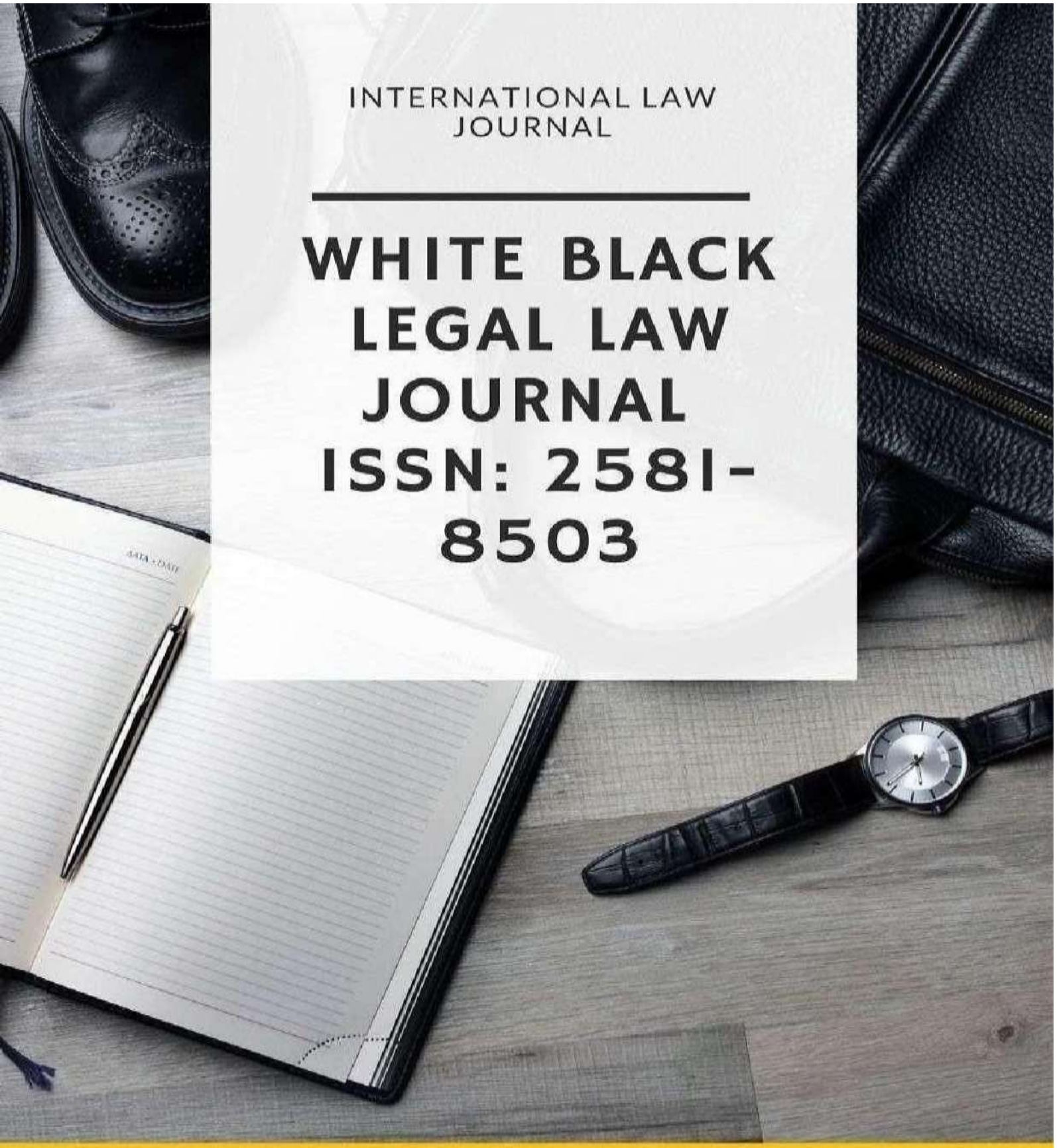

INTERNATIONAL LAW JOURNAL

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.

AI, CYBERSECURITY, AND THE EVOLVING LEGAL FRAMEWORK OF LIVE-IN RELATIONSHIPS IN INDIA: A SOCIO-LEGAL PERSPECTIVE

AUTHORED BY - MR. ANKUR GUPTA
Research Scholar
Department of Law, Shobhit University, Meerut

CO-AUTHOR - DR PARANTAP KUMAR DAS
Research Supervisor
Department of Law, Shobhit University, Meerut

Abstract

The rapid integration of artificial intelligence (AI) and digital technologies into everyday life has significantly transformed the nature of human relationships, including the emergence and normalization of live-in relationships in India. While the Indian legal system has gradually acknowledged live-in relationships through judicial interpretations, the intersection of such relationships with AI-driven platforms and cybersecurity concerns remains underexplored. This paper examines how digital ecosystems—particularly AI-enabled dating applications, social media platforms, and data-driven surveillance—shape the formation, maintenance, and dissolution of live-in relationships.

