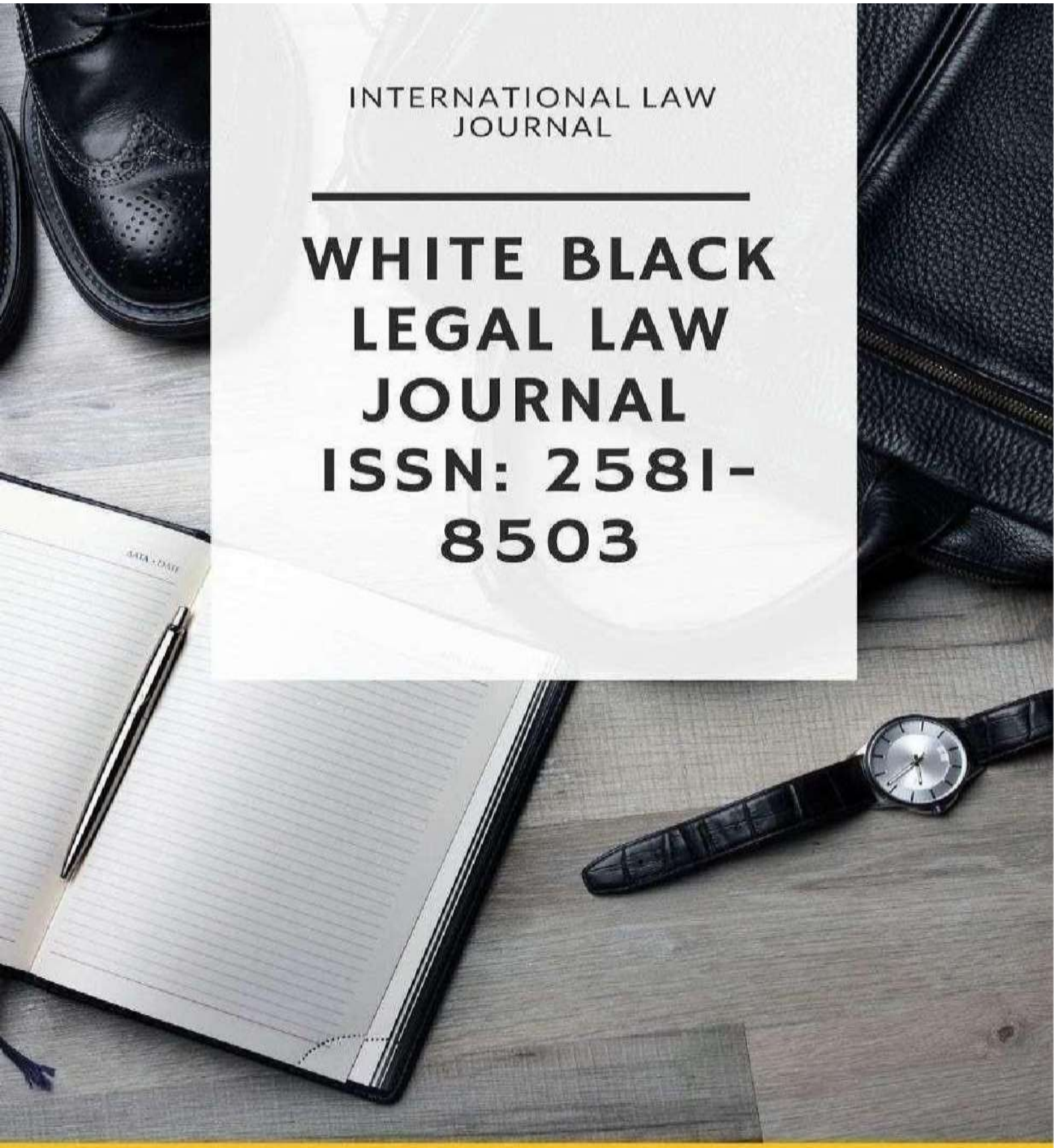

INTERNATIONAL LAW JOURNAL

WHITE BLACK LEGAL LAW JOURNAL

ISSN: 2581-8503

Peer - Reviewed & Refereed Journal

The Law Journal strives to provide a platform for discussion of International as well as National Developments in the Field of Law.

DISCLAIMER

ABOUT WHITE BLACK LEGAL

White Black Legal – The Law Journal is an open-access, peer-reviewed, and refereed legal journal established to provide a scholarly platform for the examination and discussion of contemporary legal issues. The journal is dedicated to encouraging rigorous legal research, critical analysis, and informed academic discourse across diverse fields of law.

The journal invites contributions from law students, researchers, academicians, legal practitioners, and policy scholars. By facilitating engagement between emerging scholars and experienced legal professionals, *White Black Legal* seeks to bridge theoretical legal research with practical, institutional, and societal perspectives.

