LEX LOCALIS-JOURNAL OF LOCAL SELF-GOVERNMENT
ISSN:1581-5374 E-ISSN:1855-363X
VOL. 23, NO. S6(2025)

THE DIGITAL EXTENSION OF COERCIVE CONTROL: SURVEY OF TECHNOLOGY'S ROLE IN DOMESTIC VIOLENCE

Pankaj[1], Dr. Reetika Bansal[2], Ms. Jessica Bansal[3], Mr. Rakesh[4], Mr. Mahesh Kumar[5], Mr. Anuj[6]

[1]Ph.D Research Scholar, Department of Law, Maharishi Markandeshwar (Deemed to be University) Mullana-Ambala, Haryana, India, and Additional District and Session Judge, District Court Solan, Himachal Pradesh, India
[2]Professor, Department of Law, Maharishi Markandeshwar (Deemed to be University) Mullana-Ambala, Haryana, India,
[3] Advocate, Panjab & Haryana High Court, Chandigarh, India
[4]Ph.D Research Scholar, Department of Law, Maharishi Markandeshwar (Deemed to be University) Mullana-Ambala, Haryana, India
[5]Ph.D Research Scholar, Department of Law, Maharishi Markandeshwar (Deemed to be University) Mullana-Ambala, Haryana, India
[6] Ph.D Research Scholar, Department of Law, Maharishi Markandeshwar (Deemed to be University) Mullana-Ambala, Haryana, India

pankaj_nk@yahoo.com[1]
bansalreetika80@gmail.com[2]
bansaljessica07@gmail.com[3]
shantidevi19781978@gmail.com[4]
soniadvmahesh@gmail.com[5]
Anujdhillon94@gmail.com[6]

Abstract: This review thoroughly examines the misuse of digital technologies within domestic violence contexts, particularly their role in enabling coercive control. It summarizes current research on the diverse forms of this digital harm, its global prevalence, and the deep psychological, economic, and physical impacts on the victims. The paper identifies critical challenges in existing intervention strategies, from legal frameworks to technological design. Further, this analysis emphasizes the urgent need for a multi-sectoral/party approach integrating ethical technological advancements, vigilant policy reforms, and comprehensive survivor centered appoach to effectively address this dangerously evolving and complex societal challenge.

Keywords: Domestic Violence; Coercive Control; Digital Technologies; Survivor Support; Policy Reform; Artificial Intelligence.

1. Introduction

The fast-paced growth of digital technology in this century has brought noticeable benefits to our society. It has made the world more connected, simplified our daily lives, and added richness to our experiences. But this technological progress also has a darker side. It has created issues for harm, especially in close personal relationships [1]. Tools that were originally designed to help us communicate, stay safe, and make life easier are now being misused by some people to control and harm their partners [2].

This dark digital aspect of intimate partner violence, frequently referred to as technology-facilitated abuse (TFA) or technology-facilitated domestic abuse (TFDA), has witnessed a rise in such incidents in recent years, posing severe and dangerous threats to the safety, privacy, and overall well-being and fundamental rights of individuals in relationships [3]. A critical aspect of this phenomenon is the illusive boundary between online and offline realities; harm initiated within

digital spaces frequently transcends virtual confines, resulting in dangers in physical environments, thereby making it challenging for victims to feel safe anywhere [3]. At its core, TFDA is deeply linked with obsessive control, a systematic pattern of behavior in order to dominate and isolate the victims, predominantly women [4]. Technology allows perpetrators a high level of access to personal information, including real-time location data, information about social media, and details of daily activities. This digital access also causes the inappropriate recording and sharing of intimate moments or acts of abuse, creating a persistent and repetitive threat of exposure and re-victimization. This extends the abuser's reach and control beyond the physical proximity, creating a constant digital shadow over the victim's life [4].

This comprehensive literature survey aims to analyze and summarize the state-of-the-art academic research on the abuse of technology in domestic violence. This survey provides an in-depth explanation of the fundamental definitions that relate to this field, forms of technology-facilitated abuse, global prevalence data, analysis of the impacts on survivors, and review the possible countermeasures. By integrating empirical data and findings from the literature, this survey provides an authoritative, evidence-based overview, highlighting critical observations, identifying emerging trends, and pointing towards significant research and policy loopholes to conceptualize future directions and strategies.

2. Conceptualizing Technology-Facilitated Abuse (TFA): Definitions and Frameworks

2.1. Defining Technology-Facilitated Abuse (TFA) and its Core Components

Technology-facilitated abuse (TFA) refers to the misuse of digital systems such as, smartphones, laptops, IoT devices, and online social media accounts to harass, control, or abuse individuals [1]. Common in domestic abuse contexts, TFA includes behaviors such as hacking, impersonation, sending inappropriate messages, and pervasive surveillance through digital techniques. Experts define TFA based on abuser’s behaviors, impact on victim, and the absence of consent, recognizing that abuse can occur beyond intimate relationships, involving groups or communities [4].

TFA's evolving nature and definitions hinder effective prevention, detection, and legal responses. The rapid pace of technological advancements outstrips stakeholders' ability to maintain a unified understanding, causing underreporting and inconsistent identification of abuse. This lack of clarity complicates legal frameworks and societal efforts to address TFA effectively.

2.2. Technology-Facilitated Coercive Control (TFCC) and its Relationship to Broader Coercive Control

Technology-facilitated coercive control (TFCC) is the use of digital tools to exert control over intimate partners [5], often as part of broader coercive behaviors typically by males against female victims. Unlike traditional intimate partner violence (IPV), TFCC leverages technology for harassment via social media, GPS/location stalking, unauthorized surveillance, threats through digital communication, hacking, impersonation, and illicit sharing of private content. Abusers may exploit children for surveillance purposes [5].

