections of the IT Act were unsupported by prima facie evidence. Additionally, the CBI's prolonged investigation over seven years yielded no substantial fresh evidence and left the case in a state of indefinite suspension. The court found the data relied upon by the prosecution unreliable due to procedural violations and questioned the investigators' conduct, labeling the prosecution as biased, malicious, and an abuse of the legal process. Consequently, the court quashed the proceedings to secure justice and prevent further misuse of the law.

In *Harnish Surendra Chadderwala* v. *State of Maharashtra*[56] the applicant faced allegations of defrauding Valiant Pacific LLC Ltd. of Rs. 80 Crores during their employment and of accessing the company's computer system without authorisation to destroy data. APP submitted that there is material to show that the applicant was using the BlackBerry mobile handset which was employed to remotely access the computer system of Valiant. The prosecution charged the applicant under both the Indian Penal Code (IPC) section 379, 381, 409, and 420, and the Information Technology (IT) Act s. 43, 65, 75, 66C, and 66E.

The applicant argued that dual prosecution under both statutes violates protection against double jeopardy, citing the *GaganSharma*[57] case where the High Court of Bombay held that when the IT Act provides a specialised framework for addressing offences like unauthorised computer access and data destruction (section 43 and 66), invoking IPC provisions for the same conduct is unwarranted. Hence, this principle should apply to their case, making the IPC charges unsustainable, the applicant contended.

56 2023:BHC-AS:33254 (decided on Nov. 1, 2023).

57 *Gagan Harsh Sharma v. State of Maharashtra* (2018) SCC OnLine Bom 17705.

The court however, distinguished the applicant's case from *Gagan Sharma,*[58] noting additional allegations beyond IT Act violations. The applicant was accused of criminal breach of trust and falsification of records to siphon funds, which involve distinct elements of fraud not covered solely by the IT Act. Referring to Supreme Court ruling, such as *Ramchandra Rabidas,*[59] which upheld simultaneous prosecutions under overlapping statutes if the offences operate in independent legal spheres. Though the Supreme Court in another case of *Aman Mittal*[60] refrained from conclusively ruling on the validity of dual prosecutions under the IPC and IT Act, leaving it to be decided on a case-by-case basis.Thus, the court held that the allegations against the applicant justified prosecution under both the IT Act and IPC, as the offences had overlapping but distinct elements.

The applicant served Valiant Pacific LLC from 2003 until tendering resignation on December 1, 2018, which was accepted on January 8, 2019. Allegations include falsifying accounts worth Rs. 80 Crores over 10 years and remotely destroying company data on January 13, 2019. However, significant delays in reporting and investigation weaken the case. Valiant allegedly suspected discrepancies in inter-company balances in June 2018 and requested a reconciliation statement, which the applicant did not furnish before resigning. Despite these suspicions, Valiant accepted the resignation without protest after a 39-day interval, providing ample time to examine the applicant's affairs.

The FIR was lodged only on August 9, 2022, despite the alleged data destruction being discovered on January 15, 2019. Forensic audits conducted in December 2019 and April 2021 indicated remote access to the desktop by an unknown user, possibly the applicant, but with a rider that local assistance was necessary. No effort was made to identify potential accomplices, as recommended by auditors.

The court observed that the FIR lacks specifics about the alleged fraud and falsification of accounts. While it is understood that an FIR need not be an encyclopaedia, the long delay in lodging it and the subsequent reliance on vague forensic findings undermine its credibility. The forensic reports only tentatively suggest the applicant's involvement, and no conclusive evidence of his participation has been presented.

The court was not convinced as to the sufficiency of charge of criminal breach of trust under section 409 IPC hence granted bail to the applicant considering that he has cooperated with the investigation. Since the applicant is not expected to flee, having roots in society, or tampering with evidence the relevant records being in the custody of Valiant.

In another case of *Sumit Singha* v. *The State of Assam,*[61] the petitioner has been charged under several sections of the Information Technology Act, 2000 (IT

58 *Ibid.*

59 *State of Arunachal Pradesh* v. *Ramchandra Rabidas alias Ratan Rabidas* (2019) 10 SCC 75.

60 *State of Uttar Pradesh* v. *Aman Mittal* (2019) 19 SCC 740.