In a rapidly evolving social, economic, and technological environment, the journal endeavours to examine the changing role of law and its impact on governance, justice systems, and society. *White Black Legal* remains committed to academic integrity, ethical research practices, and the dissemination of accessible legal scholarship to a global readership.

AIM & SCOPE

The aim of *White Black Legal – The Law Journal* is to promote excellence in legal research and to provide a credible academic forum for the analysis, discussion, and advancement of contemporary legal issues. The journal encourages original, analytical, and well-researched contributions that add substantive value to legal scholarship.

The journal publishes scholarly works examining doctrinal, theoretical, empirical, and interdisciplinary perspectives of law. Submissions are welcomed from academicians, legal professionals, researchers, scholars, and students who demonstrate intellectual rigour, analytical clarity, and relevance to current legal and policy developments.

The scope of the journal includes, but is not limited to:

- Constitutional and Administrative Law
- Criminal Law and Criminal Justice
- Corporate, Commercial, and Business Laws
- Intellectual Property and Technology Law
- International Law and Human Rights
- Environmental and Sustainable Development Law
- Cyber Law, Artificial Intelligence, and Emerging Technologies
- Family Law, Labour Law, and Social Justice Studies

The journal accepts original research articles, case comments, legislative and policy analyses, book reviews, and interdisciplinary studies addressing legal issues at national and international levels. All submissions are subject to a rigorous double-blind peer-review process to ensure academic quality, originality, and relevance.

Through its publications, *White Black Legal – The Law Journal* seeks to foster critical legal thinking and contribute to the development of law as an instrument of justice, governance, and social progress, while expressly disclaiming responsibility for the application or misuse of published content.

HARASSMENT & STALKING THROUGH ONLINE: DOES CURRENT CRIMINAL LAWS IS SUFFICIENT ENOUGH TO PROVIDE LEGAL JUSTICE?

Author name : Lavanya Damodaran
Designation : Research Scholar
Qualification : B.A.L.L.B (Hons)., L.L.M., NET

Co-Author name : Aruna Devi
Designation : Research Scholar
Qualification : B.C.A.L.L.B (Hons)., L.L.M., NET

Co-Author name : Alex K
Designation : Research Scholar
Qualification : B.A, L.L.B, (Hons)., L L.M.

ABSTRACT

The quick unexpected growth of technology which made it easy to interact with everyone around the world. It also gave birth to the new forms of criminal activity i.e., cyberbullying, cyberstalking, abusing other people through online. Such crimes include psychological threats, intimidation, and continuous monitoring through digital means. So these pose a serious risk to personal freedom, privacy, and mental health. In India, provisions from the (IPC) now BNS, 2023, & IT Act, 2000 and interpretation of the court that expand the scope of fundamental rights which is guaranteed under the art 21 of the constitution are relied for legal response. This paper analyse whether existing criminal laws are enough to face the challenges caused by cyberstalking and online harassment. Laws like section 78 of BNS and section 66E and 67 of the IT Act are analysed which address the privacy violation and obscene content. While these laws provide a basic framework but definition, narrow scope, jurisdiction issue, delay in the procedure & limits their effectiveness. The study also highlights the challenges in enforcement including lack of digital knowledge among law enforcement difficulties in gathering the evidences cross border jurisdiction issues and under reporting due to social stigma. Judicial pronouncement like Shreya Singhal vs U.O.I have significantly impacted the legal environment

in balancing freedom of speech with regulation. The paper concludes that while current law provide certain remedies they fall short in addressing the complex nature of the cyber harassment. It highlights the need for legislative reform, which specifically dedicated only for cybercrime unit, victim focused solution and increased awareness initiative.

(Keywords: Crime, Cyber, Digital, Online Harassment & Harm)

INTRODUCTION:

The growth of internet and the arise of social media have totally converted the nature of communication which enables individuals to interact with everyone around the globe. Nonetheless, this technology conversion has delivered some new forms of crimes such as Cyberstalking, Cyberbullying, Phishing and Online harassment. Comparing to traditional crimes, these crimes have no territorial confinement as they let the wrongdoers to attack their victims secretly and continuously. The act of stalking someone through electronic means of communication constitutes cyberstalking and creates severe psychological problems for victims. Some examples of online harassment include sending threatening messages, trolling, and doxxing., sharing private data without consent. These actions violate the fundamental right to privacy, which is recognized in K.S. Puttaswamy vs U.O.I[1], where the Supreme Court has confirmed that privacy is a constitutional right under Art 21. Despite of the increasing occurrence of such crimes, question arises like how the Indian legal system can handle them effectively.

