
DIGITAL DOMESTIC VIOLENCE AGAINST WOMEN IN BHARAT: A CRITICAL SOCIO-LEGAL STUDY OF CYBERSTALKING, DIGITAL SURVEILLANCE, ECONOMIC ABUSE AND COERCIVE CONTROL

Dr. Deepti Trivedi, Assistant Professor, Department of Law,
M.D.S. University, Ajmer, Rajasthan
ORCID ID: 0009-0005-2026-3291

ABSTRACT

The rapid growth of digital technology has transformed family relationships and everyday communication in Bharat. Smartphones, social media, online banking, digital payment systems, messaging applications and location-based services have created valuable opportunities for women in education, employment, financial participation and social interaction. Though, these technologies can also be misused as instruments of domestic abuse. Digital domestic violence refers to the use of digital devices, electronic communication, online platforms or personal information to threaten, monitor, intimidate, harass, control, humiliate or economically restrict women within domestic or intimate relationships. Cyber stalking, digital surveillance, unauthorised access to accounts, password coercion, misuse of private images and digital economic control are important manifestations of this emerging form of abuse.

This research examines digital domestic violence against women in Bharat from a critical socio-legal perspective. It analyses the relevance of the Protection of Women from Domestic Violence Act 2005, the Information Technology Act 2000, the Bharatiya Nyaya Sanhita 2023, the Bharatiya Sakshya Adhiniyam 2023 and the Digital Personal Data Protection Act 2023. Particular attention is given to electronic monitoring as stalking and the challenges associated with digital evidence. The study argues that existing laws provide important remedies but do not comprehensively address the continuing and complex nature of technology-facilitated domestic abuse. It recommends stronger institutional coordination, specialised training, effective evidence preservation, accessible remedies, digital literacy and greater recognition of coercive control to strengthen the protection of women in the digital age.

Keywords: Digital Domestic Violence, Cyber stalking, Digital Surveillance, Economic Abuse, Coercive Control.

1. Introduction:

Domestic violence remains a serious social and legal challenge affecting women in Bharat. It is no longer appropriate to understand domestic violence only as physical assault occurring within the four walls of a household. It may also include sexual abuse, emotional and psychological harm, verbal humiliation, economic deprivation, intimidation, threats and controlling behaviour. Such conduct can have lasting consequences for a woman's dignity, privacy, personal autonomy, financial independence, family relationships, professional life and participation in society. The rapid development of digital technology has added a new dimension to this problem. Smartphones, social media platforms, instant messaging applications, online banking, digital payment systems, email, cloud services and location-based applications have become closely connected with everyday personal and family life. These technologies provide significant opportunities for women in education, employment, financial management, communication and access to support services. However, they can also be misused by an abusive spouse or intimate partner to monitor, threaten, isolate, humiliate and control a woman.

Digital domestic violence may be understood as the use of digital devices, electronic communication, online platforms, personal information or digital services to facilitate or continue abusive conduct within a domestic or intimate relationship. It may include cyber stalking, unauthorised access to digital accounts, compulsory disclosure of passwords, location tracking, monitoring of online conversations, repeated threatening messages, misuse of private photographs, online impersonation, social media harassment and control over digital financial resources. In many situations, digital abuse does not occur as an independent incident. It may operate together with emotional, psychological, economic, sexual or physical violence and may strengthen an existing pattern of domestic domination. The important issue is therefore not merely whether technology has been used but whether it has been used without genuine consent or for the purpose of intimidation, surveillance, restriction or control.

A distinctive feature of digital domestic violence is its ability to continue beyond physical separation. A woman may leave an abusive household but may still be monitored through her mobile phone, social media accounts, location services, financial applications or other digital platforms. Repeated messages and calls may reach her at home, at work or at other locations. An abusive partner may also attempt to control her online friendships, professional

communications, financial transactions or access to personal information. This continuous connectivity can create a sense of constant observation and insecurity. At the same time, certain forms of digital interaction may appear normal within an intimate relationship. Password sharing or location sharing may sometimes occur voluntarily. Therefore every instance of digital access between partners should not automatically be treated as domestic violence. Consent, purpose, duration, method, frequency and the impact of the conduct must be examined to determine whether technology is being used for legitimate communication or as an instrument of coercive control.