It further analyses the legal challenges arising from issues such as digital privacy, data protection, cyber harassment, and the admissibility of electronic evidence in disputes involving live-in partners. The study critically evaluates existing legal frameworks, including the Information Technology Act, 2000, the Indian Evidence Act, 1872, and the Protection of Women from Domestic Violence Act, 2005, alongside constitutional protections such as the right to privacy recognized in Justice K.S. Puttaswamy v. Union of India.

Adopting a socio-legal methodology, the paper highlights gaps in legal protection, particularly concerning digital abuse, algorithmic bias, and the lack of regulatory oversight of AI-driven relationship platforms. It argues for a more nuanced legal approach that integrates technological realities with evolving social norms.

The paper concludes by proposing reforms aimed at strengthening cybersecurity frameworks, ensuring data protection, and expanding legal recognition and safeguards for individuals in

live-in relationships within India's digital future. These reforms are essential for achieving a balanced and sustainable legal ecosystem that protects individual autonomy, dignity, and rights in the age of AI.

Keywords

AI and Law; Live-in Relationships; Cybersecurity; Digital Privacy; Socio-Legal Study

1. Introduction

The growing integration of artificial intelligence (AI) and digital technologies into everyday life has fundamentally reshaped the nature of intimate relationships, including live-in relationships in India. Once examined primarily through sociological and cultural frameworks, such relationships are now increasingly influenced by digital communication platforms, algorithmic interactions, and data-driven environments. This technological shift has introduced new dimensions of vulnerability, particularly in relation to privacy, consent, and cybersecurity, thereby raising important legal concerns. While the Indian judiciary has gradually acknowledged live-in relationships within the ambit of the right to life and personal liberty under Article 21, the legal framework continues to evolve in response to emerging technological realities.[1]

The proliferation of AI-enabled systems and online platforms has heightened risks such as cyberstalking, data breaches, non-consensual surveillance, and digital abuse within intimate relationships. These concerns are especially significant in the context of live-in arrangements, which often lack formal legal recognition and structured safeguards. Existing legal instruments, including the Information Technology Act, 2000 and the Protection of Women from Domestic Violence Act, 2005, provide certain remedies; however, they do not comprehensively address the intersection of AI-driven harms and personal relationships.[2]

Moreover, the recognition of the right to privacy as a fundamental right by the Supreme Court has added a crucial constitutional dimension to the discourse on digital autonomy and informational self-determination.[3] In this context, the role of legal institutions becomes critical in ensuring effective access to justice and safeguarding individual rights. This paper seeks to examine the interplay between AI, cybersecurity, and the evolving legal status of live-in relationships in India, adopting a socio-legal perspective to highlight gaps, challenges, and the

[1] Indra Sarma v. V.K.V. Sarma
[2] Information Technology Act, 2000; Protection of Women from Domestic Violence Act, 2005
[3] Justice K.S. Puttaswamy (Retd.) v. Union of India

need for a more adaptive legal framework.

2. Conceptual Framework: Live-in Relationships in India

The concept of live-in relationships in India reflects a gradual shift from traditional marital norms toward more individualized forms of companionship. Although not expressly codified in statutory law, such relationships have received judicial recognition, particularly where they resemble the nature of marriage in terms of stability, duration, and shared domestic arrangements. The Supreme Court, in Indra Sarma v. V.K.V. Sarma, laid down indicative criteria to determine whether a live-in relationship qualifies for legal protection, emphasizing factors such as a shared household and social presentation as a couple.[4]

From a constitutional perspective, live-in relationships are anchored in the fundamental rights to life, liberty, and personal autonomy under Article 21. Judicial pronouncements have affirmed that consenting adults have the freedom to cohabit without societal or state interference, thereby recognizing such relationships as part of the broader right to choose one's partner.[5] This evolving jurisprudence reflects a shift from social morality to constitutional morality, enabling greater legal acceptance of non-marital unions.

