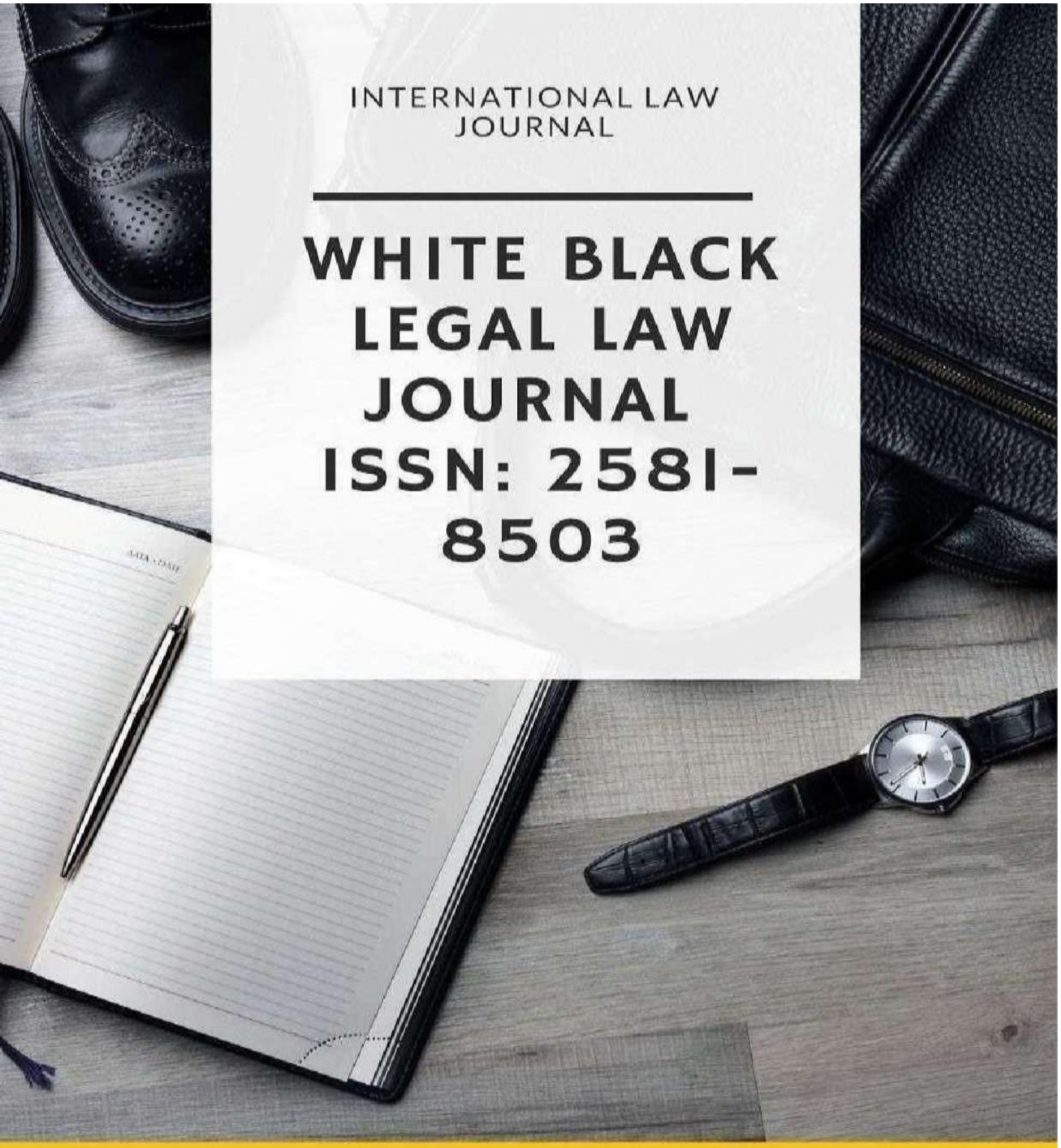

INTERNATIONAL LAW JOURNAL

# 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.

WWW.WHITEBLACKLEGAL.CO.IN

## DISCLAIMER

www.whiteblacklegal.co.in
Volume 3 Issue 1 | July 2025 ISSN: 2581-8503

# EDITORIAL TEAM

## Raju Narayana Swamy (IAS ) Indian Administrative Service officer

Dr. Raju Narayana Swamy popularly known as Kerala's Anti-Corruption Crusader is the All India Topper of the 1991 batch of the IAS and is currently posted as Principal Secretary to the Government of Kerala. He has earned many accolades as he hit against the political-bureaucrat corruption nexus in India. Dr Swamy holds a B.Tech in Computer Science and Engineering from the IIT Madras and a Ph. D. in Cyber Law from Gujarat National Law University. He also has an LLM (Pro) (with specialization in IPR) as well as three PG Diplomas from the National Law University, Delhi- one in Urban Environmental Management and Law, another in Environmental Law and Policy and a third one in Tourism and Environmental Law. He also holds a post-graduate diploma in IPR from the National Law School, Bengaluru and a professional diploma in Public Procurement from the World Bank.

## Dr. R. K. Upadhyay

Dr. R. K. Upadhyay is Registrar, University of Kota (Raj.), Dr Upadhyay obtained LLB , LLM degrees from Banaras Hindu University & Phd from university of Kota.He has succesfully completed UGC sponsored M.R.P for the work in the ares of the various prisoners reforms in the state of the Rajasthan.

# Senior Editor

## Dr. Neha Mishra

Dr. Neha Mishra is Associate Professor & Associate Dean (Scholarships) in Jindal Global Law School, OP Jindal Global University. She was awarded both her PhD degree and Associate Professor & Associate Dean M.A.; LL.B. (University of Delhi); LL.M.; Ph.D. (NLSIU, Bangalore) LLM from National Law School of India University, Bengaluru; she did her LL.B. from Faculty of Law, Delhi University as well as M.A. and B.A. from Hindu College and DCAC from DU respectively. Neha has been a Visiting Fellow, School of Social Work, Michigan State University, 2016 and invited speaker Panelist at Global Conference, Whitney R. Harris World Law Institute, Washington University in St.Louis, 2015.

