TECHNOLOGICALLY FACILITATED VIOLENCE: CRIMINOLOGICAL ASPECTS OF TECHNOLOGY ABUSE IN FAMILY AND INTIMATE RELATIONSHIPS

Elena Maksimova[1]**, PhD**
Faculty of Law, Goce Delcev University, Stip, North Macedonia

ABSTRACT

Purpose: The purpose of this paper is to analyze the growing phenomenon of technologically facilitated violence (TFV) in the context of family and intimate partner relationships. Technology has slowly penetrated every pore of social life, so no matter how much it facilitates everyday life, it inevitably becomes an integral part of human deviant behavior. The study aims to discover how digital tools are used to exercise psychological, emotional, and coercive control over victims and to explore the criminological implications of this new form of abuse. Technology can leave room for new forms of violence but also help in carrying out existing ones. Therefore, the main goal is to investigate new trends in the abuse of technological and digital opportunities in this direction. A special focus will be placed on the Republic of North Macedonia, the emerging forms, cases, and legal amendments that will be considered to determine the extent to which they offer protection from this phenomenon.

Design/Methods/Approach: The research employs a qualitative criminological approach supported by legal analysis. It draws on secondary data from academic literature, international documents, and reports, alongside selected case studies and statistics from national stakeholders. Macedonian criminal law is critically examined to identify legislative gaps, while practices from developed countries and trends are reviewed as models for reform.

Findings: The study identifies several key forms of technology abuse in intimate settings, including cyberstalking, online tracking, control via social media or smart home devices, etc. It highlights how these acts often remain invisible to traditional legal definitions of violence and are frequently underreported. The paper finds that existing criminal law provisions in North Macedonia offer limited direct protection against TFV and that there is an urgent need for digital-specific legal mechanisms, institutional training, and cross-sectoral coordination.

Originality/Value: This paper contributes to the limited regional scholarship on technology-facilitated domestic abuse by providing a criminological lens to a globally emerging issue. It emphasizes the importance of recognizing digital abuse as a legitimate and serious form of victimization and offers evidence-based recommendations for legal and institutional reform, especially in the context of harmonizing national legislation.

Keywords: Technology-facilitated violence, intimate partner abuse, cyberstalking, criminology, gender-based violence, North Macedonia, domestic violence.

1 elena.maksimova@ugd.edu.mk

About the author

Elena Maksimova is an associate professor in Criminal Law and Criminology, University Goce Delcev – Stip. Maksimova has finished her Bachelor, LL.M, and PhD studies at the Faculty of Law "Iustinianus Primus", Ss. Cyril and Methodius University in Skopje. Her narrower fields of interest are crimes committed by women, domestic and gender-based violence, and the migrant crisis and its criminological aspects, participating in a series of international projects with a group of researchers, analysing the criminological consequences of the crisis. Elena Maksimova has attended plenty of conferences, seminars, and trainings. She has also been included in a few projects and has many publications as an author or coauthor in national and international journals.

INTRODUCTION: ABOUT THE TECHNOLOGICALLY FACILITATED VIOLENCE

In the twenty-first century, the penetration of technology into all aspects of human life has transformed the landscape of social interaction. From online communication to smart home devices, digital technology has blurred the boundaries between the private and public spheres. Digitalisation affects most fields of criminology, from financial crime and enabling new forms of identification, but also ID theft, to social media that enable social networks that have a preventive effect on their members, but also propaganda, radicalisation and 'networked hate' (Kaufmann & Lomell, 2025, p. 9). One way that criminology can account for the enabling and disabling effects of technologies is to conceptualise crime, deviance, and justice as increasingly techno-social practices within a digital society (Stratton, Powell, & Cameron, 2017, p. 24). Studying digital dimensions of crime is not the same as studying cybercrime. Cybercrime is often used as an umbrella term that includes all offences occurring in or being facilitated by an online environment. Research on cybercrime is well-established in the field of criminology. Digital criminology underlines that a study of online crime would take offline, analogue, or other aspects that enable criminal practice into account. Since digitalisation is a process of constant change, definitions as to what counts as crime and what is criminalised and in need of regulation are under constant development, too (Kaufmann & Lomell, 2025).