However, the conceptual framework becomes more complex in the digital era, where AI-driven technologies and cybersecurity concerns intersect with intimate relationships. The increasing use of digital communication platforms exposes individuals in live-in arrangements to risks such as cyberstalking, data misuse, and unauthorized surveillance. While statutory protections under the Information Technology Act, 2000 provide a basic legal framework to address cyber offences, they do not specifically account for relational harms arising within live-in contexts.[6] Thus, the conceptual understanding of live-in relationships in India must expand beyond traditional socio-legal parameters to incorporate digital realities. A nuanced framework integrating constitutional protections, judicial interpretation, and technological safeguards is essential to ensure effective recognition and protection of such relationships in contemporary society.

3. AI and the Transformation of Intimate Relationships

Artificial Intelligence (AI) has significantly transformed the nature of intimate relationships by mediating how individuals communicate, interact, and form emotional bonds. In the Indian

[4] Indra Sarma v. V.K.V. Sarma
[5] Lata Singh v. State of U.P
[6] Information Technology Act, 2000

context, where live-in relationships are gradually gaining legal and social recognition, AI-driven technologies—such as dating algorithms, social media platforms, and virtual assistants—play an increasingly influential role in shaping relational dynamics. These technologies not only facilitate connection but also structure patterns of interaction through predictive analytics and behavioral profiling, often influencing partner selection and communication styles.[7]

The integration of AI into everyday life has also blurred the boundaries between private and public spheres, raising concerns about autonomy, consent, and informational privacy within intimate relationships. Algorithmic surveillance, data tracking, and digital monitoring can create asymmetries of power between partners, potentially leading to forms of control or abuse that are not easily addressed within traditional legal frameworks. In this regard, the recognition of the right to privacy as a fundamental right by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India assumes particular significance, as it establishes informational self-determination as a core constitutional value.[8]

Furthermore, AI-enabled platforms may inadvertently reinforce social biases and stereotypes, thereby affecting the autonomy of individuals in choosing partners and maintaining relationships. The absence of specific regulatory mechanisms addressing AI in the context of intimate relationships creates challenges for legal institutions in ensuring accountability and protection. Existing frameworks, including the Information Technology Act, 2000, primarily address cyber offences but do not adequately capture the nuanced implications of AI-mediated relational harms.[9]

Thus, AI is not merely a technological tool but a transformative force that reshapes intimacy itself. A comprehensive socio-legal approach is essential to address its implications and to ensure that evolving legal frameworks remain responsive to the complexities introduced by AI in live-in relationships.

4. Cybersecurity Challenges in Live-in Relationships

Cybersecurity concerns have emerged as a critical dimension of intimate relationships in the digital age, particularly within the context of live-in relationships in India. As partners increasingly rely on digital devices, social media platforms, and AI-enabled applications for communication and daily coordination, the risk of cyber threats within such relationships has

[7] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books, 2019)
[8] Justice K.S. Puttaswamy (Retd.) v. Union of India
[9] Information Technology Act, 2000

intensified. Unlike traditional marital frameworks, live-in relationships often lack clearly defined legal protections, making individuals—especially women—more vulnerable to technology-facilitated abuse such as cyberstalking, unauthorized access to personal data, and non-consensual sharing of intimate content.[10]

One of the key challenges lies in the misuse of digital surveillance tools, including spyware, location tracking applications, and password breaches, which can enable one partner to exert coercive control over the other. Such practices not only violate personal autonomy but also infringe upon the fundamental right to privacy recognized by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India.[11] The digital dimension of abuse complicates evidentiary processes and often discourages victims from seeking legal remedies due to stigma, lack of awareness, or institutional barriers.

While statutory provisions under the Information Technology Act, 2000 criminalize certain cyber offences such as hacking and identity theft, they do not adequately address the relational context in which such violations occur.[12] Similarly, the Protection of Women from Domestic Violence Act, 2005 extends protection to women in relationships "in the nature of marriage," yet its application to cyber abuse remains limited and underdeveloped in practice.[13]

The absence of a comprehensive legal framework that integrates cybersecurity with intimate partner protections highlights a significant gap in access to justice. Addressing these challenges requires not only legal reform but also greater institutional sensitivity, digital literacy, and robust enforcement mechanisms. A socio-legal approach that recognizes the intersection of technology, power, and vulnerability is essential to ensure effective protection for individuals in live-in relationships in an increasingly digitalized society.