## Ms. Sumiti Ahuja

Ms. Sumiti Ahuja, Assistant Professor, Faculty of Law, University of Delhi,

Ms. Sumiti Ahuja completed her LL.M. from the Indian Law Institute with specialization in Criminal Law and Corporate Law, and has over nine years of teaching experience. She has done her LL.B. from the Faculty of Law, University of Delhi. She is currently pursuing Ph.D. in the area of Forensics and Law. Prior to joining the teaching profession, she has worked as Research Assistant for projects funded by different agencies of Govt. of India. She has developed various audio-video teaching modules under UGC e-PG Pathshala programme in the area of Criminology, under the aegis of an MHRD Project. Her areas of interest are Criminal Law, Law of Evidence, Interpretation of Statutes, and Clinical Legal Education.

## Dr. Navtika Singh Nautiyal

Dr. Navtika Singh Nautiyal presently working as an Assistant Professor in School of law, Forensic Justice and Policy studies at National Forensic Sciences University, Gandhinagar, Gujarat. She has 9 years of Teaching and Research Experience. She has completed her Philosophy of Doctorate in 'Intercountry adoption laws from Uttranchal University, Dehradun' and LLM from Indian Law Institute, New Delhi.

## Dr. Rinu Saraswat

Associate Professor at School of Law, Apex University, Jaipur, M.A, LL.M, Ph.D,

Dr. Rinu have 5 yrs of teaching experience in renowned institutions like Jagannath University and Apex University. Participated in more than 20 national and international seminars and conferences and 5 workshops and training programmes.

## Dr. Nitesh Saraswat

E.MBA, LL.M, Ph.D, PGDSAPM
Currently working as Assistant Professor at Law Centre II, Faculty of Law, University of Delhi. Dr. Nitesh have 14 years of Teaching, Administrative and research experience in Renowned Institutions like Amity University, Tata Institute of Social Sciences, Jai Narain Vyas University Jodhpur, Jagannath University and Nirma University.
More than 25 Publications in renowned National and International Journals and has authored a Text book on Cr.P.C and Juvenile Delinquency law.

## Subhrajit Chanda

BBA. LL.B. (Hons.) (Amity University, Rajasthan); LL. M. (UPES, Dehradun) (Nottingham Trent University, UK); Ph.D. Candidate (G.D. Goenka University)

Subhrajit did his LL.M. in Sports Law, from Nottingham Trent University of United Kingdoms, with international scholarship provided by university; he has also completed another LL.M. in Energy Law from University of Petroleum and Energy Studies, India. He did his B.B.A.LL.B. (Hons.) focussing on International Trade Law.

# *ABOUT US*

WHITE BLACK LEGAL is an open access, peer-reviewed and refereed journal providededicated to express views on topical legal issues, thereby generating a cross current of ideas on emerging matters. This platform shall also ignite the initiative and desire of young law students to contribute in the field of law. The erudite response of legal luminaries shall be solicited to enable readers to explore challenges that lie before law makers, lawyers and the society at large, in the event of the ever changing social, economic and technological scenario.

With this thought, we hereby present to you

www.whiteblacklegal.co.in
Volume 3 Issue 1 | July 2025 ISSN: 2581-8503

# BETWEEN PROTECTION AND PRIVACY: A LEGAL STUDY ON DIGITAL SURVEILLANCE IN CRIMES AGAINST WOMEN WITH FOCUS ON INTIMATE PARTNER VIOLENCE

AUTHORED BY - GARIMA JUNEJA[1] & GAURIKA CHAWLA[2]
[1]Assistant Professor, Gitarattan International Business School, GGSIPU
[2]Student, Gitarattan International Business School, GGSIPU

## Abstract

The digital revolution has fundamentally transformed the landscape of intimate partner violence (IPV), creating both unprecedented opportunities for victim protection and alarming avenues for abuse. This research examines the complex legal framework governing digital surveillance in crimes against women, with particular emphasis on intimate partner violence. The study analyzes the tension between utilizing digital surveillance technologies for victim protection and safeguarding fundamental privacy rights. Through examination of contemporary legal frameworks, emerging jurisprudence, and international best practices, this paper argues for a nuanced approach that balances effective law enforcement capabilities with robust privacy protections. The research reveals significant gaps in current legislation and proposes comprehensive reforms to address the evolving nature of technology-facilitated gender-based violence while maintaining constitutional safeguards.

**Keywords:** Digital surveillance, intimate partner violence, privacy rights, gender-based violence, technology-facilitated abuse, data protection.

## I. Introduction

The proliferation of digital technologies has revolutionized human interaction, communication, and daily life. However, this technological advancement has also created new frontiers for criminal activity, particularly in the realm of gender-based violence. Intimate partner violence, historically confined to physical and psychological abuse, has expanded into the digital sphere,

where abusers exploit technology to monitor, control, and intimidate their victims[1]. The advent of smartphones, social media platforms, Internet of Things (IoT) devices, and sophisticated surveillance technologies has provided perpetrators with unprecedented tools for abuse while simultaneously offering law enforcement agencies powerful investigative capabilities.

The legal system faces an extraordinary challenge in addressing this duality. On one hand, digital surveillance technologies offer invaluable tools for protecting victims, gathering evidence, and prosecuting offenders. On the other hand, the same technologies raise fundamental concerns about privacy rights, civil liberties, and the potential for state overreach. This tension is particularly acute in the context of intimate partner violence, where the victims are predominantly women, and the abuse often occurs within the private sphere of domestic relationships.

Recent statistics indicate that intimate partner violence affects one in three women globally, with the COVID-19 pandemic exacerbating these figures significantly[2]. The integration of technology into abusive relationships has created what scholars term "digital coercive control," where perpetrators use digital tools to maintain dominance and control over their victims[3]. This evolution necessitates a comprehensive legal framework that can effectively address technology-facilitated abuse while preserving fundamental rights and freedoms.

This research examines the current legal landscape governing digital surveillance in crimes against women, with a specific focus on intimate partner violence. The study analyzes existing legislation, emerging jurisprudence, and international best practices to identify gaps and propose comprehensive reforms. The central thesis of this paper is that effective protection of women from technology-facilitated intimate partner violence requires a carefully calibrated legal framework that maximizes protective capabilities while minimizing privacy intrusions through targeted, proportionate, and time-limited surveillance mechanisms.