LEGAL FRAMEWORK UNDER BNS AND IT ACT:

1) Bharatiya Nyaya Sanhita Act, 2023

Earlier, IPC dealt all criminal offence now it has been repealed by BNS is not originally designed to deal with digital offenses, but it addresses several forms of online harassment and abuses.

Section 78[2] of the BNS deals with "Stalking" any man who tries to interact with a woman through repeated text or calls or following in person even after clear disinterest shown shall be punished with imprisonment up to 3 years(1st conviction) in certain cases 5 years (subsequent conviction) and including fine.

[1] Justice K.S. Puttaswamy v. Union of India (2018) AIR 2017 S.C 4161 (India).
[2] The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, Section 78.

Section 79[3] of the BNS states that any act which is abusive or sexually explicit or derogatory messages directed at a woman which insult the modesty of a woman is criminalised in the act and shall punished with imprisonment up to 3 years and also with fine.

Section 356[4] of the BNS deals with "Defamation" any person with the intention to destroy someone's reputation speculate the fake news either online or through gestures amounts to criminal defamation and this offence shall be punished with 2 years' imprisonment or community service. This provisions collectively provide a legal response to Cyber harassment, there applicability in digital environment depends on judicial interpretation. This provisions were framed in pre-digital era and they do not exclusively captures the online behaviour complexities.

2. Information Technology Act, 2000

The IT Act, 2000 acts as the primary legislative framework that governs the cyber offenses in India and it plays an important role in addressing the online harassment and misuse of a digital platform.

Section 66E[5] provides that whoever transfer or publish the private (images or videos) or share personal data of someone without consent of such person will amounts to violation of privacy under this section. It shall be punished with 3 years of imprisonment or fine up to 2 lakhs or with both.

Section 67[6] deals with the punishment for circulating or transferring of obscene material through electronics form such activity are considered as harmful in cyber space. The punishment for this offence shall be imprisonment up to 3 years and 5 years (Subsequent conviction), including fine up to 10 lakhs.

Section 67A & 67B[7] these two sections deals with transferring of sexually exclusive material and child sexual abuse materials are more worsened form of online sexual content. Both of these offence amount to the punishment. And the punishment can be imposed up to 5 years of imprisonment and 10 years (Subsequent conviction) and fine up to 10 lakhs. Despite, all this provision the framework still does not comprehensively addresses the issue of cyber stalking and other form of evolving Cyber harassment which leaves certain gap in the regulatory scope.[8]

[3] The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, Section 79.
[4] The Bharatiya Nyaya Sanhita, 2023, No. 45, Acts of Parliament, Section 356.
[5] Information Technology Act, 2000, No.21, Act of parliament, section 66E.
[6] Information Technology Act, 2000, No.21, Act of parliament, sec 67.
[7] Information Technology Act, 2000, No.21, Act of parliament, sec 67A & 67B.
[8] Shreya Singhal v. Union of India, (2015) 5 S.C.C 1 (India).

JUDICIAL INTERPRETATION AND EXPANDING SCOPE:

The judiciary have played an important role in expanding the interpretation and the application of the cyber law in response to the evolving technological challenges. The court tries to protect free speech while allowing necessary regulation of online activities. The court have balanced the constitutional freedom with regulatory needs. The SC struck down the vague provision relating to the online communication which emphasized the need to protect right to free speech and also ensuring those restriction meets constitutional standard[9]. The court to strengthen the legal foundation for addressing the digital surveillance and data misuse has recognised the privacy as a fundamental rights[10]. Even at the earlier phase of development of cyber Law the court acknowledged instance of online harassment like through emails, thereby laying foundation for recognizing cyber stalking and digital abuse[11]. These judicial pronouncement shows the adaptability in interpreting the existing legal frameworks and also highlights the limitation of legislative drafting to align with the change in technology.

CRITICAL TO CHECK ADEQUACY OF EXISTING LAWS?

1. **Absence of specific legislation**

   There is no particular framework which exclusively deals with the cyberstalking or cyberbullying in Indian law. BNS and IT act are relied but these law not originally enacted to address these issues so the evolving nature of online abuse is not adequately covered.

2. **Gender specific limitation**

   Section 78 of the BNS is limited to women. Male and non-binary victims are excluded which creates a significant gap. Such gender specific provisions undermine the principle of equality before law and ignores the fact that irrespective of the gender cybercrime can affect every individual.

3. **Unclear definition**

   The term Harassment and stalking is not defined under in Indian legal framework. So this uncertainty leads to unstable enforcement which makes it difficulty to interpret the statue then it decreases the efficient of the remedies which is available to the victims.