The integration of digital technologies into personal relationships has introduced various cybersecurity risks, including:

4.1 Digital Surveillance

Digital surveillance has become a significant cybersecurity concern within live-in relationships, particularly as intimate partners increasingly share digital spaces and devices. The use of smartphones, social media accounts, and AI-enabled applications often facilitates constant connectivity; however, it also creates opportunities for intrusive monitoring. Practices

[10] Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press, 2014)
[11] Justice K.S. Puttaswamy (Retd.) v. Union of India
[12] Information Technology Act, 2000
[13] Protection of Women from Domestic Violence Act, 2005

such as unauthorized access to personal messages, installation of spyware, and real-time location tracking can enable one partner to exercise coercive control over the other. Such forms of surveillance, though subtle, may amount to violations of autonomy, dignity, and informational privacy.[14]

In the Indian legal context, these concerns must be examined in light of the fundamental right to privacy recognized by the Supreme Court in Justice K.S. Puttaswamy (Retd.) v. Union of India, which affirms the individual's right to control personal information and make intimate decisions free from unwarranted intrusion.[15] Despite this constitutional protection, enforcement remains challenging, particularly in live-in relationships where boundaries of consent are often blurred and evidentiary standards for digital abuse are difficult to meet.

Statutory remedies under the Information Technology Act, 2000 address offences such as hacking and data theft; however, they do not fully capture the relational context of digital surveillance within intimate partnerships.[16] Consequently, there is a pressing need to develop a more nuanced legal framework that recognizes technology-facilitated abuse as a form of domestic harm. Strengthening institutional mechanisms and promoting digital awareness are essential to ensure effective protection and access to justice in such cases.

4.2 Cyber Harassment and Abuse

Cyber harassment and abuse have become pressing concerns within live-in relationships as digital communication increasingly mediates intimate interactions. Partners may engage in online harassment through repeated messaging, threats, doxxing, or the non-consensual dissemination of private images, often exploiting emotional vulnerabilities and the absence of formal legal safeguards in such relationships.[17] These acts not only cause psychological harm but also undermine personal dignity and autonomy, particularly affecting women in live-in arrangements.

In India, such conduct may attract liability under provisions of the Information Technology Act, 2000 and relevant sections of the Indian Penal Code; however, these laws do not specifically address the relational context of cyber abuse.[18] The constitutional recognition of privacy and dignity in Justice K.S. Puttaswamy (Retd.) v. Union of India further underscores

[14] Evan Selinger & Woodrow Hartzog, "The Incoherent Justifications for Third-Party Doctrine," (2016) 100 *Minnesota Law Review* 289
[15] Justice K.S. Puttaswamy (Retd.) v. Union of India
[16] Information Technology Act, 2000
[17] Danielle Keats Citron, *Hate Crimes in Cyberspace* (Harvard University Press, 2014)
[18] Information Technology Act, 2000

the need to treat cyber harassment as a violation of fundamental rights.[19] Strengthening legal responses and institutional sensitivity is essential to ensure effective remedies for victims.

4.3 Data Breaches

Data breaches represent a growing cybersecurity risk within live-in relationships, where partners often share devices, passwords, and access to personal accounts. Such informal sharing, while rooted in trust, can lead to unauthorized disclosure of sensitive information when relationships deteriorate. Breaches may involve access to emails, financial data, private photographs, or social media accounts, potentially resulting in identity theft, reputational harm, or emotional distress.[20] The absence of clearly defined digital boundaries in live-in arrangements further complicates questions of consent and liability.

In the Indian context, offences relating to unauthorized access and data theft are addressed under the Information Technology Act, 2000, particularly provisions dealing with hacking and identity misuse.[21] However, these provisions do not sufficiently account for breaches occurring within intimate relationships where prior consent may be contested. The recognition of informational privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India highlights the need for stronger safeguards.[22] A more nuanced legal approach is necessary to address such relational data vulnerabilities. The Information Technology Act, 2000 provides legal remedies for certain cyber offenses, but it does not specifically address relational contexts.

5. Privacy and Constitutional Safeguards

Privacy has emerged as a foundational constitutional value shaping the legal recognition and protection of live-in relationships in India. In the absence of explicit statutory regulation governing such relationships, constitutional interpretation—particularly under Article 21—has played a decisive role in expanding the scope of individual autonomy, dignity, and decisional freedom. The Supreme Court, in Justice K.S. Puttaswamy (Retd.) v. Union of India, firmly established privacy as a fundamental right, encompassing both informational and decisional dimensions.[23] This judgment provides a crucial doctrinal basis for protecting intimate choices, including the right of consenting adults to cohabit outside marriage without state or societal interference.