The Protection of Women from Domestic Violence Act 2005 provides an important legal foundation for addressing such conduct. Section 3 recognizes physical abuse, sexual abuse, verbal and emotional abuse and economic abuse and adopts a contextual approach to domestic violence. This framework is significant because digital conduct may produce emotional harm, restrict personal freedom or cause economic deprivation without necessarily causing visible physical injury. Digital financial control may therefore have relevance to economic abuse, while repeated threats and monitoring may contribute to emotional or psychological abuse. The Bharatiya Nyaya Sanhita 2023 also recognizes electronic monitoring within the offence of stalking under Section 78. The Bharatiya Sakshya Adhiniyam 2023 further provides a statutory framework concerning electronic records and evidence. These developments demonstrate the growing relevance of technology within the Indian legal system.

In spite of these legal developments, digital domestic violence presents significant practical challenges. Victims may hesitate to report abuse because of fear of retaliation, social stigma, economic dependency or further misuse of their private information. Digital evidence may also be temporary, easily deleted, copied, altered or redistributed. Effective investigation therefore requires appropriate knowledge of electronic evidence and digital security. Police authorities, Protection Officers, lawyers and judicial institutions need greater awareness of technology-facilitated domestic abuse. Digital domestic violence should consequently be examined as a socio-legal issue rather than merely as a cybercrime problem. It lies at the intersection of gender justice, privacy, dignity, autonomy, economic independence, domestic power relations, criminal law, evidence law and human rights. The present study critically examines cyber stalking, digital surveillance, economic abuse and coercive control against women in Bharat and considers whether the existing legal framework is sufficiently capable of responding to these emerging forms of domestic violence.

2. Meaning and Nature of Digital Domestic Violence:

Digital domestic violence refers to the use of digital devices, electronic communication, online platforms, personal information or digital services to threaten, monitor, harass, intimidate, control or otherwise abuse a woman within a domestic or intimate relationship. It is not necessarily a completely separate form of domestic violence. Rather, it represents a modern technological dimension of physical, emotional, sexual, psychological and economic abuse. Digital technology can strengthen existing patterns of domestic violence by enabling an abusive partner to maintain contact with a woman, monitor her activities, restrict her communication and exercise control even when the parties are physically separated. It can also create new forms of abusive conduct that have become possible because of widespread digital connectivity.

Digital domestic violence may include cyber stalking, unauthorised access to mobile phones and online accounts, monitoring of social media activities, location tracking, compulsory sharing of passwords, repeated threatening messages, online humiliation, misuse of private photographs, impersonation and interference with digital financial resources. Technology may also be used to isolate a woman from her family, friends, colleagues and support networks. Individual acts may sometimes appear insignificant when viewed separately. However, repeated conduct may become serious when it forms part of a continuing pattern of intimidation, surveillance and control. The central issue is therefore not merely the use of technology but the purpose, manner, circumstances and consequences of its use.

The Protection of Women from Domestic Violence Act 2005 provides an important legal foundation for understanding technology-facilitated domestic abuse. Section 3 recognizes physical abuse, sexual abuse, verbal and emotional abuse and economic abuse. Its broad approach is significant because digital abuse may cause psychological harm, threaten personal security, restrict communication or interfere with financial independence without producing visible physical injuries. Digital economic control is also an important aspect of this problem. Online banking, digital payments, mobile wallets and electronic financial accounts may be misused to restrict a woman's access to money or employment income. Such conduct can increase economic dependency and make it more difficult for a woman to leave an abusive relationship or seek legal assistance. Digital domestic violence is therefore characterized by continuity, accessibility, surveillance, control and invisibility. It can extend beyond the

physical household and operate at any time. Its proper socio-legal assessment requires consideration of technology, gender relations, privacy, autonomy, economic independence and domestic power structures.