Digital devices allow abusers to maintain constant "omnipresence", intruding physical boundaries to monitor and control victims continuously [4]. This relentless digital oversight heightens victims' fear, paranoia, and hypervigilance, making it hard to feel safe even after leaving the relationship. TFCC’s unique nature demands specialized, tech-savvy interventions beyond conventional domestic violence responses [6].

2.3. Cyber Violence Against Women and Girls (CVAWG) as an Intersectional Phenomenon

Cyber violence against women and girls (CVAWG) is an intersectional form of violence, where gender combined with factors like age, ethnicity, sexual orientation, gender identity, disability, religion, and profession increase vulnerability. This "multiplicative effect" means that discrimination compounds digital harm, making certain groups more susceptible and sensitive [7]. Key factors include:

- Age: Young women face cyberbullying; older women are prone to identity theft [7]
- Ethnicity: Racial minority women face intense cyber violence.
- Sexual Orientation & Gender Identity: LBT and non-binary individuals face hate-motivated abuse [7], [8].
- Disability: Higher rates of online violence compared to non-disabled women [7].
- Religion: Discriminatory beliefs intensify cyber threats [7].
- Profession: Public figures, like journalists and lawmakers, face elevated online attacks [3], [7].

Addressing CVAWG requires intersectional policies that admits these diverse vulnerabilities. Inclusive tech design and culturally competent support are essential to avoid perpetuating systemic discrimination and abuse [3], [7], [8].

Table 1: Key Definitions and Conceptualizations of Technology-Facilitated Abuse

Term	Primary Definition	Key Components/Characteristics	Relevant Context
Technology-Facilitated Abuse (TFA) [1]	Misuse or repurposing of digital systems to harass, coerce, or abuse.	Perpetrator's behavior, victim's harm/impact, absence of consent. Can extend beyond intimate relationships.	Domestic abuse, intimate relationships, broader digital systems (phones, laptops, smart home/IoT, online accounts).
Technology-Facilitated Coercive Control (TFCC) [9]	Use of digital technologies to coercively control current or former intimate partners.	Occurs within broader coercive control patterns; includes physical/non-physical violence, ongoing strategies; aims to control and make victim feel inferior/dependent.	Intimate relationships (current or former partners).
Cyber Violence Against Women and Girls (CVAWG) [5]	Any act committed, assisted, aggravated, or amplified by ICTs or digital tools, resulting in or likely to result in physical, sexual,	Intersectional form of violence; patterns and vulnerability exacerbated by gender in combination with other factors (age, race, sexual orientation, disability, profession).	Digital spaces, online platforms, broader societal context of gender inequality.

	psychological, social, political, or economic harm, or other infringements of rights.		
Technology-Facilitated Abuse in Relationships (TAR) [10]	A patterned (or single) use of abusive or controlling behaviors in intimate relationships, enacted via digital mediums.	Engenders negative consequences (distress, fear); unique omnipresence and coercive control.	Intimate relationships (young adults).
Digital Coercive Control [7]	A pattern of behavior asserting influence and control over an individual's life through threats, dependence, isolation, intimidation, and/or physical violence, often leading to loss of self-worth and safety, mediated by technology.	Increasingly used instead of "domestic violence" to include non-cohabiting partners and non-physical abuse. Perpetrators often gain access through physical device access, password knowledge/coercion.	Intimate relationships (family or dating violence), violence from strangers weaponizing intimate information.

3. Modalities and Manifestations of Technology Abuse

Technology-facilitated abuse (TFA) takes various evolving forms, often overlapping and rooted in control and manipulation tactics outlined in frameworks like the Duluth Power & Control Wheel [11], [12].

Common Types and Tactics:

- Mobile & Social Media Abuse: Includes incessant calls/texts, public humiliation online, hacking, controlling digital accounts, and sexting coercion [3], [11].

- Image-Based Sexual Abuse (IBSA): Involves inappropriate sharing of sexual content, sextortion, and threats to manipulate victims [3], [11], [13], [14].
- Economic Abuse: Abusers control finances via online banking restrictions, employment abuse, and exploiting smart devices [11], [15].
- Emotional Abuse: Utilizes gaslighting through smart devices, humiliation, and psychological manipulation [11].
- Harassment & Intimidation: Persistent stalking, doxing, spoof calls, and online threats [3], [9], [11], [16].
- Device & Account Control: Includes hacking, password changes, and installing spyware on personal or children's devices [5], [9], [11].

TFA is interconnected with offline abuse, often leading to physical violence, highlighting the need for integrated legal and social interventions [3], [7], [17], [18].

- Tracking and Monitoring Technologies: Abusers exploit GPS, spyware, smart home devices, and children's gadgets for covert surveillance. Design flaws in IoT devices, like lack of access indicators, facilitate abuse, underscoring the need for "safety by design" in technology [5], [9], [11], [18].
- Emerging Forms of Abuse [3], [15], [19], [20]:
  - AI & Deepfakes: Used for reputational harm and coercion.
  - Smart Devices: Weaponized for eavesdropping, economic control, and surveillance [21].
  - Online Misogyny: The "manosphere" fosters harmful narratives that normalize abuse [3].

Addressing TFA requires ethical technology development, proactive policies, and cross-disciplinary collaboration to protect victims and mitigate both online and offline harm.