[19] Justice K.S. Puttaswamy (Retd.) v. Union of India
[20] Daniel J. Solove, *Understanding Privacy* (Harvard University Press, 2008)
[21] Information Technology Act, 2000
[22] Justice K.S. Puttaswamy (Retd.) v. Union of India
[23] Justice K.S. Puttaswamy (Retd.) v. Union of India

Within live-in relationships, constitutional safeguards ensure that personal liberty is not curtailed by moral policing or social stigma. Judicial decisions such as Lata Singh v. State of U.P. have reinforced the principle that adults are free to choose their partners and live together, thereby affirming autonomy in personal relationships.[24] However, the expansion of digital technologies and AI-driven platforms has complicated the exercise of privacy rights, introducing new risks such as surveillance, data profiling, and unauthorized access to personal communications.

Although the Information Technology Act, 2000 provides a statutory framework to address certain cyber offences, it does not comprehensively safeguard privacy in the context of intimate relationships.[25] The recognition of privacy as a constitutional right thus demands stronger institutional mechanisms to ensure effective enforcement, particularly in cases involving technology-facilitated intrusion within live-in arrangements.

Furthermore, constitutional safeguards must be understood in conjunction with evolving socio-legal realities. The intersection of AI, cybersecurity, and intimate relationships necessitates a more dynamic interpretation of privacy that goes beyond traditional state-centric concerns and addresses private actor intrusions as well. Strengthening data protection norms, enhancing judicial sensitivity, and ensuring accessible remedies are essential to uphold constitutional guarantees in the digital age.

6. Digital Evidence and Legal Challenges

Digital evidence has become increasingly central to disputes arising out of live-in relationships in India, particularly with the growing use of AI-driven communication platforms, smartphones, and cloud-based storage systems. Messages, call logs, emails, social media interactions, and location data often serve as crucial proof in cases involving allegations of abuse, breach of trust, or domestic violence. However, the admissibility, authenticity, and integrity of such evidence raise significant legal challenges in the absence of clear procedural safeguards tailored to digitally mediated relationships.[26]

Under Indian law, electronic records are admissible subject to conditions laid down in Section 65B of the Indian Evidence Act, 1872, which requires proper certification for electronic evidence to be considered valid in court. Despite this statutory framework, courts frequently encounter difficulties in verifying the originality and chain of custody of digital data, especially

[24] Lata Singh v. State of U.P
[25] Information Technology Act, 2000
[26] Stephen Mason, *Electronic Evidence* (LexisNexis, 2017)

when devices are shared between partners in live-in arrangements.[27] The potential for manipulation, deletion, or fabrication of digital content further complicates evidentiary assessment.

In cases involving intimate relationships, these challenges are amplified by the blurred boundaries of consent and access. For instance, shared passwords or mutual device usage may create ambiguity regarding whether access to personal data constitutes authorization or intrusion. The Justice K.S. Puttaswamy (Retd.) v. Union of India judgment, which recognizes informational privacy as a fundamental right, underscores the need to balance evidentiary requirements with constitutional protections against unlawful surveillance and data misuse.[28]

Moreover, the Information Technology Act, 2000 provides a limited framework for addressing cyber offences, but it does not comprehensively regulate the collection and authentication of digital evidence in interpersonal disputes. This gap highlights the need for updated procedural rules and judicial guidelines that can address the complexities of AI-generated and digitally stored evidence.

Thus, the legal system must evolve to ensure that digital evidence is both reliable and constitutionally compliant, particularly in cases arising from live-in relationships where personal and technological boundaries are deeply intertwined. Strengthening forensic capabilities, ensuring procedural clarity, and enhancing judicial awareness are essential to achieving fairness and effective access to justice in the digital era.

7. Gendered Dimensions and Vulnerability

The intersection of AI, cybersecurity, and live-in relationships in India reveals a pronounced gendered dimension of vulnerability, where technological misuse disproportionately impacts women. In live-in arrangements, women often face heightened risks of cyber harassment, digital surveillance, non-consensual sharing of intimate content, and coercive control through technology. These vulnerabilities are amplified by socio-cultural factors such as stigma surrounding non-marital cohabitation, economic dependency, and unequal bargaining power within intimate relationships.[29]

AI-driven platforms and digital tools, while facilitating communication and autonomy, also enable subtle forms of gendered abuse. Predictive analytics, location tracking applications, and

[27] Indian Evidence Act, 1872, s. 65B
[28] Justice K.S. Puttaswamy (Retd.) v. Union of India
[29] Flavia Agnes, *Law and Gender Inequality: The Politics of Women's Rights in India* (Oxford University Press, 1999)

social media monitoring can be misused to regulate women's mobility and privacy, thereby reinforcing patriarchal patterns in a technologically mediated form. Such conduct raises serious concerns under constitutional guarantees of equality and dignity, particularly under Articles 14 and 21 of the Constitution of India.[30] The Supreme Court's recognition of privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India further strengthens the legal foundation for addressing gendered digital harms.