61 GAHC010266332023(Decided on Nov. 30, 2023).

Act), including section 65, 66, 66B, 66C, and 66D, which pertain to cybercrimes such as hacking, identity theft, and the fraudulent use of digital information. The case involves an alleged scam wherein fake call centers were set up in Guwahati to cheat Indian and foreign nationals by posing as tech support staff. The FIR accuses the petitioner and others of using forged documents and identities to operate the scam and of manipulating electronic records to siphon significant amounts of money.

The sections of the IPC in *parimateria* to the sections of the IT Act, under which the petitioner is booked will be governed solely by the IT Act and all the offences under which the petitioner is booked under the IT Act are bailable offences.The petitioner argues that s. 81 of the IT Act, which has an overriding effect, takes precedence over any conflicting provisions of the IPC. Therefore, the charges under the IPC that are similar to those under the IT Act should be governed by the IT Act, which makes the offences bailable. The petitioner further contends that no offence under s. 467 IPC (forgery of valuable documents) should apply at this stage, as it has been incorporated with *mala fide* intentions. While the court acknowledges the serious nature of the charges, it noted that cybercrime can be committed from remote locations, and the petitioner has pledged to abide by bail conditions. The court therefore granted bail, despite the ongoing investigation into the applicability of section 467 IPC, under strict conditions, including non-interference with the investigation, non-repetition of the offence, and no foreign travel without prior permission. The matter remains unresolved till the final adjudication in the case.

VII CONCLUSION

The year 2023 marked a significant turning point for cyber law in India, primarily due to the enactment of the Digital Personal Data Protection Act, 2023 (DPDPA). The DPDPA establishes a comprehensive framework for the protection of personal data in India.It emphasizes obtaining explicit consent from individuals before processing their personal data and restricts data collection to what is necessary for specified purposes.It imposes obligations on entities handling personal data, including implementing reasonable security safeguards. DPDPA grants individuals rights such as the right to access, correction, and erasure of their personal data. It creates an independent regulatory body to oversee enforcement and address grievances. This includes discussions around self-regulation by the industry, age verification mechanisms, and measures to prevent addiction and financial fraud. The DPDPA is expected to have a significant impact on how businesses operate in India, requiring them to adopt robust data protection practices. It also empowers individuals with greater control over their personal data.

While 2023 was dominated by the DPDPA in terms of new legislation, it's crucial to acknowledge the broader context of criminal law reforms that will significantly impact how cybercrimes are handled in India. Three key legislative acts-Bharatiya Nyaya Sanhita (BNS),Bharatiya Nagarik Suraksha Sanhita(BNSS)

and Bharatiya Sakshya Adhiniyam (BSA) passed in 2023 are set to overhaul the criminal justice system, and they have important implications for cyber law. It is aimed at providing more comprehensive definitions of cybercrimes and enhancing penalties; enabling law enforcement to effectively investigate and prosecute cybercrimes using modern technology and ensuring that digital evidence is reliably admitted in court.

YEAR 2023 witnessed significant developments in Indian cyber law, marked by a dynamic interplay between legislative actions and judicial interpretations. While the Digital Personal Data Protection Act, 2023, dominated the legislative landscape, establishing a new paradigm for data protection, the courts actively shaped the application and scope of existing and emerging legal frameworks. Landmark judgments addressed crucial issues like the Right to Be Forgotten, intermediary liability, online content blocking, and cyber obscenity.

Cases like *SK* v. *Union of India*, and those concerning Aadhaar disclosure reinforced the judiciary's commitment to safeguarding individual privacy in the digital realm. The *X Corp (Twitter)* case, however, highlighted the potential for broad interpretations of section 69A of the IT Act to regulate online expression, raising some concerns about the balance between national security and freedom of speech.

The interpretation of intermediary liability under section 79 of the IT Act saw further refinement through cases like *Suki Sivam* v. *YouTube* and *Google LLC* v. *DRS Logistics*, clarifying the "actual knowledge" standard and the limits of safe harbor protection. Cases involving NCII, such as *X* v. *Union of India*, underscored the urgent need for swift action by intermediaries to remove harmful content. Finally, cases like *Harnish Surendra Chadderwala* and *Sumit Singha* illustrated the complexities of prosecuting cybercrimes under the overlapping provisions of the IPC and IT Act.

Collectively, these developments in 2023 demonstrate the ongoing efforts to create a robust and effective legal framework for addressing the challenges of cybercrime and protecting digital rights in India. The emphasis on data protection, the nuanced approach to intermediary liability, and the continuous struggle to balance security with freedom of expression will continue to shape the future of cyber law in the country.