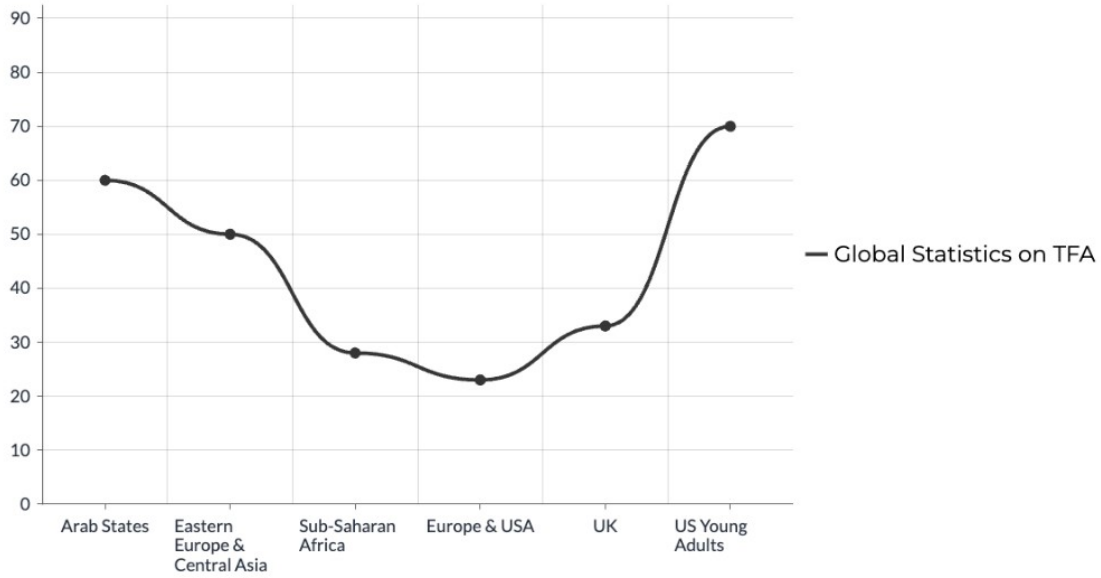

Figure 1: Graphical Depiction of Technology Assisted Abuse.

4. Prevalence and Demographics

4.1. Global and Regional Statistics on TFA

Technology-facilitated abuse (TFA) is alarmingly prevalent, affecting 99.3% of gender-based violence cases according to a 2020 Australian survey [16]. Globally, 16% to 58% of women experience TFA. Regional data highlights its widespread impact [3]:

- Arab States: 60% of women internet users report online violence.
- Eastern Europe & Central Asia: Over 50% of women aged 18+ face TFA.
- Sub-Saharan Africa: 28% of women report online abuse.
- Europe & USA: 23% of women aged 18–55 have experienced online harassment.
- UK: 1 in 3 women face social media abuse; 1 in 6 suffer from partner-related online abuse.
- US Young Adults: 70% report TFA; 40% of college students have faced cyber abuse.

Despite high prevalence, TFA is underreported due to stigma, shame, and systemic minimization, creating a feedback loop that hinders data collection, awareness, policy-making, and support services [22].

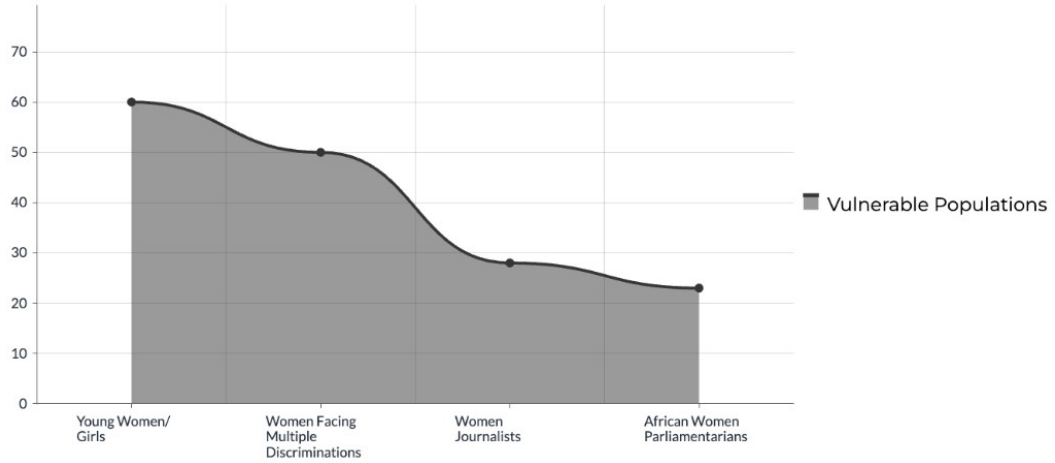

Figure 2: Vulnerable Populations due to online and offline abuse.

Vulnerable Populations [3]:

- Young Women/Girls: 58% face online harassment due to high tech usage.
- Women Facing Multiple Discriminations: Includes women with disabilities, women of color, migrants, and LGBTIQ+ individuals, who experience compounded abuse.
- Public Figures: 73% of women journalists and 58% of African women parliamentarians report online violence, leading to self-censorship and reduced public participation.

Marginalized groups often bear higher financial costs from TFA, with technology amplifying social inequalities [23]. Culturally competent, inclusive interventions are necessary to address the "digital divide" and ensure equitable protection and support for at-risk populations.