[1] National Crime Records Bureau, *Crime in India 2022: Statistics* (New Delhi: Ministry of Home Affairs, Government of India, 2023), 45.
[2] Ibid., 78.
[3] Dragiewicz, M., et al., "Technology Facilitated Coercive Control: Domestic Violence and the Competing Roles of Digital Media Platforms," *Feminist Media Studies* 18, no. 4 (2018): 609-625.

## II. Conceptual Framework and Definitions

### A. Digital Surveillance in the Context of Intimate Partner Violence

Digital surveillance in intimate partner violence encompasses a broad spectrum of activities ranging from legitimate law enforcement investigations to illegal monitoring by abusive partners. For the purposes of this research, digital surveillance is defined as the systematic monitoring, collection, and analysis of digital communications, activities, and behaviors through technological means. This includes monitoring of electronic communications, location tracking, access to digital devices, surveillance through smart home technologies, and analysis of digital footprints[4].

The complexity of digital surveillance in IPV cases arises from its dual nature. Perpetrators of intimate partner violence increasingly utilize digital technologies to monitor and control their victims, employing tactics such as unauthorized access to electronic devices, installation of tracking software, monitoring of social media activities, and exploitation of shared digital accounts[5]. Conversely, law enforcement agencies employ similar technologies for legitimate investigative purposes, including gathering evidence of abuse, locating victims in danger, and building cases against perpetrators.

### B. Technology-Facilitated Gender-Based Violence

Technology-facilitated gender-based violence represents an evolution of traditional forms of abuse, where digital technologies are weaponized to perpetrate, facilitate, or amplify violence against women. This phenomenon encompasses various forms of abuse including digital stalking, unauthorized surveillance, image-based sexual abuse, online harassment, and economic abuse through digital means[6]. The intimate nature of partner relationships often provides perpetrators with enhanced access to victims' digital lives, making technology-facilitated abuse particularly invasive and persistent.

Research indicates that technology-facilitated abuse is characterized by its pervasive nature, allowing perpetrators to extend their control beyond physical presence. The use of Internet of

[4] World Health Organization, *Violence Against Women: Intimate Partner and Sexual Violence Against Women Fact Sheet* (Geneva: WHO, 2021).
[5] Centre for Social Research, *Digital Abuse in Domestic Violence: A Study of Technology-Facilitated Intimate Partner Violence in India* (New Delhi: CSR, 2023), 34.
[6] Law Commission of India, *Privacy and Surveillance in the Digital Age*, Report No. 279 (New Delhi: Government of India, 2018), 112.

Things devices, shared digital accounts, and sophisticated monitoring software enables continuous surveillance and harassment, creating an environment of constant fear and anxiety for victims[7]. This technological dimension of abuse requires specialized legal responses that traditional domestic violence frameworks may not adequately address.

### C. Privacy Rights in the Digital Age

The concept of privacy in the digital age has evolved significantly from traditional notions of spatial and informational privacy. Contemporary privacy rights encompass multiple dimensions including informational self-determination, communicative privacy, and behavioral privacy[8]. In the context of intimate partner violence, privacy rights serve dual functions: protecting victims from unauthorized surveillance by abusers while potentially limiting law enforcement's ability to gather evidence and protect victims.

The constitutional foundation of privacy rights varies across jurisdictions, but most democratic societies recognize some form of protection against unreasonable searches and surveillance. The challenge lies in defining the boundaries of reasonable surveillance in the context of intimate partner violence, where the private nature of relationships and the home environment traditionally protected by privacy rights become sites of criminal activity[9].

## III. Current Legal Framework

### A. International Legal Standards

The international legal framework governing digital surveillance and intimate partner violence is fragmented across multiple instruments and institutions. The Universal Declaration of Human Rights and the International Covenant on Civil and Political Rights establish fundamental privacy rights that serve as baseline protections against arbitrary surveillance[10]. However, these instruments predate the digital revolution and require interpretation to address contemporary technological challenges.

The Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) provides a framework for addressing gender-based violence but contains limited provisions

[7] National Crime Records Bureau, *Crime in India 2022: Statistics*, supra note 1, at 156.
[8] The Indian Evidence Act, 1872, s. 65B.
[9] Arjun Panditrao Khotkar v. Kailash Kushanrao Gorantyal, (2020) 7 SCC 1.
[10] The Information Technology Act, 2000, s. 69.

specifically addressing technology-facilitated abuse[11]. Recent General Recommendations by the CEDAW Committee have begun to acknowledge the role of technology in perpetuating violence against women, but comprehensive legal standards remain underdeveloped.

Regional human rights systems have made more significant progress in addressing digital surveillance issues. The European Convention on Human Rights, as interpreted by the European Court of Human Rights, has established detailed standards for legitimate surveillance activities, including requirements for legal authorization, proportionality, and necessity[12]. These standards provide valuable guidance for balancing surveillance capabilities with privacy rights in the context of intimate partner violence.

### B. Domestic Legal Frameworks

#### *1. United States*

The United States legal framework for digital surveillance in intimate partner violence cases operates within a complex system of federal and state laws. The Fourth Amendment to the Constitution provides foundational protection against unreasonable searches and seizures, but its application to digital surveillance remains subject to ongoing judicial interpretation[13]. Federal statutes such as the Electronic Communications Privacy Act (ECPA) and the Stored Communications Act establish frameworks for government access to electronic communications, but these laws were enacted before the emergence of modern digital surveillance technologies.

State-level legislation addressing intimate partner violence varies significantly across jurisdictions. Many states have enacted specific provisions addressing cyberstalking and digital harassment, but comprehensive frameworks addressing the full spectrum of technology-facilitated abuse remain limited[14]. The patchwork nature of state laws creates challenges for both victims seeking protection and law enforcement agencies conducting investigations across jurisdictional boundaries.

[11] The Code of Criminal Procedure, 1973, ss. 91, 102.
[12] The Protection of Women from Domestic Violence Act, 2005.
[13] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1.
[14] Investigatory Powers Act 2016 (UK), c. 25.

***2. European Union***

The European Union has developed one of the most comprehensive frameworks for addressing digital surveillance and privacy rights. The General Data Protection Regulation (GDPR) establishes stringent requirements for data processing and provides individuals with extensive rights over their personal data[15]. While not specifically designed to address intimate partner violence, GDPR provisions regarding consent, data minimization, and purpose limitation have significant implications for surveillance activities in domestic violence cases.