3. Cyber stalking as a Form of Digital Domestic Violence:

Cyber stalking is a significant form of technology-facilitated domestic violence that enables an abusive spouse or intimate partner to maintain repeated contact and monitor a woman through digital platforms. It may include unwanted messages, repeated calls, monitoring of social media activities, tracking of online communications, creation of fake accounts or persistent attempts to contact the victim despite her unwillingness. The problem can become more serious in domestic relationships because the perpetrator may already possess detailed knowledge about the woman's family, friends, workplace and daily routine and personal relationships. Such information can be misused to increase digital surveillance and intimidation. Cyber stalking may also become part of a wider pattern of coercive control. An abusive partner may demand immediate responses, question online interactions, monitor conversations or use threats to obtain passwords and access to personal accounts. Section 78 of the Bharatiya Nyaya Sanhita 2023 expressly recognizes monitoring a woman's use of the internet, email or other electronic communication as stalking, subject to the statutory exceptions. This is an important recognition of electronic monitoring within criminal law. However, cyber stalking should be assessed in its broader context by considering its frequency, duration, purpose, nature and impact. Continuous digital monitoring accompanied by threats or intimidation can seriously affect a woman's privacy, dignity, autonomy, communication and personal security.

4. Digital Surveillance and Women's Autonomy:

Digital surveillance is an important form of technology-facilitated domestic abuse in which an abusive spouse or intimate partner uses digital tools to monitor and control a woman's activities. It may involve location tracking, unauthorised access to mobile phones, checking private messages, monitoring email or social media accounts, installing tracking applications or observing digital communications. Digital information may be voluntarily shared between partners for genuine purposes such as communication or safety. Though, when such access is obtained through coercion, threats, intimidation, manipulation or deception, it can become a serious form of digital abuse. Continuous monitoring may affect a woman's freedom of movement and communication and may discourage her from contacting family members,

friends, colleagues, lawyers or support organizations. The constitutional right to privacy is particularly relevant in this context. In *Justice K.S. Puttaswamy [Retd] v. Union of India*, the Supreme Court recognized privacy as a constitutionally protected right connected with dignity, autonomy and personal liberty. Marriage or a domestic relationship should not automatically be treated as consent to unrestricted digital surveillance. However, every form of digital interaction between partners cannot be regarded as domestic violence. The circumstances, consent, purpose, duration and effect of the conduct must be considered. Persistent and coercive surveillance can undermine privacy, dignity, communication and personal autonomy and may therefore constitute an important component of digital domestic violence.

5. Digital Economic Abuse:

Digital economic abuse is an emerging form of domestic violence in which digital technologies and financial platforms are used to control a woman's access to money, financial resources, employment income or economic opportunities. The growing use of online banking, digital payment applications, mobile wallets and electronic financial accounts has created new methods of exercising financial control within domestic relationships. An abusive partner may demand banking credentials, monitor transactions, control digital wallets, restrict access to online accounts or interfere with a woman's employment income. Such conduct can reduce financial independence and increase economic dependency on the perpetrator.

Section 3 of the Protection of Women from Domestic Violence Act 2005 recognizes economic abuse as a form of domestic violence. It includes deprivation of financial resources and restrictions on access to resources or facilities connected with the domestic relationship. This provision is particularly relevant in the digital environment because financial activities are increasingly conducted through electronic systems. Digital economic control can therefore become a modern method of traditional economic abuse.

The consequences may be severe for women who depend upon digital platforms for employment, business or receipt of income. Restricted access to financial resources can make it difficult to meet essential expenses, arrange alternative accommodation, obtain legal assistance or leave an abusive relationship. Digital economic abuse can therefore operate both as a method of financial domination and as a barrier to access to justice. Effective protection requires greater awareness, accessible remedies and appropriate institutional mechanisms to safeguard women's independent control over their financial resources.