With the rapid development of the internet and technological devices, despite their enormous benefits for everyday life, multiple questions about human rights endangerment and security challenges have been raised as inevitable. In that regard, technology-facilitated abuse is often described as the misuse or repurposing of digital systems to harass, coerce, or abuse, involving both existing and emerging technologies (Koukopoulos, Janickyj, & Tanczer, 2025). The UN Special Rapporteur on violence against women in 2018 defined technology-facilitated gender-based violence as any act of gender-based violence against women that is committed, assisted, or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms, or email, against a woman because she is a woman, or affects women disproportionately (UNDP, 2018). It is regularly discussed in the context of domestic abuse, where it is perpetrated via a range of systems, including personal electronic devices (phones, laptops, and tablets) and smart home/Internet of Things appliances, as well as online accounts that are either shared or accessed without the partner's consent (Tanczer, Parkin, & López-Neira, 2021). According to UN Women and the World Health Organization, technology-facilitated violence against women (as the most common domestic violence victim) is any act that is committed, assisted, aggravated, or amplified by the use of information and communications technologies (ICTs)[2] or other digital tools that results in or is likely to result in physical, sexual, psychological, social,

2 'ICT' is described as an umbrella term that includes mobile phones, the Internet, social media platforms, computer

political, or economic harm or other infringements of rights and freedoms (UN Women; World Health Organization, 2023). In their research, they are stressing that perpetrators of technology-facilitated violence against women (TF VAW) use a variety of technology-based tactics to enact harm, and while some are unique to digital contexts (doxing, gender trolling, hacking, cybergrooming, using fake accounts, and image-based abuse), TF VAW also includes behaviours that are not unique to digital contexts (harassment, stalking, and exploitation) but may be assisted, aggravated, or amplified by the use of ICTs or other digital tools. Those who are at greater risk of experiencing this behaviour within a family and/or intimate relationship are women and LGBTQI+ people (Australian Government, eSafety Commissioner, 2023). Although both genders can find themselves in a situation of victimisation, here, as in violence between family members and intimate partners, the women are more vulnerable and more frequently in a position to become a victim (Vogels, 2021). Migrant women, women in religious, rural, or remote areas, and women with disability, are often seen as a group that may experience elevated risk of such victimisation (MacDonald, Truong, Willoughby, & March, 2023).

Digital violence against women is gender-based violence that occurs directly or indirectly through information and communication technologies and that results in, or is likely to result in, physical, sexual, psychological, or economic harm or suffering to women and girls, including threats of such acts, whether occurring in public or private life, or violations of their fundamental rights and freedoms. This violence against women is not limited to, but includes invasions of privacy, stalking, harassment, gender-based hate speech, sharing of personal content without consent, sexual abuse based on images, hacking, identity theft, and direct violence. It is part of a continuum of violence against women: it does not exist in a vacuum; instead, it stems from and supports many forms of offline violence (Advisory Committee on Equal Opportunities for Women and Men, 2020). Although more research is needed to fully understand the phenomenon and its impacts, current knowledge points to the fact that they are very similar to other types of violence against women: they are driven by the same reasons: misogyny, sexism, and male domination (Advisory Committee on Equal Opportunities for Women and Men, 2020). Therefore, in the paper below, the focus will be on women as victims of violence in the family and intimate relationships facilitated by technological devices.

The Technology Facilitates Violence Against Women in Domestic and Intimate Relationships

Digital gender violence is spreading uncontrollably, from the harassment of women who are public figures on social media to the tracking of intimate partners using dedicated applications. In the digital age, violence against women has transcended physical boundaries and entered the virtual sphere, creating new and complex patterns of harm. The growing integration of digital technologies into everyday life has not only reshaped communication, intimacy, and privacy but has also expanded the tools available for abuse. Within criminological discourse, this phenomenon, conceptualised as *technologically facilitated violence against women*, covers a multifaceted form of gender-based violence perpetrated through or assisted by digital means. It encompasses a wide range of behaviours, from online harassment and surveillance to the non-consensual dissemination of intimate images and financial control through digital platforms. Different types of perpetrators can commit such violent behaviours. They might be relatives or acquaintances of the victim, (ex-) intimate partners using digital devices to track and control their victims, classmates, co-workers, or anonymous users or online criminals like impersonators and hackers (Advisory Committee on Equal Opportunities for Women and Men, 2020).

Technology is not neutral. It mirrors existing gender inequalities and amplifies the reach and impact of abuse. In this sense, technologically facilitated violence against women represents both an evolu-

games, text messaging, email, and other related technologies.

tion and a continuation of patriarchal control, demanding equally adaptive legal and criminological responses. Gender-based violence in digital space includes various forms of deviant and/or criminal behaviour, such as online hate speech (mostly misogynistic), cyberstalking, online sexual harassment, other forms of cyber harassment, cyberbullying, image-based sexual abuse, and other forms (Stanojoska, 2025). The following section examines these divisions and their criminological implications, highlighting how each subforum reveals a distinct yet interconnected mode of digital victimisation.