Table 2: Reported Prevalence Rates of Technology-Facilitated Violence by Region and Demographic

Category	**Prevalence/Statistics**
Overall Prevalence	Occurs in 99.3% of gender-based violence situations (Australia, 2020) [16].
	Between 16% and 58% of women globally have experienced technology-facilitated violence [16].
	7 in 10 young adults reported experiencing technology-facilitated abuse [3].
	Nearly three-quarters of respondents reported experiencing cyber aggression

	victimization in intimate relationships in the past year [3].
	Overall prevalence of cyber abuse victimization in a college student sample was 40% [17].
Regional Breakdown	Arab States: 60% of women internet users experienced online violence [16].
	Eastern Europe & Central Asia: >50% of women over 18 experienced some TFA (12 countries) [16].
	Sub-Saharan Africa: 28% of women experienced online violence (5 countries) [16].
	Europe & USA: 23% of women aged 18-55 reported at least one online abuse/harassment experience (8 countries) [16].
	United Kingdom: 1 in 3 women experienced online abuse (Refuge, 2021) [16], [17].
	United Kingdom: 1 in 6 women experienced online abuse from current/ex-partner (Oct 2021 national survey) [16], [24].
Demographics at Higher Risk	Young Women & Girls: 58% experienced some form of online harassment globally [16], [17].
	Women Facing Multiple Forms of Discrimination: Higher risks for women with disabilities, Black/Indigenous women, other women of color, migrant women, LGBTIQ+ people [16], [17].
	Women in Political & Public Life: 73% of women journalists experienced online violence; 58% of African women parliamentarians experienced online attacks [16], [17], [24].
	Demographics with Higher Financial Costs from TFA: Older age, non-Hispanic Black/African American, Hispanic/Latino/a/x, sexual/gender minority [17], [24].

5. Impacts on Survivors

The abuse of technology in domestic violence inflicts profound and multifaceted harms on survivors, extending across psychological, emotional, economic, and physical domains. These impacts are often lasting, complex, and wide-ranging, creating a pervasive environment of vulnerability.

5.1. Psychological and Emotional Harms

Technology-facilitated abuse in relationships (TAR) leads to severe, lasting physical, emotional, and mental health harms, including anxiety, depression, PTSD, and suicidal thoughts [6]. These issues are three to five times more common among survivors of intimate partner violence (IPV) [25]. The "spaceless 24/7 nature" of digital devices allows perpetrators to exert constant, invasive control, intensifying fear and distress [18], [26].

This digital "omnipresence" erodes survivors' sense of privacy and safety, affecting personal devices, home environments, and online presence [4]. Unlike traditional abuse limited by physical boundaries, technology makes the abuser's influence inescapable, fostering chronic stress and hindering psychological recovery [6]. Effective interventions must address not just overt abuse but

also the psychological impact of digital surveillance, emphasizing digital hygiene, privacy management, and tailored psychological support.

5.2. Economic and Financial Burdens

Technology-facilitated abuse (TFA) imposes significant, long-term economic impacts on survivors. Nearly 18.2% of U.S. young adult TFA survivors reported direct financial losses, with median costs of $900, often due to fraud, technology-related expenses, and housing costs [15]. Digital-financial abuse exploits technology to control financial independence, frequently co-occurring with other tech-based gender violence—affecting 78% of survivors [23]. Tactics include spending restrictions, stalking, blackmail, and threats, jeopardizing employment and credit.

Beyond financial losses, TFA leads to mental health costs; 11.3% of survivors sought counseling (~$6,228 per person), and 11.6% used prescribed medications for an average of 37.4 weeks. Factors like older age, minority status, and LGBTQ+ identity correlate with higher costs [15], [23].

TFA's economic and psychological impacts form a vicious cycle, where financial insecurity fosters mental distress, increasing recovery costs [23]. Effective interventions require integrated support—combining financial literacy, economic empowerment, tech safety, and mental health resources—while addressing the specific vulnerabilities of marginalized groups [11].

5.3. Physical Safety Risks and Offline Consequences

Online abuse extends beyond the digital realm, endangering women's safety in homes, workplaces, and public spaces [3]. Acts like doxing and deepfake abuse lead to real-life consequences such as stalking, threats, and reputational harm. GPS tracking exacerbates these risks, blurring the line between online and offline threats. Research shows technology-facilitated abuse often coincides with in-person violence, eroding the concept of safe spaces. Traditional interventions focusing solely on physical safety are insufficient. Effective strategies now require integrated digital and physical safety planning, emphasizing privacy management and recognizing that true security demands protection in both realms [17], [18].

6. Responses and Countermeasures

Addressing the complex and evolving landscape of technology-facilitated abuse requires a multi-pronged approach, encompassing effective digital interventions, proactive safety-by-design principles for technology, robust legal and policy frameworks, and comprehensive support mechanisms for survivors.

6.1. Effectiveness of Digital Interventions and Safety Planning Tools

Research highlights the effectiveness of digital interventions in supporting intimate partner violence (IPV) survivors [27]. Utilizing mobile apps, text messaging, web platforms, and virtual reality, these tools offer social and emotional support, enhance safety planning, provide psychoeducation, aid evidence documentation, and improve mental health outcomes [28].

The myPlan app, grounded in decision-making science and risk assessment, exemplifies such tools. It aids survivors in making safe decisions privately, reducing decisional conflict, increasing safety strategy use, and promoting the safe termination of dangerous relationships [29]. Similarly, the Internet Safety Decision Aid significantly reduces safety-related decisional conflict after just one use. These digital tools are crucial for bridging gaps in traditional IPV support services, especially for those facing access barriers [22], [30], [31].