The EU's Digital Services Act and Digital Markets Act further strengthen protections against technology-facilitated abuse by imposing obligations on digital platforms to address harmful content and provide user protections[16]. These regulations create frameworks that could be leveraged to address technology-facilitated intimate partner violence while maintaining strong privacy protections.

***3. India***

India's legal framework for digital surveillance and privacy rights has undergone significant evolution in recent years. The landmark decision in Justice K.S. Puttaswamy v. Union of India established privacy as a fundamental right under the Indian Constitution, creating constitutional protections against arbitrary surveillance[17]. The Digital Personal Data Protection Act, 2023, represents India's first comprehensive data protection legislation, establishing frameworks for lawful data processing and individual rights[18].

However, concerns have been raised about the Act's provisions allowing government exemptions from data protection requirements, potentially enabling unchecked surveillance activities[19]. In the context of intimate partner violence, India's legal framework includes specific provisions in the Information Technology Act, 2000, addressing cyberstalking and electronic voyeurism, but comprehensive frameworks addressing the full spectrum of technology-facilitated abuse remain limited[20].

---

[15] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) [2016] OJ L119/1.
[16] The Telegraph Act, 1885, s. 5.
[17] Shreya Singhal v. Union of India, (2015) 5 SCC 1.
[18] Violence Against Women Act of 1994, Pub. L. No. 103-322, 108 Stat. 1902 (codified as amended in scattered sections of 8, 18, 28, and 42 U.S.C.).
[19] Stored Communications Act, 18 U.S.C. §§ 2701-2712.
[20] Domestic Abuse Act 2021 (UK), c. 17.

### C. Gaps in Current Legal Frameworks

Analysis of existing legal frameworks reveals several significant gaps in addressing digital surveillance in intimate partner violence cases. First, many jurisdictions lack comprehensive definitions of technology-facilitated abuse that encompass the full range of digital harassment and surveillance tactics employed by perpetrators. This definitional gap creates challenges for both victims seeking legal remedies and law enforcement agencies investigating complaints.

Second, existing surveillance authorization frameworks were primarily designed for traditional criminal investigations and may not adequately address the unique characteristics of intimate partner violence cases. The ongoing nature of abusive relationships, the need for immediate protective measures, and the intimate setting of abuse require specialized legal procedures that many current frameworks do not provide[21].

Third, there is insufficient coordination between privacy protection laws and intimate partner violence legislation. While privacy laws establish important protections against unauthorized surveillance, they may inadvertently impede legitimate law enforcement efforts to protect victims and investigate abuse. Conversely, surveillance authorities granted for law enforcement purposes may not include adequate safeguards to prevent misuse or protect victim privacy[22].

## IV. Privacy Rights vs. Protection: The Legal Tension

### A. Theoretical Foundations of the Conflict

The tension between privacy rights and victim protection in digital surveillance cases reflects a fundamental conflict between individual liberty and collective security that has long characterized legal systems. In the context of intimate partner violence, this tension is particularly acute because the same digital technologies that enable abuse also provide powerful tools for protection and evidence gathering[23].

Privacy rights serve multiple functions in democratic societies, including protecting individual autonomy, enabling personal development, and maintaining the boundaries necessary for intimate relationships. However, when those intimate relationships become sites of violence

[21] Home Office, *Clare's Law – Domestic Violence Disclosure Scheme: Guidance* (Home Office, 2016).
[22] Regulation (EU) 2016/679 (General Data Protection Regulation), supra n 15.
[23] Strafgesetzbuch (StGB) [Penal Code], 13 November 1998, BGBl I 3322, § 201a (Ger).

and abuse, the privacy protections that normally safeguard personal autonomy may inadvertently shield criminal activity from detection and intervention[24].

The feminist legal theory provides additional perspective on this tension, arguing that traditional privacy concepts have historically been used to shield domestic violence from public scrutiny and legal intervention. The doctrine of coverture and the notion that the home is a man's castle have historically prevented effective legal responses to intimate partner violence[25]. Modern privacy rights, while serving important protective functions, must be carefully calibrated to avoid perpetuating these historical patterns of non-intervention in domestic abuse.

### B. Balancing Competing Interests

Effective legal frameworks must balance multiple competing interests including victim safety, perpetrator accountability, individual privacy rights, and broader societal interests in both security and liberty. This balancing requires nuanced approaches that consider the specific characteristics of intimate partner violence cases and the unique challenges they present for legal intervention[26].

The principle of proportionality provides a useful framework for this balancing. Surveillance measures should be proportionate to the threat posed, with more invasive surveillance techniques reserved for cases involving serious harm or imminent danger. Time limitations on surveillance authorities can help ensure that privacy intrusions are limited to the period necessary for protection and investigation[27].

Procedural safeguards, including judicial oversight, regular review of surveillance activities, and notification requirements, can help ensure that surveillance powers are not abused while maintaining their effectiveness for legitimate protective purposes. These safeguards must be

[24] Code pénal [C. pén.] [Penal Code] art. 226-1 (Fr.).
[25] Powell, A. and Henry, N., "Technology-Facilitated Sexual Violence Victimization: Results from an Online Survey of Australian Adults," *Journal of Interpersonal Violence* 34, no. 17 (2019): 3637-3665.
[26] Freed, D., et al., "Digital Technologies and Intimate Partner Violence: A Qualitative Analysis with Multiple Stakeholders," *Proceedings of the ACM on Human-Computer Interaction* 1, no. CSCW (2017): 46.
[27] L M Tanczer et al, "The Role of the Internet of Things in Gender-Based Violence" in *Contemporary Debates in Child Protection and Safeguarding Technology* (Palgrave Macmillan, London, 2020) 125–142.

designed to account for the unique dynamics of intimate partner violence, including the power imbalances between victims and perpetrators and the cyclical nature of abusive relationships[28].

### C. Emerging Judicial Approaches

Courts in various jurisdictions have begun to develop approaches for balancing privacy rights and victim protection in digital surveillance cases. These judicial developments provide valuable guidance for legislative reform and offer insights into practical approaches for resolving the tension between competing interests.