In criminological analysis, researchers typically identify several main divisions of technologically facilitated violence, each representing distinct manifestations of abuse. These include the following:

Technology-facilitated coercive control (TFCC), which focuses on the use of digital tools to exercise dominance and surveillance within intimate relationships. Technology-facilitated coercive control (TFCC) focuses on the use of digital tools to exercise dominance and surveillance within intimate relationships. With this term, some researchers want to emphasise the technological and relational aspects of abuse in the specific context of coercive and controlling intimate relationships (Dragiewicz, et al., 2018). This can include: harassment on social media, stalking using GPS data, clandestine and conspicuous audio and visual recording, threats via SMS, monitoring email, accessing accounts without permission, impersonating a partner, publishing private information ('doxing'), or sexualised content without consent (Dragiewicz, et al., 2018).

Technology-facilitated sexual violence (TFSV) refers to behaviours where digital technologies are used to facilitate both virtual and face-to-face sexually based harms. Such behaviours include online sexual harassment, gender- and sexuality-based harassment, cyberstalking, image-based sexual exploitation, and the use of a carriage service to coerce a victim into an unwanted sexual act (Henry & Powell, 2018). Digital sexual violence includes image-based abuse as an umbrella term that covers various forms of digital gender-based violence and includes upskirting and creepshots, non-consensual pornography (revenge porn), sextortion, synthetic sexual media and deepfake pornography, sexting and abusive sexting, documenting or broadcasting sexual assault/rape videos, cyberflashing, technology-facilitated unwanted sexual experiences, online grooming, and electronically facilitated trafficking (UNDP, 2018).

Additionally, scholars recognise **public or platform-based forms of gendered violence**, such as doxxing, misogynistic hate speech, and coordinated online harassment targeting women in public life. It means persistent targeting of an individual with threats, defamation, and privacy invasions that cause severe emotional distress or the fear of physical harm (Citron & Penney, 2018).

Technology-facilitated domestic or intimate partner violence (TFDV) is a term used by scholars to describe a situation where digital means are used to maintain control and intimidation within the private sphere. It is crucial to acknowledge the distinct nature of technology-facilitated abuse. In an era of constant digital connectivity, where individuals can reach one another at any time and from any place, perpetrators can transcend physical and temporal boundaries to covertly or overtly inflict harm through a wider range of abusive practices. The resulting scope and opportunity for technologically facilitated victimisation are therefore extensive. When this expansive potential is coupled with victims' experiences of abuse as omnipresent and inescapable, their "space for action", the capacity to resist and seek help, becomes severely constrained (Rogers, Fisher, Ali, Allmark, & Frontes, 2023, p. 2221). Digital domestic and inter-partner abuse refers to the intentional use of digital technologies (including smartphones, social media platforms, and other internet-based tools) to harass, monitor, threaten, stalk, or intimidate the victim. This form of violence reflects how technological advancement not only transforms modes of connection but also expands opportunities for control, surveillance, and victimisation in both private and public spheres (Crisis House, 2023). As noted earlier, the expansion of digital communication has produced not only new forms of social interaction but also digitally

mediated versions of intimacy. This is particularly evident in relationships between partners who do not share the same geographic space. In long-distance intimate relationships, much of the emotional connection is transferred into online environments, where interaction primarily occurs through digital communication. Regular messaging, video calls, sharing personal experiences, and planning future visits are common practices that foster closeness, attachment, and mutual vulnerability. Consequently, the absence of physical proximity does not diminish the presence of intimacy. In fact, partners routinely engage in disclosures and emotional exchanges that mirror offline intimacy. Yet, this very vulnerability creates opportunities for abuse, as the digital sphere becomes a space where one party may manipulate communication, monitor behaviour, or exert control. In this way, digitally mediated intimacy can both sustain relationships and expose individuals to unique forms of technology-facilitated harm (Anayiotou, 2024).

For this purpose, perpetrators exploit digital tools to invade victims' privacy, monitor their behaviour, and erode their autonomy and sense of safety. In many cases, such abuse transforms the domestic sphere into a digital environment of constant surveillance and coercion. Abusers employ technological means in several interrelated ways (Crisis House, 2023).

- **Surveillance:** Perpetrators may install spyware or tracking applications on victims' devices to monitor communications, browse histories, or even use GPS technology to follow their physical movements.
- **Isolation:** By controlling access to communication channels, such as calls, text messages, or social media, abusers restrict victims' interaction with family, friends, and support networks, thereby reinforcing emotional dependency and social isolation.
- **Impersonation:** Offenders can hijack victims' online identities by gaining unauthorised access to social media or email accounts, using them to send false messages, post damaging content, or manipulate relationships, ultimately harming the victim's reputation and credibility.

These forms of abuse reveal how digital technologies, initially designed to enhance connection, can be repurposed into tools of coercion and domination. As such, technology-facilitated domestic violence represents not only an evolution of traditional patterns of control but also a significant criminological and legal challenge, demanding updated frameworks for prevention, investigation, and victim protection.