6.2. Technological Countermeasures and "Safety by Design" Principles

To mitigate technology-based intimate partner violence (IPV), adopting "safety by design" principles is essential [15]. These principles embed protective features into technology to empower victims and limit attackers [32], [33].

Key Countermeasures for remediating the root cause [33], [34]:

- Authentication Systems: Implement non-modifiable device access logs, secure recovery methods, clear access notifications, and approval mechanisms for new devices or locations.
- Media Control: Ensure quick removal of non-consensual media, prevent reposts via detection mechanisms, and provide confidential reporting tools.
- Social Media: Develop robust blocking systems extending to linked accounts and enforce privacy settings for messaging controls.
- Browser Privacy: Default to automatic deletion of browsing history and metadata to prevent surveillance.
- End-to-End Encryption: Make this standard for secure communications.
- Gender-Sensitive Design: Address structural inequalities to support victims' needs.
- Local Security: Design applications to resist attacks from individuals with physical access.
- Detection Tools: Create IPV-specific algorithms to identify abusive patterns and enhance activity monitoring.
- Plausible Deniability & Transparency: Support victims with features for plausible deniability, improved logging, and transparent reporting.

Addressing Digital Coercive Control: IPV perpetrators often exploit physical access and intimate knowledge, bypassing traditional security. Thus, "safety by design" must address these unique internal threats, focusing on user interface vulnerabilities over technical exploits [34].

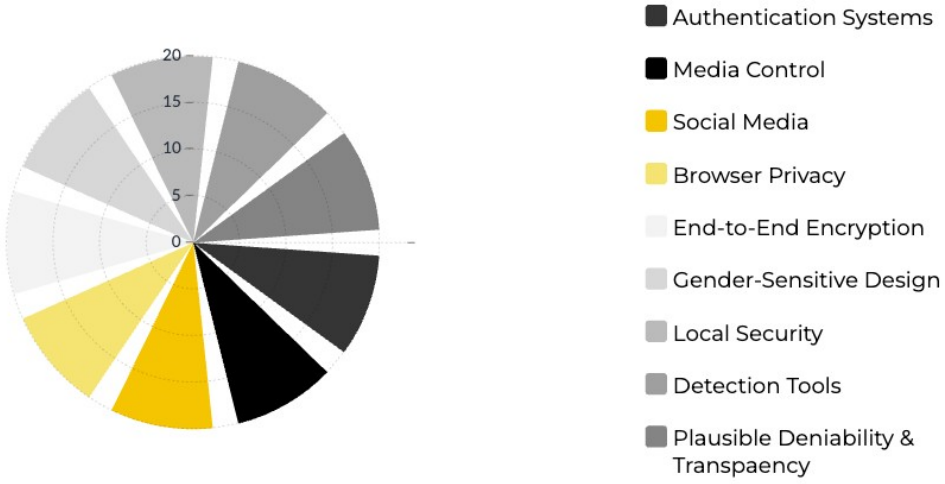

Figure 3: Key Countermeasures for remediation.

6.3. Legal and Policy Frameworks

The legal and policy landscape addressing technology-facilitated domestic violence is complex, characterized by both existing statutes and significant gaps that hinder effective prosecution and victim protection.

6.4. Current Legal Landscape and Application

Current U.S. laws, particularly stalking and cyberstalking statutes, can potentially apply to IoT-facilitated domestic violence. Federally, the Interstate Stalking Punishment and Prevention Act (18 U.S.C. § 2261A), amended in 2013, criminalizes intent to "harass... or place under surveillance"

and includes causing "substantial emotional distress" via "any electronic communication system". While not explicitly used for IoT abuse, its language suggests potential applicability to networked devices. At the state level, all fifty states criminalize stalking, with some recognizing cyberstalking as a distinct crime or incorporating it into general stalking statutes [35].

6.5. Limitations and Gaps in Application

Despite existing laws, IoT-facilitated abuse faces legal gaps. Many statutes don't explicitly cover networked devices, leaving harassment claims vulnerable if abuse appears as mere device interaction [35]. Physical threat or direct communication requirements often exclude indirect IoT abuses like remote thermostat manipulation [35]. Tort law definitions of "surveillance" may overlook in-home monitoring, common with IoT.

Evidentiary issues are significant proof often exists only on the abuser's device or online, challenging for survivors to access. Law enforcement lacks resources and training, sometimes relying on invasive survivor data. Jurisdictional issues arise from cyberspace's borderless nature, and First Amendment concerns complicate online regulation, though exceptions exist for "true threats." Additionally, law enforcement may downplay nonphysical abuse, and narrow legal definitions of domestic violence hinder recognizing coercive control through technology [3], [35].

6.6. Challenges in Prosecution of Digital Evidence

Prosecutors and investigators face key challenges with digital evidence in criminal cases due to rapid technological changes and privacy concerns. The evolving nature of digital data, the volume and complexity involved, and outdated forensic tools complicate evidence reliability and courtroom presentation [36]. Proprietary forensic tools, often "black boxes," hinder transparency, and AI's complexity adds further difficulties. Plea bargains limit courtroom scrutiny of these tools.

Privacy issues also pose hurdles: digital evidence has a fragile chain of custody, prosecutors may struggle with data relevance, and obtaining third-party information can be slow due to provider resistance. Risks include misinterpretation of data and missing exculpatory evidence. Additionally, legislation often lags behind technology, causing legal inconsistencies [36].

6.7. Policy Recommendations and Legislative Gaps

Policy recommendations call for urgent legal and systemic reforms to address online abuse as a harmful form of domestic abuse. This includes robust sanctions, victim protection without blame, and parity between online and offline protections. Laws must be strengthened for image-based sexual abuse, ensuring victim anonymity, and restraining orders should explicitly cover online abuse with breaches criminalized [37].