Despite existing legal provisions under the Protection of Women from Domestic Violence Act, 2005, protection mechanisms often fall short in addressing technology-facilitated abuse within live-in relationships, particularly due to evidentiary challenges and limited institutional awareness.[31] Similarly, the Information Technology Act, 2000 criminalizes certain cyber offences but does not explicitly account for gendered patterns of digital abuse in intimate partnerships.

The vulnerability of women in live-in relationships is further intensified by gaps in legal recognition and social acceptance, which may discourage reporting and reduce access to justice. Addressing these challenges requires a gender-sensitive legal framework that integrates cybersecurity protections with constitutional principles of equality, dignity, and autonomy. Strengthening enforcement mechanisms, improving digital literacy, and sensitizing law enforcement agencies are essential steps toward mitigating gendered risks in the evolving digital landscape.

8. Regulatory Gaps and Need for Reform

The rapid evolution of artificial intelligence and digital technologies has exposed significant regulatory gaps in the legal framework governing live-in relationships in India. While such relationships have gained limited judicial recognition under constitutional principles of personal liberty and dignity, there remains no comprehensive statutory framework specifically addressing their legal status, particularly in the context of cybersecurity and AI-driven harms. This gap becomes more pronounced as digital platforms increasingly mediate intimate relationships, creating new forms of vulnerability such as data exploitation, cyberstalking, and algorithmic surveillance.[32]

Existing legal provisions, including the Information Technology Act, 2000, primarily address conventional cyber offences such as hacking, identity theft, and unauthorized access to data.

[30] Justice K.S. Puttaswamy (Retd.) v. Union of India
[31] Protection of Women from Domestic Violence Act, 2005; Information Technology Act, 2000
[32] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books, 2019)

However, they do not adequately capture the relational and contextual dimensions of digital abuse within live-in partnerships. Similarly, while the Protection of Women from Domestic Violence Act, 2005 extends protection to relationships "in the nature of marriage," its application to technology-facilitated abuse remains limited and inconsistently interpreted in practice.[33]

Judicial recognition of privacy as a fundamental right in Justice K.S. Puttaswamy (Retd.) v. Union of India has laid an important constitutional foundation for protecting individual autonomy in the digital age.[34] However, the absence of specific legislative provisions addressing AI-mediated harms in intimate relationships highlights the urgent need for reform. The current legal regime lacks clarity on issues such as digital consent, admissibility of electronic evidence in relational disputes, and accountability for algorithm-driven surveillance. Reform is necessary to bridge the gap between technological realities and legal protections. A dedicated legal framework addressing live-in relationships in the digital context should incorporate robust cybersecurity safeguards, clear evidentiary standards for digital abuse, and gender-sensitive enforcement mechanisms. Additionally, regulatory oversight of AI systems that process personal and relational data is essential to prevent misuse and discrimination.

Thus, addressing regulatory gaps requires a multidimensional approach combining legislative reform, judicial innovation, and institutional capacity-building to ensure effective access to justice in an increasingly digitalized society.

9. Recommendations

To address these challenges, the paper proposes:

9.1 Enactment of comprehensive data protection legislation

To address the complex challenges emerging at the intersection of artificial intelligence, cybersecurity, and live-in relationships in India, this paper recommends the enactment of a comprehensive data protection legislation that specifically safeguards individuals' digital autonomy within intimate relationships. The increasing reliance on AI-enabled communication platforms and digital surveillance tools has intensified risks of non-consensual data collection, profiling, and misuse of personal information in domestic contexts.

[33] Protection of Women from Domestic Violence Act, 2005; Information Technology Act, 2000
[34] Justice K.S. Puttaswamy (Retd.) v. Union of India

While India has introduced the *Digital Personal Data Protection Act, 2023*,[35] its current framework primarily focuses on general data fiduciary obligations and does not adequately address relational power imbalances that often exist in live-in relationships. In such arrangements, partners may have informal yet deep access to each other's digital lives, creating opportunities for covert surveillance, cyberstalking, and AI-assisted manipulation.