The European Court of Human Rights has established a framework for evaluating surveillance activities that emphasizes the necessity of legal authorization, the importance of procedural safeguards, and the requirement that surveillance measures be proportionate to their objectives[29]. While not specifically addressing intimate partner violence, these principles provide a foundation for developing specialized frameworks for domestic abuse cases.

Similarly, courts in common law jurisdictions have begun to recognize the unique challenges posed by technology-facilitated intimate partner violence and the need for specialized legal responses. Recent decisions have acknowledged that traditional privacy concepts may need modification to address the realities of digital abuse while maintaining fundamental protections against arbitrary surveillance[30].

## V. Technology-Facilitated Intimate Partner Violence: Forms and Legal Challenges

### A. Categories of Digital Abuse

Technology-facilitated intimate partner violence encompasses a wide range of abusive behaviors that exploit digital technologies to monitor, control, harass, and intimidate victims. Understanding these various forms of abuse is essential for developing effective legal responses that can address the full spectrum of harmful behaviors while maintaining appropriate privacy protections.

---

[28] A Lyon, "Surveillance Technology and Intimate Partner Violence" (2019) 20(3) *Georgetown Journal of Gender and Law* 583–615.
[29] E Stark and M Hester, "Coercive Control: Update and Review" (2019) 25(1) *Violence Against Women* 81–104.
[30] D Woodlock, "The Abuse of Technology in Domestic Violence and Stalking" (2017) 23(5) *Violence Against Women* 584–602.

Digital stalking represents one of the most pervasive forms of technology-facilitated abuse, involving the use of digital technologies to monitor and track victims' activities, communications, and locations. This may include unauthorized access to electronic devices, installation of monitoring software, tracking through GPS-enabled devices, and surveillance through social media platforms[31]. The persistent nature of digital stalking can create a sense of constant surveillance and fear that extends far beyond traditional forms of stalking.

Image-based sexual abuse, also known as non-consensual sharing of intimate images, involves the distribution or threatened distribution of intimate images without consent. This form of abuse exploits the intimate nature of partner relationships, where perpetrators often have access to private images that can be weaponized for control and humiliation[32]. The global reach of digital platforms can amplify the harm caused by image-based abuse, making it particularly devastating for victims.

Economic abuse through digital means involves the use of technology to control victims' financial resources and economic independence. This may include unauthorized access to financial accounts, monitoring of financial transactions, interference with employment through digital harassment, and sabotage of victims' digital devices or online presence[33]. The increasing digitization of financial services and employment opportunities makes this form of abuse particularly concerning for victim safety and independence.

### B. Legal Challenges in Addressing Digital Abuse

The legal system faces numerous challenges in effectively addressing technology-facilitated intimate partner violence. These challenges stem from the unique characteristics of digital abuse, the rapid pace of technological change, and the limitations of traditional legal frameworks designed for physical forms of violence.

Jurisdictional issues present significant challenges for addressing digital abuse, particularly when perpetrators and victims are located in different jurisdictions or when abusive conduct

[31] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510-2522, 2701-2712, 3121-3127).
[32] C Southworth et al, "Intimate Partner Violence, Technology, and Stalking" (2007) 13(8) *Violence Against Women* 842–856.
[33] B A Harris, "Technology and Violence Against Women" in Nancy Lombard (ed), *Violence Against Women: Current Theory and Practice in Domestic Abuse, Sexual Violence and Exploitation* (Jessica Kingsley Publishers, London, 2015) 234–251.

occurs across multiple platforms and technologies. The global nature of digital communications and the cross-border operations of many technology platforms create complex jurisdictional questions that can impede effective legal intervention[34].

Evidence gathering and preservation in digital abuse cases require specialized knowledge and procedures that may not be available to all law enforcement agencies. Digital evidence is often fragile and easily destroyed or modified, requiring rapid response and specialized technical expertise. Additionally, the private nature of many digital communications and the use of encrypted platforms can create challenges for evidence collection while raising important privacy concerns[35].

The anonymity and pseudonymity available through digital technologies can make it difficult to identify perpetrators of digital abuse, particularly when sophisticated technical measures are employed to conceal identity. This challenge is compounded by the fact that many forms of digital abuse occur through platforms and services that may not maintain detailed user identification records[36].

### C. Impact on Victims and Legal Remedies

The impact of technology-facilitated intimate partner violence on victims extends far beyond the immediate harm caused by specific incidents of abuse. The pervasive nature of digital surveillance and harassment can create lasting psychological trauma, social isolation, and economic hardship that requires comprehensive legal remedies.

Victims of digital abuse often experience heightened levels of anxiety, depression, and post-traumatic stress compared to victims of traditional forms of intimate partner violence. The constant nature of digital surveillance and the ability of perpetrators to access victims remotely can eliminate safe spaces and create a sense of helplessness that traditional protective measures may not address[37].

[34] International Covenant on Civil and Political Rights, adopted 16 December 1966, 999 UNTS 171 (entered into force 23 March 1976), Art. 17.
[35] Convention on the Elimination of All Forms of Discrimination Against Women, adopted 18 December 1979, 1249 UNTS 13 (entered into force 3 September 1981).
[36] European Convention for the Protection of Human Rights and Fundamental Freedoms, opened for signature 4 November 1950, 213 UNTS 221 (entered into force 3 September 1953).
[37] U.S. Const. amend. IV.

Current legal remedies for digital abuse vary significantly across jurisdictions and may not adequately address the full range of harms experienced by victims. Restraining orders and protective orders, while valuable, may be difficult to enforce in digital contexts and may not address the ongoing availability of previously collected digital information[38]. Civil remedies, including tort claims for invasion of privacy and intentional infliction of emotional distress, may provide some recourse but often fail to address the specific harms associated with technology-facilitated abuse.

## VI. Surveillance Technologies and Legal Implications

### A. Types of Surveillance Technologies

The landscape of surveillance technologies relevant to intimate partner violence cases encompasses a broad range of tools and techniques, each with distinct legal implications and privacy concerns. Understanding these technologies is essential for developing appropriate legal frameworks that can address their legitimate uses while preventing abuse.

Communication surveillance technologies include tools for monitoring electronic communications such as emails, text messages, voice calls, and social media interactions. These technologies range from simple software applications that can be installed on shared devices to sophisticated systems capable of intercepting communications in real-time[39]. The legal implications of communication surveillance vary depending on factors such as consent, ownership of devices, and the specific technologies employed.