6. Coercive Control through Digital Technology:

Coercive control refers to a continuous pattern of behaviour through which an individual seeks to dominate another person and restrict their freedom, autonomy and ability to make independent decisions. Digital technology has created new ways of exercising such control within domestic and intimate relationships. An abusive partner may use smart phones, social media, messaging applications, digital financial services and location-based technologies to monitor a woman's activities and relationships. Such conduct may include demanding immediate responses to messages, compulsory location sharing, checking online activities, demanding passwords, monitoring financial transactions, restricting digital contacts or threatening to disclose private information. Although an individual act may appear minor when considered separately, repeated conduct accompanied by threats, intimidation or emotional pressure can create a continuing pattern of domination. Constant digital monitoring may also cause fear and may lead a woman to change her behaviour to avoid confrontation or punishment.

The Protection of Women from Domestic Violence Act 2005 provides some legal scope for addressing such behaviour because the overall circumstances and nature of conduct can be considered while determining domestic violence. However, Indian law does not presently provide a comprehensive statutory framework specifically dealing with coercive control as an independent form of abuse. There is therefore a need for further legislative and judicial consideration of technology-enabled coercive control while ensuring due process, proportionality, fairness and protection against misuse of legal provisions.

7. Social Media Abuse and Misuse of Private Images:

Social media platforms have become an important medium through which domestic abuse can be extended into the digital environment. An abusive spouse or intimate partner may monitor a woman's online activities, restrict her social contacts, demand access to her social media accounts, impersonate her or publish offensive and humiliating content. Such conduct can cause emotional distress, fear, social isolation and reputational harm. When these actions are repeated and accompanied by threats or intimidation, they may become part of a broader pattern of coercive control.

The misuse of private or intimate images is another serious form of digital domestic violence. A woman may voluntarily share a private image with her partner on the basis of trust and confidentiality. Such consent should not be understood as permission to publish, forward or distribute that image to other persons. The Bharatiya Nyaya Sanhita 2023 recognizes the importance of consent in its provisions relating to voyeurism and distinguishes consent to capture an image from consent to its dissemination. Threatening to publish private images may also be used to intimidate a woman and discourage her from ending an abusive relationship or seeking legal assistance. The rapid copying and redistribution of digital content makes such abuse difficult to control. Therefore, effective protection requires prompt legal intervention, proper preservation of electronic evidence, victim-sensitive procedures and efficient mechanisms for reporting and removing unlawful content from digital platforms.

8. Protection of Women from Domestic Violence Act 2005:

The Protection of Women from Domestic Violence Act 2005 is an important legal framework for protecting women from violence within domestic relationships. Section 3 adopts a broad understanding of domestic violence by recognizing physical abuse, sexual abuse, verbal and emotional abuse and economic abuse. This broad approach is relevant to the emerging problem of digital domestic violence because technology-enabled conduct may contribute to emotional harm, financial control, intimidation and continuous surveillance. For instance, repeated threatening messages, unauthorised monitoring of digital activities, control over online financial resources and misuse of private information may form part of a wider pattern of domestic abuse.

The Act provides several protective and remedial measures, including protection orders, residence orders, monetary relief, custody orders, compensation and interim relief. These remedies can become particularly important for women facing technology-facilitated abuse because digital violence may continue even after physical separation from the perpetrator. However, the effective application of the Act to digital domestic violence requires greater awareness among women, Protection Officers, police authorities, lawyers, and courts. A victim-centered approach is necessary to ensure that existing legal remedies are effectively applied to contemporary forms of digital abuse and that technological methods of control do not remain outside the practical protection provided by domestic violence law.