Online providers need to enhance abuse prevention, offer clear guidelines, and train law enforcement on product-related risks. Collaboration with specialist services is essential for safety assessments and effective crime response. Police should integrate online abuse into domestic abuse strategies, supported by adequate training and resources [37]. Victim support requires sustainable funding and online provider involvement, while education on online abuse and healthy relationships is vital [3].

Legislative reforms must address outdated laws, unclear criminal definitions, and insufficient penalties. Strong statutory provisions are needed to reflect the true impact of these crimes. Key issues include the absence of automatic online restrictions in protective orders, limited anonymity for perpetrators, and inadequate definitions of image-based sexual abuse. Action is needed to shut down sites profiting from such abuse.[25], [37].

6.8. Challenges in Criminal Justice Response

The criminal justice system faces key challenges in addressing cyber violence against women and girls. Data collection at the EU level is limited, lacking longitudinal trends and national surveys. Even where offenses are criminalized, data often isn't disaggregated by victim/perpetrator sex or relationship, hindering gender analysis. Legal frameworks lack EU-wide definitions and fail to capture the social and psychological impacts of digital abuse. Enforcement is weak; in the UK, 61% of revenge porn cases saw no further action. Police often view online abuse as isolated incidents, ignoring behavioral patterns, and tend to downplay cyber violence compared to offline abuse. Victim-blaming attitudes, especially in revenge porn cases, highlight gaps in authority understanding [38].

6.9. Support Mechanisms and Advocacy Programs

Support mechanisms for survivors of technology-facilitated abuse now include traditional resources like hotlines and advocacy centers, alongside innovative tech solutions. AI chatbots such as Aimee and Sophia help recognize abuse, guide next steps, and provide multilingual resources, complementing human support [39]. Virtual reality (VR) aids in fostering empathy and behavior training for perpetrators by simulating survivors' experiences [40].

These digital tools prioritize privacy, data security, and user safety, with features like quick exit buttons and minimal data storage. Ethical design and multi-stakeholder collaboration among researchers, practitioners, and policymakers are key to effective, comprehensive responses [21], [22].

7. Research Gaps and Future Directions

Despite a growing body of literature on technology-facilitated abuse, several significant research gaps persist, hindering a comprehensive understanding and effective response to this evolving phenomenon. Addressing these gaps is crucial for informing future interventions, policy development, and technological innovation.

7.1. Current Gaps

There is a lack of longitudinal research on the co-occurrence and interaction between online and offline intimate partner violence. While early findings indicate online abuse may precede face-to-face aggression, more studies are needed to clarify causal links.

Understanding the scale and forms of technology-facilitated violence, particularly its impact on women facing multiple discriminations, remains limited. Challenges include inconsistent definitions, global jurisdiction issues, and privacy concerns in data collection. Additionally, data often focuses on the Global North, limiting cultural relevance of interventions elsewhere.

Increased funding is crucial for expert-led technology safety scans, as current reliance on non-specialists undermines efficacy. This gap extends to frontline workers' awareness, leading to under-recognition of technology-facilitated coercive control and misinterpretation of abuse patterns by police, heightening risks for victim-survivors.

7.2. Emerging Issues

The rapid advancements in artificial intelligence (AI) present both new challenges and opportunities. While AI can be weaponized to create sophisticated forms of abuse like deepfakes, it also holds potential for predictive analytics in identifying domestic violence risk factors and developing AI-assisted interventions. However, the ethical implications of AI, including privacy concerns, data bias, and the potential for technological exploitation, require careful consideration. The expansion of the "manosphere," an ecosystem of misogynistic content seeping into

mainstream culture, is another emerging challenge that shapes public attitudes and contributes to online violence.

7.3. Future Research Directions

Future research should focus on longitudinal studies to determine if online experiences predict offline violence and their impact on victims, guiding potential interventions. Developing inclusive algorithms and expanding cross-cultural datasets are crucial for equitable AI solutions. Additionally, integrating AI into public health and social services is vital for domestic violence prevention.

Ongoing studies aim to create AI tools to help IPV survivors manage technology-enabled cognitive security risks, complementing traditional support. Research should also explore victims' resistance to tech-facilitated abuse and digital platforms addressing survivors' housing needs. Understanding young adults' digital communication habits is key to enhancing IPV services for this group.

8. Conclusion

Technology has significantly reshaped domestic violence, with technology-facilitated abuse (TFA) becoming a prevalent, rapidly growing aspect of intimate partner violence. TFA includes digital monitoring, social media harassment, image-based abuse, economic exploitation, and smart device manipulation, blurring online and offline harm.

The fragmented understanding of TFA across disciplines hampers consistent responses, leading to underreporting and inadequate systemic support. TFA disproportionately impacts young women, women of color, LGBTIQ+ individuals, and public figures, exacerbating psychological harm like anxiety, depression, and PTSD through constant digital surveillance.

However, technology also offers solutions. Digital safety tools and "safety by design" principles can enhance survivor protection. Yet, legal frameworks often lag behind, with outdated definitions and enforcement challenges.

Key strategies to combat TFA such as, Unified Conceptualization and Data Collection, Proactive "Safety by Design", Legal and Policy Reforms, Integrated Support Services, Ethical AI and Continuous Research. Addressing these areas can ensure technology protects and empowers, rather than perpetuates abuse.