Location tracking technologies have become increasingly sophisticated and pervasive, with many devices and applications automatically collecting and storing location data. These technologies include GPS tracking in vehicles and mobile devices, location tracking through mobile applications, and monitoring through Internet of Things devices such as smart home systems[40]. The continuous nature of location tracking and the detailed behavioral patterns it can reveal raise significant privacy concerns that must be balanced against legitimate protective uses.

[38] Cal. Penal Code § 647(j)(4) (West 2019).
[39] Digital Personal Data Protection Act, 2023, No. 22 of 2023 (India).
[40] UN Women, *Technology-Facilitated Gender-Based Violence: A Growing Concern* (New York: United Nations Entity for Gender Equality and the Empowerment of Women, 2020).

Biometric surveillance technologies, including facial recognition, voice recognition, and behavioral biometrics, are increasingly being integrated into consumer devices and security systems. While these technologies can provide valuable security benefits, they also create opportunities for unauthorized surveillance and monitoring that may be exploited in intimate partner violence contexts[41].

### B. Legal Frameworks for Surveillance Authorization

The legal frameworks governing surveillance authorization in intimate partner violence cases must balance the need for effective investigation and protection with fundamental privacy rights and civil liberties. These frameworks typically establish procedures for obtaining legal authorization for surveillance activities, specify the circumstances under which surveillance may be conducted, and provide safeguards against abuse.

Warrant requirements represent the primary legal mechanism for authorizing surveillance activities in many jurisdictions. Traditional warrant standards, developed for physical searches and seizures, may require modification to address the unique characteristics of digital surveillance in intimate partner violence cases. The ongoing nature of abusive relationships and the need for immediate protective measures may require expedited warrant procedures and emergency authorization mechanisms[42].

Consent-based surveillance presents particular challenges in intimate partner violence contexts, where the power dynamics between victims and perpetrators may compromise the validity of consent. Legal frameworks must carefully address situations where devices or accounts are shared between intimate partners and establish clear standards for when surveillance consent is valid and when it may be compromised by coercion[43].

Third-party disclosure requirements govern law enforcement access to surveillance data held by private companies such as telecommunications providers, social media platforms, and

[41] Barocas, S. and Nissenbaum, H., "Big Data's End Run around Anonymity and Consent," in *Privacy, Big Data, and the Public Good: Frameworks for Engagement*, ed. Julia Lane et al. (Cambridge: Cambridge University Press, 2014), 44-75.
[42] Citron, D.K., "Sexual Privacy," *Yale Law Journal* 128, no. 7 (2019): 1870-1960.
[43] Fourth Amendment to the U.S. Constitution; see also Riley v. California, 573 U.S. 373 (2014).

device manufacturers. These requirements must balance law enforcement needs with privacy protections and may require specialized procedures for intimate partner violence cases[44].

### C. Emerging Technologies and Legal Adaptation

The rapid pace of technological development creates ongoing challenges for legal frameworks governing surveillance in intimate partner violence cases. Emerging technologies such as artificial intelligence, machine learning, and advanced data analytics create new capabilities for both protection and abuse that existing legal frameworks may not adequately address.

Artificial intelligence and machine learning technologies are increasingly being used to analyze large volumes of digital data to identify patterns of abuse and predict risk levels. While these technologies offer promising capabilities for victim protection, they also raise concerns about accuracy, bias, and privacy that require careful legal consideration[45].

The Internet of Things (IoT) represents a particularly significant challenge for legal frameworks, as the proliferation of connected devices creates numerous opportunities for surveillance and monitoring that may not be covered by existing legal protections. Smart home devices, wearable technology, and connected vehicles all create new vectors for both protective surveillance and abusive monitoring[46].

Blockchain and distributed technologies present both opportunities and challenges for addressing intimate partner violence. While these technologies may offer enhanced privacy protections and secure evidence storage, they may also create new opportunities for anonymous harassment and make law enforcement investigations more difficult[47].

## VII. Comparative Analysis of International Approaches

### A. European Union Approach

The European Union has developed one of the most comprehensive and rights-protective approaches to balancing digital surveillance capabilities with privacy protections. The EU framework is characterized by strong privacy rights, detailed procedural safeguards, and

[44] Carpenter v. United States, 138 S. Ct. 2206 (2018).
[45] European Court of Human Rights, *Big Brother Watch and Others v. the United Kingdom*, Judgment of 25 May 2021, Applications nos. 58170/13, 62322/14 and 24960/15.
[46] *Klass and Others v Germany* (1978) 6 EHRR 214.
[47] *Malone v the United Kingdom* (1984) 7 EHRR 14.

sophisticated balancing tests that could serve as a model for other jurisdictions addressing intimate partner violence.

The General Data Protection Regulation establishes fundamental principles for data processing that have significant implications for surveillance activities in intimate partner violence cases. The principles of data minimization, purpose limitation, and storage limitation require that surveillance activities be targeted, proportionate, and time-limited[48]. These principles help ensure that privacy intrusions are limited to what is necessary for legitimate protective purposes.

The EU's e-Evidence framework provides procedures for cross-border access to digital evidence that could be valuable for addressing intimate partner violence cases that involve multiple jurisdictions. These procedures include safeguards for fundamental rights and require coordination between law enforcement agencies and judicial authorities[49].

Recent EU legislation addressing online gender-based violence, including provisions in the Digital Services Act requiring platforms to address harmful content, demonstrates a comprehensive approach to technology-facilitated abuse that encompasses both regulatory measures and individual rights protections[50].

### B. United States Approach

The United States approach to digital surveillance in intimate partner violence cases reflects the country's federal system and the resulting patchwork of federal and state laws. This approach is characterized by varying levels of privacy protection, different procedural requirements across jurisdictions, and ongoing judicial development of surveillance standards. Federal legislation such as the Violence Against Women Act includes provisions addressing cyberstalking and digital harassment, but these provisions are primarily focused on criminal penalties rather than surveillance authorities[51]. The Electronic Communications Privacy Act provides a framework for government access to digital communications, but this framework

[48] Justice K.S. Puttaswamy (Retd.) v. Union of India, (2017) 10 SCC 1, para. 180.
[49] Regulation (EU) 2016/679 (General Data Protection Regulation), supra note 15, Arts. 5, 6.
[50] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services (Digital Services Act) [2022] OJ L277/1.
[51] Violence Against Women Act of 1994, supra note 18, § 40507.

was developed before modern digital surveillance technologies and may not adequately address contemporary challenges.