9. Bharatiya Nyaya Sanhita 2023 and Digital Abuse:

The Bharatiya Nyaya Sanhita, 2023, provides an important criminal law framework for addressing technology-facilitated abuse against women. Section 78 expressly recognizes monitoring a woman's use of the internet, email or other electronic communication as a form of stalking, subject to the exceptions provided under the law. This provision is significant because it acknowledges that stalking can occur through digital means and need not involve physical following. The BNS also contains provisions relating to cruelty by a husband or the relatives of a husband. These provisions may become relevant where digital harassment or surveillance forms part of a wider pattern of cruelty within a domestic relationship.

The BNS therefore creates an important connection between traditional criminal law and emerging forms of digital abuse. However, criminal prosecution alone cannot address all the needs of a victim of digital domestic violence. A woman may require immediate protection, financial assistance, safe accommodation, counseling, legal support and preservation of electronic evidence. Therefore, the BNS should operate alongside the Protection of Women from Domestic Violence Act 2005 and other applicable laws to provide a comprehensive and victim-centered response to technology-facilitated domestic violence.

10. Information Technology Act 2000 and Digital Abuse:

The Information Technology Act, 2000 remains an important part of the Indian legal framework for addressing technology-related misconduct. Its provisions may become relevant in cases of digital domestic abuse depending upon the nature and circumstances of the conduct. Unauthorised access to computer resources, misuse of identity or digital credentials, violation of privacy and the transmission or publication of certain unlawful electronic material may attract legal consequences under applicable provisions. These provisions are particularly relevant where an abusive spouse or intimate partner misuses digital devices, accounts, personal information or online platforms to threaten or control a woman. However, the Information Technology Act should not be examined in isolation because digital domestic violence involves both technological and domestic dimensions.

The Protection of Women from Domestic Violence Act 2005 may provide protective and remedial measures, while the Bharatiya Nyaya Sanhita 2023, may apply where the conduct constitutes a criminal offence. The Bharatiya Sakshya Adhiniyam 2023 is relevant to the

treatment of electronic records and digital evidence. These legal frameworks therefore need to operate together according to the facts of each case. A coordinated approach can help ensure that technology-facilitated abuse is properly identified, investigated and addressed while providing effective protection to women.

11. Electronic Evidence under the Bharatiya Sakshya Adhiniyam 2023:

Electronic evidence is an essential component in cases involving technology-facilitated domestic violence. Such evidence may include text messages, emails, photographs, videos, social media conversations, call records, digital payment information, location data and records of online account activity. The Bharatiya Sakshya Adhiniyam 2023 gives statutory recognition to electronic and digital records and provides an important evidentiary framework for cases involving digital abuse. Section 61 recognizes the legal validity of electronic or digital records and provides that their admissibility cannot be denied merely because they exist in electronic form. Section 63 further establishes the conditions governing the admissibility of electronic records and computer-generated information. These provisions are particularly significant for women who may depend upon digital material to demonstrate cyber stalking, threats, surveillance, financial control or misuse of private information.

On the other hand, preservation and authenticity of such evidence remain important concerns. Messages may be deleted, accounts may be altered, devices may be damaged and digital information may be manipulated or lost. Screenshots may also fail to provide the complete context of a communication. Victims should therefore be guided on the proper preservation of relevant digital material. Investigating authorities should follow appropriate procedures for collection, authentication and forensic examination. Courts should evaluate electronic evidence according to the statutory requirements while ensuring that the privacy and dignity of victims are adequately protected.