9. References:

[1] “Reaching a consensus: Technology-facilitated abuse conceptualisation, definition, terminology, and measurement,” *City Vision*. Available: https://vision.city.ac.uk/news/reaching-a-consensus-technology-facilitated-abuse-conceptualisation-definition-terminology-and-measurement/. [Accessed: Jun. 01, 2025]

[2] “Tech Abuse Awareness,” *NARIKA*, Nov. 01, 2017. Available: https://www.narika.org/tech-abuse-awareness. [Accessed: Jun. 01, 2025]

[3] “FAQs: Digital abuse, trolling, stalking, and other forms of technology-facilitated violence against women,” *UN Women – Headquarters*, Feb. 10, 2025. Available: https://www.unwomen.org/en/articles/faqs/digital-abuse-trolling-stalking-and-other-forms-of-technology-facilitated-violence-against-women. [Accessed: Jun. 01, 2025]

[4] K. Brookfield, R. Fyson, and M. Goulden, “Technology-Facilitated Domestic Abuse: An under-Recognised Safeguarding Issue?,” *Br. J. Soc. Work*, vol. 54, no. 1, pp. 419–436, Jan. 2024, doi: 10.1093/bjsw/bcad206

[5] "Technology-facilitated coercive control." Available: https://aifs.gov.au/resources/practice-guides/technology-facilitated-coercive-control. [Accessed: Jun. 01, 2025]
[6] "Fear and Distress: How Can We Measure the Impact of Technology-Facilitated Abuse in Relationships?" Available: https://www.mdpi.com/2076-0760/13/1/71. [Accessed: Jun. 01, 2025]
[7] "Combating Cyber Violence against Women and Girls," Nov. 2022, Available: https://eige.europa.eu/publications-resources/publications/combating-cyber-violence-against-women-and-girls?language_content_entity=en
[8] E. A. Mumford, P. Maitra, J. Sheridan, E. F. Rothman, E. Olsen, and E. Roberts, "Technology-facilitated abuse of young adults in the United States: A latent class analysis," *Cyberpsychology J. Psychosoc. Res. Cyberspace*, vol. 17, no. 3, Art. no. 3, Jun. 2023, doi: 10.5817/CP2023-3-7. Available: https://cyberpsychology.eu/article/view/21041. [Accessed: Jun. 01, 2025]
[9] "Technology-facilitated Abuse | Columbia Health." Available: https://www.health.columbia.edu/content/technology-facilitated-abuse. [Accessed: Jun. 01, 2025]
[10] "Technology-facilitated violence against women: Taking stock of evidence and data collection," *UN Women – Headquarters*, Sep. 19, 2024. Available: https://www.unwomen.org/en/digital-library/publications/2023/04/technology-facilitated-violence-against-women-taking-stock-of-evidence-and-data-collection. [Accessed: Jun. 01, 2025]
[11] M. M. Rogers, C. Fisher, P. Ali, P. Allmark, and L. Fontes, "Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review," *Trauma Violence Abuse*, vol. 24, no. 4, pp. 2210–2226, Oct. 2023, doi: 10.1177/15248380221090218
[12] "Power & Control Wheel - C.A. Goldberg." Available: https://www.cagoldberglaw.com/resources/power-control-wheel/. [Accessed: Jun. 01, 2025]
[13] "Online and digital abuse," *Women's Aid*. Available: https://www.womensaid.org.uk/information-support/what-is-domestic-abuse/online-safety/. [Accessed: Jun. 01, 2025]
[14] "Technology-Facilitated Gender-Based Violence | Office for the Prevention of Domestic Violence." Available: https://opdv.ny.gov/technology-facilitated-gender-based-violence. [Accessed: Jun. 01, 2025]
[15] "Technology-Facilitated Economic Abuse: Addressing the Digital Impact on Survivors – CCFWE." Available: https://ccfwe.org/2024/12/12/technology-facilitated-economic-abuse-addressing-the-digital-impact-on-survivors/. [Accessed: Jun. 01, 2025]
[16] "Technology-Facilitated Gender-Based Violence," *Office for the Prevention of Domestic Violence*. Available: https://opdv.ny.gov/technology-facilitated-gender-based-violence. [Accessed: Jun. 01, 2025]
[17] A. Marganski and L. Melander, "Intimate Partner Violence Victimization in the Cyber and Real World: Examining the Extent of Cyber Aggression Experiences and Its Association With In-Person Dating Violence," *J. Interpers. Violence*, vol. 33, no. 7, pp. 1071–1095, Apr. 2018, doi: 10.1177/0886260515614283
[18] R. Ronzón-Tirado, R. Charak, I. Cano-Gonzalez, S. Karsberg, and P. W. Schnarrs, "Latent Classes of Bidirectional Face-to-Face and Cyber Intimate Partner Violence Among Lesbian,

Gay, and Bisexual Emerging Adults: The Role of Minority Stressors," *J. Interpers. Violence*, vol. 37, no. 21–22, pp. NP21092–NP21118, Nov. 2022, doi: 10.1177/08862605211055158

[19] I. B. Ibiso, E. F. OJo, O. A. Ogunkorede, and A. S. Afolalu, "AI-Powered Predictive Analytics for Identifying Domestic Violence Risk Factors Across Cultures- An Overview," *ABUAD J. Eng. Res. Dev. AJERD*, vol. 8, no. 1, Art. no. 1, Mar. 2025, doi: 10.53982/ajerd.2025.0801.20-j

[20] L. Christie and S. Wright, "Technology and domestic abuse," Nov. 2020, Available: https://post.parliament.uk/technology-and-domestic-abuse/. [Accessed: Jun. 01, 2025]