4. **Inadequate punishments**

   In repeated severe harassment cases, penalty in IT Act, 2000 is insufficient, it does not

[9]Shreya Singhal v. Union of India, (2015) 5 S.C.C 1 (India).
[10] Justice K.S. Puttaswamy v. Union of India (2018) AIR 2017 S.C 4161 (India).
[11] SMC Pneumatics (India) Pvt. Ltd. V. Jogesh Kwatra, 2004 (29) P.T.C 492 (India)

adequately address the psychological and emotional harm caused to the victim.

5. **Overlap and confusion**

Multiple provisions under BNS and IT Act causes confusion in their application which makes law enforcement authorities face difficulties in deciding appropriate charges which affects the effective enforcement and delay in justice.

ENFORCEMENT CHALLENGES:

1. **Lack of technical expertise**

The crucial challenge in implementing cyber laws is that there is lack of competence among the enforcement agencies. VPN, fake accounts, and encrypted platforms are involved in cyber stalking cases, which require specialized digital investigation skills. Many police officers especially at the local level or not trained adequately in cyber forensic or for platform based investigation. Relying on traditional method which are ineffective in digital context causes delays and error in handling the evidence which in term weakens prosecution outcomes. The difficulty in fixing liability in online platforms due to these investigative limitation are recognised by courts [12].

2. **Issue in evidence collection**

In cybercrime cases, it is difficult to collect digital evidence and preserve them because they are highly volatile and it can be easily deleted, altered, or encrypted. Such data, as chat records, IP logs, and metadata may be lost if they are not secured quickly. The cross-border storage of data and for maintaining chain of custody lacks uniform procedures and create evidentiary gaps. The Court mandated strict compliance with Section 63(4)(c) for electronic evidence, as if procedures are not followed it makes prosecution difficult[13] ,Which is reaffirmed in later judgements[14].

3. **Jurisdictional Challenges**

In addition, cybercrimes tend to have an international nature. The criminal could conduct the crime from a certain location while being far away from where the victim is situated. This brings out the issue of whose jurisdiction it falls under. Differences in domestic laws, data protection framework, and cooperation level between these jurisdictions complicates the enforcement, which allow the offenders to escape through these legal gaps. Courts have recognized the cross-border nature of the digital

[12] Avnish Bajaj v. State (NCT of Delhi), 2005 (3) Comp LJ 364 (India)
[13] Anvar P.V. v. P.K. Basheer, (2014) 10 S.C.C 473 (India).
[14] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 S.C.C 1 (India).

harassment and also the enforcement challenges[15].

4. **Under reporting**

   Cybercrime cases involving women and marginalized groups often face an issue of underreporting. Victims avoid reporting due to various reasons, like lack of awareness of the legal remedies available to them, fear of retaliation, and doubts about the effectiveness of the justice system. As many cases remains unreported courts have recognised these psychological impact of such offences[16].

5. **Delayed Adjudication**

   Enforcement of the cyber law is weakened by the procedural delay in the investigation and adjudication. In cyber cases, such delay affects the effectiveness of timely intervention and worsen harm faced by victims. The Courts have attempted to prevent injustice caused by procedural delay by relaxing evidentiary requirement[17].

CONCLUSION:

In the present world of internet and social media, cyberstalking and online harassment is an undeniable challenge that require urgent attention. The anonymity and global nature of the cyber space have enabled the abuser to commit serious offences that would cause considerable harm on the dignity mental health and autonomy of the victim. although several provisions in IPC and IT act of 2000 offers a foundation for prosecuting offenders but these framework lack coherence and relevance in lights of the current trend in online conduct. The court through judicial activism addressed certain identified loop holes through interpretation of basic rights and have established the constitutional guarantee of privacy and cautioned against the restrictive legislation concerning freedom of expression. Judicial innovation alone cannot solve the issue, court may interpret existing law but cannot provide me a holistic solution to emerging problems. A review in the present legal system shows several deficiencies. Problems like poor technical capabilities, evidence gathering, jurisdiction issues and delay in legal procedure affects the effective functioning of existing legislation and problem of under reporting worsen the matter. This calls for a change in existing legal frameworks and highlights the need to adopt a more preventive than reactive system. The efficient and comprehensive law against the cyber harassment has to be implemented. Further preventive steps to be taken to strengthen law enforcement agencies, develop technological capacity in forensics and ensure support to

[15] SMC Pneumatics (India) Pvt. Ltd. V. Jogesh Kwatra, 2004 (29) PTC 492 (India).
[16] Kalandi Charan Lenka v. State of Odisha, 2017 SCC OnLine Ori 570(India).
[17] Shafhi Mohammad v. State of Himachal Pradesh (2018) 2 S.C.C 801 (India).

victims. The awareness must be given to the people to prevent further offence or to get justice for the victim who suffered.