12. Socio-Legal Dimensions of Digital Domestic Violence:

Digital domestic violence cannot be effectively understood through statutory provisions alone because social attitudes, gender relations, family structures and economic conditions strongly influence how technology-enabled control is perceived. In some domestic relationships, checking a wife's mobile phone, demanding passwords, monitoring social media accounts or continuously seeking location information may be regarded as normal marital behaviour rather

than potential abuse. Such attitudes can prevent women from identifying coercive conduct and may discourage them from seeking legal assistance. Economic dependency further increases vulnerability because women without independent financial resources may find it difficult to resist digital financial control or leave an abusive relationship. Digital literacy is another important concern. Familiarity with smartphones and online applications does not necessarily provide adequate knowledge about privacy settings, account security, unauthorised monitoring, evidence preservation or reporting mechanisms. Language can also create barriers to accessing legal and technological information, particularly for women in rural and semi-urban communities. Information regarding legal remedies and digital safety should therefore be made available in Hindi and other regional languages. Addressing digital domestic violence requires a combination of legal protection, institutional support, social awareness and digital education. Legal rights can provide meaningful protection only when women understand those rights and can access the institutions and technological resources necessary to exercise them effectively.

13. Role of Police and Protection Officers:

Effective implementation of the legal framework requires police authorities and Protection Officers to possess adequate knowledge of technology-facilitated domestic violence. Police officers should be trained to identify digital abuse and distinguish ordinary disagreements within domestic relationships from repeated patterns of surveillance, intimidation, harassment and coercive control. Complaints involving threatening messages, unauthorised account access, location tracking, digital financial control or repeated electronic communication should be examined in their wider context.

Investigators should also ensure the proper preservation and collection of relevant electronic evidence. Protection Officers appointed under the Protection of Women from Domestic Violence Act 2005 should receive basic training in digital safety, privacy protection and electronic evidence. They should be capable of guiding victims regarding password security, account protection, evidence preservation and appropriate reporting mechanisms. Effective institutional coordination is equally important. Police authorities, Protection Officers, cybercrime units, courts, legal services institutions and women's support organizations should develop coordinated mechanisms for responding to digital domestic violence. Such coordination can provide faster assistance and reduce the need for victims to repeatedly explain their experiences before different authorities. A victim-centered institutional approach can

therefore strengthen access to justice and ensure that existing legal remedies are effectively applied to emerging forms of technology-facilitated domestic abuse.

Conclusion:

Digital domestic violence has emerged as a significant contemporary dimension of violence against women in Bharat. The rapid development of smartphones, social media, digital payment systems, online banking, messaging applications and location-based technologies has changed the manner in which individuals communicate and maintain relationships. These developments have created valuable opportunities for women but they have also provided new methods through which abusive partners can exercise surveillance, intimidation, economic control and coercive behaviour. Digital domestic violence therefore demonstrates that violence within domestic and intimate relationships is no longer confined to the physical household. It can continue through digital devices and online platforms even when the woman and the perpetrator are physically separated.

The present study demonstrates that cyber stalking, digital surveillance, digital economic abuse, social media abuse, misuse of private images and coercive control are closely connected forms of technology-facilitated domestic abuse. A Smartphone can be misused to monitor a woman's movements and communications. Social media accounts can be used to restrict relationships humiliate the victim or threaten reputational harm. Digital banking and payment applications can become instruments of financial control. Messaging platforms can be used for repeated threats, intimidation and unwanted communication. These forms of abuse may appear minor when examined individually but their cumulative effect can seriously affect a woman's privacy, dignity, autonomy, emotional well-being, financial independence and freedom of choice.

The Protection of Women from Domestic Violence Act 2005 continues to provide an important foundation for responding to these emerging forms of abuse. Its recognition of physical, sexual, verbal and emotional and economic abuse allows the law to address different dimensions of domestic violence. The requirement to consider the overall circumstances of the case is particularly relevant to digital domestic violence because technology-enabled abuse frequently occurs through a continuing pattern rather than through one isolated incident. Digital financial control may fall within the understanding of economic abuse, while repeated threats, harassment and surveillance may form part of emotional or controlling behaviour. The Act

therefore provides significant protective possibilities, although its effective application to rapidly developing forms of digital abuse requires greater institutional awareness.