State-level approaches vary significantly, with some states developing comprehensive frameworks for addressing technology-facilitated intimate partner violence while others rely on traditional domestic violence laws that may not adequately address digital abuse[52]. This variation creates challenges for both victims and law enforcement, particularly in cases involving interstate activity.

Recent federal initiatives, including the Strengthening Online Abuse Resistance Act and other proposed legislation, demonstrate growing recognition of the need for comprehensive approaches to technology-facilitated gender-based violence[53]. However, comprehensive federal legislation addressing the full spectrum of digital surveillance issues in intimate partner violence cases remains under development.

### C. Asian Approaches

Asian jurisdictions have developed varying approaches to digital surveillance and intimate partner violence that reflect different legal traditions, cultural contexts, and technological capabilities. These approaches offer valuable insights into alternative frameworks for balancing surveillance capabilities with privacy protections.

Singapore has developed a comprehensive framework for addressing online harassment and cyberstalking that includes specialized procedures for obtaining surveillance authorities in intimate partner violence cases. The Protection from Harassment Act provides for expedited protective orders and includes provisions specifically addressing digital forms of abuse[54].

South Korea has implemented sophisticated approaches to technology-facilitated gender-based violence, including comprehensive legislation addressing digital sex crimes and unauthorized surveillance. The country's approach emphasizes victim protection while maintaining strong procedural safeguards for surveillance activities[55].

[52] N.Y. Penal Law § 240.30 (McKinney 2019) (aggravated harassment in the second degree).
[53] Strengthening Online Abuse Resistance Act, H.R. 5024, 117th Cong. (2021).
[54] Protection from Harassment Act 2014 (Singapore), c. 256A.
[55] Act on Special Cases Concerning the Punishment, etc. of Sexual Crimes (Sexual Violence Punishment Act), Act No. 15977 (S. Korea 2018).

Japan's approach to digital surveillance in intimate partner violence cases has evolved significantly in recent years, with new legislation addressing stalking behavior and digital harassment. The country's framework emphasizes prevention and early intervention while providing for enhanced surveillance capabilities in cases involving serious threats[56].

### D. Lessons from Comparative Analysis

The comparative analysis reveals several key insights that can inform the development of effective legal frameworks for addressing digital surveillance in intimate partner violence cases. First, comprehensive approaches that address the full spectrum of technology-facilitated abuse are more effective than piecemeal legislation addressing individual forms of digital harassment.

Second, strong procedural safeguards and judicial oversight are essential for maintaining the legitimacy and effectiveness of surveillance authorities. Frameworks that provide clear standards for surveillance authorization, regular review of surveillance activities, and robust appeal procedures are more likely to strike an appropriate balance between protection and privacy.

Third, international cooperation and harmonization of legal standards are increasingly important as digital abuse often involves cross-border activity and global technology platforms. Frameworks that facilitate international cooperation while maintaining strong privacy protections are essential for effective responses to technology-facilitated intimate partner violence.

## VIII. Recommendations and Legal Reforms

### A. Comprehensive Legislative Framework

Based on the analysis of current legal frameworks and international best practices, this research recommends the development of comprehensive legislation specifically addressing digital surveillance in intimate partner violence cases. This legislation should establish clear definitions of technology-facilitated abuse, provide specialized procedures for surveillance authorization, and include robust safeguards for privacy rights and civil liberties.

[56] Act on Regulation of Stalking Behavior, etc., Act No. 88 of 2021 (Japan).

The proposed framework should include specific definitions of digital stalking, unauthorized surveillance, image-based sexual abuse, and other forms of technology-facilitated intimate partner violence. These definitions should be sufficiently comprehensive to address current forms of abuse while remaining flexible enough to address emerging technologies and tactics[57]. Specialized surveillance authorization procedures should be established for intimate partner violence cases, including expedited procedures for emergency situations and provisions for ongoing surveillance in cases involving persistent threats. These procedures should include clear standards for determining when surveillance is necessary and proportionate, time limitations on surveillance activities, and regular review requirements[58].

The legislative framework should also establish clear standards for evidence collection and preservation in digital abuse cases, including specialized training requirements for law enforcement personnel and procedures for maintaining the integrity of digital evidence while protecting victim privacy[59].

### B. Judicial Oversight and Procedural Safeguards

Effective legal frameworks for digital surveillance in intimate partner violence cases require robust judicial oversight and procedural safeguards to prevent abuse and maintain public confidence in surveillance activities. These safeguards should be designed to account for the unique characteristics of intimate partner violence while maintaining fundamental protections for privacy rights and civil liberties.

Judicial authorization should be required for all non-consensual surveillance activities, with clear standards for determining when surveillance is justified and proportionate. Emergency authorization procedures should be available for situations involving imminent danger, but these procedures should include prompt judicial review and time limitations[60].

[57] Model legislation proposed in Law Commission of India, *Reforms in Criminal Laws*, Report No. 277 (New Delhi: Government of India, 2020), 145-162.
[58] Draft amendments to The Protection of Women from Domestic Violence Act, 2005, proposed by National Commission for Women (2022).
[59] Guidelines for Handling of Digital Evidence by Law Enforcement Agencies, Bureau of Police Research and Development (New Delhi: Ministry of Home Affairs, 2021).
[60] See Justice K.S. Puttaswamy (Retd.) v. Union of India, supra note 13, para. 180 (establishing the three-pronged test for privacy invasion).

Regular review of ongoing surveillance activities should be required, with provisions for terminating surveillance when it is no longer necessary or proportionate. This review should consider factors such as the effectiveness of surveillance in achieving protective objectives, the availability of less intrusive alternatives, and the impact of surveillance on victim privacy and autonomy[61].

Notification requirements should be established to ensure that subjects of surveillance are informed of surveillance activities when disclosure would not compromise ongoing investigations or victim safety. These notification requirements should include provisions for delayed notification when immediate disclosure would create safety risks[62].