Therefore, it is proposed that the legislation be strengthened by incorporating specific safeguards against intra-relationship data misuse, including explicit recognition of "intimate partner data abuse" as a distinct category of harm. Further, stricter consent requirements, enhanced penalties for unauthorized data access within personal relationships, and mandatory privacy-by-design obligations for AI-based applications should be introduced.

Such a framework would complement existing judicial recognition of live-in relationships as "relationships in the nature of marriage" in *Indra Sarma v. V.K.V. Sarma*,[36] ensuring that legal protections evolve in line with technological realities and uphold constitutional guarantees of privacy and dignity under *Justice K.S. Puttaswamy v. Union of India*.[37]

9.2 Regulation of AI-driven platforms

Regulation of AI-driven platforms is essential to address the emerging risks posed by algorithmic systems in the context of live-in relationships in India. AI-enabled applications, including dating platforms, social media networks, and predictive communication tools, increasingly influence intimate decision-making, partner selection, and interpersonal interactions. However, the absence of targeted regulatory oversight allows these systems to operate with limited accountability, often leading to issues such as biased profiling, unauthorized data processing, and intrusive behavioral monitoring.[38]

A robust regulatory framework should mandate transparency in algorithmic design, ensuring that users are informed about how their data is collected, processed, and used for profiling or recommendation purposes. Additionally, AI systems that handle sensitive personal information should be subject to periodic audits to prevent misuse and discriminatory outcomes. Such regulation becomes particularly significant in live-in relationships, where digital platforms may inadvertently reinforce power imbalances or enable covert surveillance.

The constitutional recognition of privacy as a fundamental right in Justice K.S. Puttaswamy

[35] *Digital Personal Data Protection Act, 2023* (India)
[36] *Indra Sarma v. V.K.V. Sarma*, (2013) 15 SCC 755
[37] *Justice K.S. Puttaswamy (Retd.) v. Union of India*, (2017) 10 SCC 1
[38] Virginia Eubanks, *Automating Inequality* (St. Martin's Press, 2018)

(Retd.) v. Union of India provides a strong normative foundation for regulating AI-driven platforms to protect informational autonomy.[39] Furthermore, aligning platform governance with the Information Technology Act, 2000 and emerging data protection standards would ensure greater accountability in the digital ecosystem.[40]

Ultimately, effective regulation of AI-driven platforms is necessary to balance technological innovation with the protection of individual rights, particularly in sensitive relational contexts such as live-in arrangements.

9.3 Expansion of domestic violence laws to include cyber abuse

To effectively address the emerging intersection of technology-facilitated abuse and intimate partner violence in live-in relationships, this paper recommends a targeted expansion of the existing domestic violence framework in India to explicitly include cyber abuse within its statutory ambit. The *Protection of Women from Domestic Violence Act, 2005* (PWDVA) currently recognizes emotional, verbal, and economic abuse, yet it does not expressly account for digital forms of coercion such as cyberstalking, non-consensual sharing of intimate images, impersonation, or surveillance through spyware.[41] Given the increasing digitisation of intimate relationships, such omissions create enforcement gaps that undermine legal protection.

Accordingly, it is proposed that the definition of "emotional and verbal abuse" under Section 3 of the PWDVA be amended to incorporate "technology-facilitated abuse," including acts committed through electronic communication platforms. This would harmonise domestic violence law with the *Information Technology Act, 2000* and its 2008 amendments, which criminalise certain online harms but operate primarily in a penal, rather than protective, framework.[42] Furthermore, judicial recognition of live-in relationships as "relationships in the nature of marriage" in cases such as *Indra Sarma v. V.K.V. Sarma*[43] necessitates extending comprehensive safeguards, including digital safety, to such partnerships.

Such reform would ensure that legal protection evolves in tandem with technological realities and strengthens preventive remedies for victims.

9.4 Judicial training on digital evidence

To address the growing complexities arising from artificial intelligence-driven cyber abuse and

[39] Justice K.S. Puttaswamy (Retd.) v. Union of India
[40] Information Technology Act, 2000
[41] *Protection of Women from Domestic Violence Act, 2005*, §3
[42] *Information Technology Act, 2000* (as amended in 2008), §§66E, 67, 72
[43] *Indra Sarma v. V.K.V. Sarma*, (2013) 15 SCC 755

digital evidence in disputes involving live-in relationships, this paper recommends structured and continuous judicial training on the appreciation and handling of digital evidence. The increasing reliance on electronic communications, metadata, cloud storage, and AI-enabled surveillance tools has made traditional evidentiary assessment inadequate in several socio-legal disputes, particularly those involving allegations of cyber harassment or coercive control within intimate relationships.