The Bharatiya Nyaya Sanhita 2023 has added an important contemporary dimension to criminal law by expressly recognizing electronic monitoring within the offence of stalking under Section 78. This development reflects the changing nature of stalking in the digital environment. Similarly, the Bharatiya Sakshya Adhiniyam 2023 provides a statutory framework for electronic and digital records. This is particularly important because digital domestic violence cases may depend upon messages, emails, photographs, videos, call records, location information, social media communications and financial records. However, effective use of digital evidence requires proper preservation, authentication, investigation and forensic examination.

The study also highlights that legal provisions alone cannot eliminate digital domestic violence. Social attitudes and gender-based power structures may normalize behaviours such as checking a woman's phone, demanding passwords, monitoring her location or controlling her online contacts. Economic dependency and inadequate digital literacy can further increase vulnerability. Many women may not know how to secure their accounts, preserve electronic evidence, report digital abuse or access appropriate legal remedies. Institutional limitations can also affect effective implementation. Police officers, Protection Officers, cybercrime authorities, legal professionals and support organizations therefore require specialised training and stronger coordination.

A comprehensive response should combine domestic violence law, criminal law, cyber law, evidence law, privacy principles and data protection mechanisms. Protection Officers and police authorities should be equipped to recognize technology-facilitated abuse and guide victims regarding digital safety and evidence preservation. Courts should adopt victim-sensitive approaches while maintaining evidentiary safeguards and due process. Greater public awareness and multilingual digital literacy programmes are also necessary so that women can understand their rights and protect their digital identities and financial resources.

In due course, protection of women in the digital age requires protection not only from physical violence but also from technological surveillance, digital intimidation, economic control, privacy violations and coercive domination. Digital domestic violence should therefore be recognized as an important issue of gender justice, constitutional dignity, privacy, autonomy

and access to justice in Bharat. Technological advancement should contribute to women's empowerment and independence rather than become a means of extending domestic domination. A responsive legal and institutional framework must therefore evolve alongside technological change and ensure that every woman can use the digital environment with safety, dignity, freedom and equal participation.

References and Bibliography:

- i. The Constitution of India 1950.
- ii. The Protection of Women from Domestic Violence Act 2005, Act No. 43 of 2005.
- iii. The Protection of Women from Domestic Violence Rules 2006.
- iv. The Information Technology Act 2000, Act No. 21 of 2000.
- v. The Information Technology [Intermediary Guidelines and Digital Media Ethics Code] Rules 2021.
- vi. The Bharatiya Nyaya Sanhita 2023, Act No. 45 of 2023.
- vii. The Bharatiya Nagarik Suraksha Sanhita, 2023 Act No. 46 of 2023.
- viii. The Bharatiya Sakshya Adhiniyam 2023, Act No. 47 of 2023.
- ix. The Digital Personal Data Protection Act 2023, Act No. 22 of 2023.
- x. Justice K.S. Puttaswamy [Retd.] v. Union of India 2017 10 SCC 1.
- xi. Hiral P. Harsora v. Kusum Narottamdas Harsora 2016 10 SCC 165.
- xii. Satish Chander Ahuja v. Sneha Ahuja 2021 1 SCC 414.
- xiii. Prabha Tyagi v. Kamlesh Devi 2022 8 SCC 90.
- xiv. Anuradha Bhasin v. Union of India 2020 3 SCC 637.
- xv. Shreya Singhal v. Union of India 2015 5 SCC 1.
- xvi. Pavan Duggal, Cyber Law: The Indian Perspective, Universal Law Publishing Delhi.
- xvii. S.R. Myneni, Information Technology Law, Asia Law House Hyderabad.
- xviii. Apar Gupta, Technology Laws Decoded, Lexis Nexis Gurgaon.

- xix. National Crime Records Bureau, Crime in India, Ministry of Home Affairs, Government of India New Delhi.
- xx. National Commission for Women, Annual Report, Government of India New Delhi.
- xxi. World Health Organization, Violence against Women Prevalence Estimates 2018, World Health Organization Geneva.