[21] "New Resource for Domestic Abuse Survivors Combines AI, Cybersecurity, and Psychology | News Center." Available: https://news.gatech.edu/news/2023/09/27/new-resource-domestic-abuse-survivors-combines-ai-cybersecurity-and-psychology. [Accessed: Jun. 01, 2025]

[22] "Bridging the Gap: How AI and Tech Can Support Domestic Violence Advocacy - Non Profit News | Nonprofit Quarterly." Available: https://nonprofitquarterly.org/bridging-the-gap-how-ai-and-tech-can-support-domestic-violence-advocacy/. [Accessed: Jun. 01, 2025]

[23] J. Sheridan-Johnson, E. A. Mumford, E. A. Moschella-Smith, P. Maitra, D. B. Rein, and E. F. Rothman, "Economic Impacts of Technology-Facilitated Abuse Among U.S. Young Adults," *J. Interpers. Violence*, p. 8862605241305146, Dec. 2024, doi: 10.1177/08862605241305146

[24] C. Wolford-Clevenger *et al.*, "An Examination of the Partner Cyber Abuse Questionnaire in a College Student Sample," *Psychol. Violence*, vol. 6, no. 1, pp. 156–162, Jan. 2016, doi: 10.1037/a0039442

[25] "Technology-facilitated abuse: Interviews with victims and survivors and perpetrators," *ANROWS - Australia's National Research Organisation for Women's Safety*. Available: https://www.anrows.org.au/publication/technology-facilitated-abuse-interviews-with-victims-and-survivors-and-perpetrators/. [Accessed: Jun. 01, 2025]

[26] G. Macassa *et al.*, "Men's Experiences of Psychological and Other Forms of Abuse in Intimate Relationships: A Qualitative Study," *Societies*, vol. 15, no. 1, Art. no. 1, Jan. 2025, doi: 10.3390/soc15010017

[27] C. Emezue, J. D. Chase, T. Udmuangpia, and T. L. Bloom, "Technology-based and digital interventions for intimate partner violence: A systematic review and meta-analysis," *Campbell Syst. Rev.*, vol. 18, no. 3, p. e1271, Aug. 2022, doi: 10.1002/cl2.1271

[28] C. Emezue and T. L. Bloom, "PROTOCOL: Technology-based and digital interventions for intimate partner violence: A meta-analysis and systematic review," *Campbell Syst. Rev.*, vol. 17, no. 1, p. e1132, Jan. 2021, doi: 10.1002/cl2.1132

[29] "Our story and the science of safety," *myPlan*. Available: https://myplanapp.org/en/our-story. [Accessed: Jun. 01, 2025]

[30] K. B. Eden *et al.*, "Use of online safety decision aid by abused women: effect on decisional conflict in randomized controlled trial," *Am. J. Prev. Med.*, vol. 48, no. 4, pp. 372–383, Apr. 2015, doi: 10.1016/j.amepre.2014.09.027

[31] V. Hui, B. Zhang, B. Jeon, K. C. A. Wong, M. L. Klem, and Y. J. Lee, "Harnessing Health Information Technology in Domestic Violence in the United States: A Scoping Review," *Public Health Rev.*, vol. 45, p. 1606654, Jun. 2024, doi: 10.3389/phrs.2024.1606654

[32] "'Safety by design' could prevent domestic abuse through smart devices - Binding Hook." Available: https://bindinghook.com/articles-binding-edge/safety-by-design-could-prevent-domestic-abuse-through-smart-devices/. [Accessed: Jun. 01, 2025]
[33] S. Celi, J. Guerra, and M. Knodel, "Intimate Partner Violence Digital Considerations," Internet Engineering Task Force, Internet Draft draft-irtf-hrpc-ipvc-01, Nov. 2024. Available: https://datatracker.ietf.org/doc/draft-irtf-hrpc-ipvc-01. [Accessed: Jun. 01, 2025]
[34] J. Slupska and A. Strohmayer, "Networks of Care: Tech Abuse Advocates' Digital Security Practices," presented at the 31st USENIX Security Symposium (USENIX Security 22), 2022, pp. 341–358. Available: https://www.usenix.org/conference/usenixsecurity22/presentation/slupska-networks. [Accessed: Jun. 01, 2025]
[35] "A Domestic Violence Dystopia: Abuse via the Internet of Things and Remedies Under Current Law," *California Law Review*. Available: https://www.californialawreview.org/print/a-domestic-violence-dystopia-abuse-via-the-internet-of-things-and-remedies-under-current-law. [Accessed: Jun. 01, 2025]
[36] C. M. Miller, "A survey of prosecutors and investigators using digital evidence: A starting point," *Forensic Sci. Int. Synergy*, vol. 6, p. 100296, Dec. 2022, doi: 10.1016/j.fsisyn.2022.100296
[37] L. Hadley, "Tackling domestic abuse in a digital age," *Recomm. Rep. Online Abuse -Party Parliam. Group Domest. Violence*, 2017.
[38] "Cyber violence against women and girls | European Institute for Gender Equality," Jun. 23, 2017. Available: https://eige.europa.eu/publications-resources/publications/cyber-violence-against-women-and-girls?language_content_entity=en. [Accessed: Jun. 01, 2025]
[39] "Victim Advocacy | Cornell Health." Available: https://health.cornell.edu/services/victim-advocacy. [Accessed: Jun. 01, 2025]
[40] "Homepage," *National Sexual Violence Resource Center*. Available: https://www.nsvrc.org/homepage. [Accessed: Jun. 01, 2025]