### C. Technology Platform Responsibilities

The proposed legal framework should establish clear responsibilities for technology platforms and service providers in addressing technology-facilitated intimate partner violence. These responsibilities should include both proactive measures to prevent abuse and responsive measures to address abuse when it occurs.

Platforms should be required to implement design features that enhance user safety and prevent abuse, including privacy controls, blocking and reporting mechanisms, and tools for evidence preservation. These features should be designed with input from domestic violence experts and should be regularly updated to address emerging threats[63].

Platforms should also be required to provide specialized support for victims of intimate partner violence, including expedited response procedures for reports of abuse, assistance with evidence preservation, and coordination with law enforcement agencies when appropriate. This support should be provided by personnel with specialized training in intimate partner violence dynamics[64].

---

[61] Proposed Digital Evidence (Special Procedures) Rules, 2024, Ministry of Electronics and Information Technology (draft).
[62] Privacy by Design principles as articulated in Ann Cavoukian, *Privacy by Design: The 7 Foundational Principles* (Toronto: Information and Privacy Commissioner of Ontario, 2009).
[63] UN Women, *Technology-Facilitated Gender-Based Violence*, supra note 40, at 78-84.
[64] National Legal Services Authority, *Model Scheme for Legal Aid in Technology-Facilitated Gender-Based Violence Cases* (New Delhi: NALSA, 2023).

Clear standards should be established for platform cooperation with law enforcement investigations, including procedures for preserving and producing evidence while protecting user privacy. These standards should balance the need for effective law enforcement with platform responsibilities to protect user data and privacy[65].

**D. Victim Protection and Support Services**

The legal framework should include comprehensive provisions for victim protection and support services that address the unique needs of victims of technology-facilitated intimate partner violence. These services should be integrated with traditional domestic violence support services while addressing the specific challenges created by digital abuse.

Specialized legal assistance should be available to help victims navigate the complex legal issues associated with technology-facilitated abuse, including assistance with obtaining protective orders, preserving evidence, and addressing privacy violations. This assistance should be provided by attorneys with specialized training in both intimate partner violence and technology law[66].

Technical assistance should be available to help victims enhance their digital security and privacy, including assistance with device security, account protection, and safe communication technologies. This assistance should be provided by personnel with both technical expertise and understanding of intimate partner violence dynamics[67].

Economic support should be available to help victims address the financial impacts of technology-facilitated abuse, including assistance with device replacement, security measures, and lost income resulting from digital harassment. This support should be integrated with existing victim compensation programs while addressing the unique economic impacts of digital abuse[68].

[65] Regulation (EU) 2016/679 (General Data Protection Regulation), supra note 15, Arts. 15-22.
[66] Specialized legal aid provisions proposed in Draft Legal Services (Amendment) Bill, 2023.
[67] Digital security assistance programs as implemented in various states; see Ministry of Women and Child Development, *Guidelines for One Stop Centres* (New Delhi: Government of India, 2022), 45-48.
[68] Victim compensation schemes under The Criminal Law (Amendment) Act, 2013, s. 357A.

## IX. Conclusion

The intersection of digital surveillance technologies and intimate partner violence presents one of the most complex legal challenges of the modern era. The dual nature of these technologies—as both tools for protection and instruments of abuse—requires nuanced legal frameworks that can harness their protective potential while preventing their misuse. This research has demonstrated that current legal frameworks are inadequate to address the full spectrum of issues presented by technology-facilitated intimate partner violence and that comprehensive reform is necessary to protect victims while maintaining fundamental rights and freedoms.

The analysis reveals that effective legal frameworks must be built on several foundational principles. First, they must recognize the unique characteristics of intimate partner violence and the ways in which digital technologies amplify and extend traditional forms of abuse. Second, they must provide clear standards for balancing surveillance capabilities with privacy rights, ensuring that protective measures are proportionate, necessary, and time-limited. Third, they must include robust procedural safeguards and judicial oversight to prevent abuse and maintain public confidence in surveillance activities.

The comparative analysis of international approaches demonstrates that comprehensive frameworks addressing the full spectrum of technology-facilitated abuse are more effective than piecemeal approaches addressing individual forms of digital harassment. The European Union's rights-protective approach, with its emphasis on data minimization, purpose limitation, and procedural safeguards, provides a valuable model for other jurisdictions. However, this model must be adapted to address the specific challenges presented by intimate partner violence, including the need for immediate protective measures and the unique power dynamics between victims and perpetrators.

The recommendations presented in this research call for comprehensive legislative reform that establishes specialized procedures for surveillance authorization in intimate partner violence cases while maintaining robust protections for privacy rights and civil liberties. These reforms should include clear definitions of technology-facilitated abuse, specialized training for law enforcement personnel, enhanced responsibilities for technology platforms, and comprehensive support services for victims.

Looking forward, the legal system must remain adaptable to address emerging technologies and evolving forms of abuse. The rapid pace of technological development means that legal frameworks must be designed with sufficient flexibility to address new challenges while maintaining fundamental principles of proportionality, necessity, and accountability. This will require ongoing collaboration between legal experts, technology specialists, domestic violence advocates, and policymakers to ensure that legal frameworks remain effective and responsive to emerging threats.

The stakes of this challenge are high. Failure to develop effective legal frameworks for addressing technology-facilitated intimate partner violence risks leaving victims without adequate protection while potentially undermining fundamental privacy rights and civil liberties. Success requires careful calibration of competing interests and ongoing commitment to protecting both victim safety and individual rights.

The path forward requires recognition that perfect solutions may not exist—that the tension between protection and privacy may never be fully resolved. However, this should not prevent the development of improved frameworks that better balance these competing interests. The goal should be to develop legal frameworks that maximize protection for victims while minimizing unnecessary privacy intrusions, recognizing that this balance may need to evolve as technology and society continue to change.

Ultimately, addressing technology-facilitated intimate partner violence requires not only legal reform but also broader social change. Legal frameworks alone cannot eliminate gender-based violence or prevent the misuse of technology for abusive purposes. However, well-designed legal frameworks can provide essential tools for protection and accountability while maintaining the fundamental rights and freedoms that characterize democratic societies. The challenge for legal systems is to rise to this occasion and develop frameworks worthy of the trust placed in them by both victims seeking protection and citizens expecting their rights to be respected.