Although the *Indian Evidence Act, 1872* (now substantially replaced by the *Bharatiya Sakshya Adhiniyam, 2023*) recognizes electronic records as admissible evidence,[44] judicial interpretation often requires specialised understanding of authenticity, integrity, and chain of custody issues. In cases involving live-in relationships—recognized as "relationships in the nature of marriage" in *Indra Sarma v. V.K.V. Sarma*[45]—the evidentiary burden frequently includes WhatsApp chats, emails, GPS logs, and AI-generated content, which demand technical literacy for fair adjudication.

Accordingly, it is proposed that judicial academies under the National Judicial Academy and State Judicial Academies incorporate mandatory modules on cybersecurity fundamentals, AI manipulation detection, and digital forensic evaluation. Such training would enhance judicial capacity to distinguish between genuine and fabricated digital evidence, ensuring procedural fairness and reducing wrongful inference. This reform aligns with the broader objective of strengthening cyber-sensitive adjudication in evolving socio-legal contexts.

9.5 Public awareness regarding digital rights

To effectively address the socio-legal challenges arising from AI-driven cyber threats in live-in relationships, this paper recommends the strengthening of public awareness regarding digital rights and cyber safety. In contemporary intimate relationships, digital platforms increasingly function as spaces of communication, control, and conflict, often leading to cyberstalking, non-consensual sharing of private content, and surveillance through AI-enabled applications. However, a significant proportion of victims remain unaware of their legal rights or available remedies under Indian law.

While the *Information Technology Act, 2000* criminalises certain forms of online harm,[46] and the *Protection of Women from Domestic Violence Act, 2005* provides civil remedies against

[44] *Bharatiya Sakshya Adhiniyam, 2023*, §§57–63 (earlier provisions under the *Indian Evidence Act, 1872* relating to electronic records)
[45] *Indra Sarma v. V.K.V. Sarma*, (2013) 15 SCC 755
[46] *Information Technology Act, 2000*, §§66E, 67, 72

abuse in relationships in the nature of marriage,[47] the effectiveness of these provisions is limited by low legal literacy and inadequate awareness of cyber rights.

Accordingly, it is proposed that the State, in collaboration with civil society and digital platforms, undertake targeted awareness campaigns focusing on digital consent, data privacy, and reporting mechanisms for cyber abuse. Educational institutions should also integrate cyber ethics and digital safety into curricula to build early awareness. Special focus must be given to vulnerable groups in live-in relationships, who often operate outside formal social recognition and thus lack access to informal support systems.

Such awareness initiatives would empower individuals to identify, prevent, and legally respond to cyber abuse, thereby bridging the gap between legal protections and their practical accessibility.

10. Conclusion

The convergence of artificial intelligence, cybersecurity, and evolving socio-legal norms surrounding live-in relationships in India presents a complex and rapidly developing legal landscape. As digital technologies increasingly mediate intimate relationships, they simultaneously generate new forms of vulnerability, particularly through cyber harassment, surveillance, and AI-enabled manipulation. These challenges expose the limitations of existing legal frameworks that were primarily designed for offline forms of abuse and traditional marital structures.

Although Indian courts have progressively recognized live-in relationships as "relationships in the nature of marriage," as seen in *Indra Sarma v. V.K.V. Sarma*,[48] the corresponding protective mechanisms under the *Protection of Women from Domestic Violence Act, 2005* remain only partially responsive to digital harms. Similarly, while the *Information Technology Act, 2000* criminalises certain cyber offences,[49] its fragmented approach does not fully address the relational and psychological dimensions of technology-facilitated abuse within intimate partnerships.

This paper, therefore, underscores the need for a holistic socio-legal response that integrates doctrinal reform, institutional capacity-building, and public awareness. The proposed measures—expansion of domestic violence law to include cyber abuse, judicial training on

[47] *Protection of Women from Domestic Violence Act, 2005*, §3
[48] *Indra Sarma v. V.K.V. Sarma*, (2013) 15 SCC 755
[49] *Information Technology Act, 2000*, §§66E, 67, 72

digital evidence, and enhanced public awareness of digital rights—collectively aim to bridge the gap between technological realities and legal protections.

Ultimately, the study highlights that legal evolution must keep pace with technological transformation. A responsive legal framework that is sensitive to both gender justice and cybersecurity concerns is essential to safeguard dignity, autonomy, and privacy in contemporary live-in relationships in India.