The Impact

Coercive control refers to a pattern of behaviours and tactics, ranging from physical violence to non-physical forms of manipulation, designed to undermine a victim-survivor's autonomy and create dependency on the perpetrator. Rather than occurring as isolated incidents, coercive control is continuous and cumulative, with repeated actions that gradually erode the victim-survivor's freedom, independence, and sense of equality. Through this sustained domination, the perpetrator can influence nearly every domain of the victim-survivor's life to the extent that her identity, agency, and personhood are diminished (MacDonald, Truong, Willoughby, & March, 2023). Behaviours that may appear ordinary or even benign in healthy relationships can become deeply abusive within the dynamics of coercive and controlling partnerships. The distinction lies not in the technology itself, but in the intent and context of its use. For example, location-tracking applications might be used consensually in non-abusive relationships to coordinate meetings or ensure mutual safety. However, within an abusive context, the same applications can be weaponised to stalk, monitor, and control a current or former partner's movements (Sugiura, et al., 2024). Similarly, digital tools that ordinarily facilitate connection, such as video-calling platforms like *FaceTime*, which may help parents maintain contact with their children, can pose significant risks for survivors of domestic abuse who share custody or communication channels with an abusive ex-partner. These technologies, while designed for connectivity, may inadvertently

enable continued access and intrusion by the perpetrator (Dragiewicz, O'Leary, & Ackerman, Children and technology-facilitated abuse in domestic and family violence situations, 2020).

The consequences for victims of this type of violence are profound.

Psychologically, TF-IPV produces constant fear, anxiety, hypervigilance, and a loss of personal freedom. Victims feel constantly monitored even in spaces where they should feel safe. The digital nature of surveillance, often invisible or covert, creates a sense of omnipresence, where victims may believe the abuser can see or access every aspect of their lives (Woodlock, Salter, Dragiewicz, & Harris, 2022). Impacts varied and included: lack of or limited access to finances and online banking; loss of employment; restrictions and prevention in securing employment; the accrual of debt; payment of hefty fees for the removal of sexual images from social media and web-based platforms; and financial implications of purchasing new or replacement devices. The reported **harms to the mental health** of victims/survivors ranged from the diagnosis of mental health conditions (e.g., depression and general anxiety disorder) to the doubting of one's sanity (through gaslighting) and suicidal ideation (Bond & Tyrrell, 2018). Widespread feelings of fear and humiliation were reported across studies, and, in some instances, embarrassment and fear meant some were unwilling to report the abuse. This can also lead to sleep disturbances, depression, emotional exhaustion, and long-term trauma. **Socially**, victims may withdraw from friends, family, and online platforms to avoid humiliation or harassment, resulting in **isolation and loss of support networks**.

Economically, the intersecting control of finances and technology results in a lack of access to banking (and therefore money) when a perpetrator changes passwords for the internet banking of a victim/survivor or destroys her devices (thereby causing social impacts of isolation of the victim from the social network). Alongside the financial impacts of this, victims'/ survivors' limited participation in the digital world can have a negative impact in terms of job prospects and other aspects of daily living (Douglas, Harris, & Dragiewicz, 2019).

Moreover, some behaviours involving technology, although not explicitly illegal, can still produce profound harm when situated within the framework of domestic abuse. Perpetrators frequently exploit online platforms and social media to harass, intimidate, or monitor victims. The use of geolocation software, spyware, and surveillance technologies extends their reach, providing new means to observe, track, and exert psychological dominance over victims – ultimately blurring the boundaries between the digital and physical dimensions of abuse (Sugiura, et al., 2024).

Research indicates **TFCC** affects victim-survivors across multiple dimensions of their lives. Studies report that victim-survivors often experience a profound sense of loss, which may relate to the end of the relationship, a disconnection from their pre-abuse identity, diminished trust in technology, and an erosion of safety and personal freedom (Woodlock, Salter, Dragiewicz, & Harris, 2022). TFCC can also reduce a person's capacity to participate in work, education, and social activities while contributing to isolation from family and friends (Douglas, Harris, & Dragiewicz, 2019). TFCC may also increase dependency on the perpetrator and restrict a victim-survivor's ability to seek assistance from police, healthcare professionals, or social supports (Douglas, Harris, & Dragiewicz, Technology-facilitated domestic and family violence: Women's experiences, 2019). Further consequences include diminished self-confidence and self-esteem, increased risk of self-harm (Harris & Woodlock, 2019) and strained relationships with children, particularly when perpetrators involve them in facilitating abuse (Dragiewicz et al., 2022). This can lead to the risk of victim-survivors stopping using technology due to the tendency to advise women to stop using technology, which can lead to reduced help-seeking behaviour and an inability to escape abuse (Australian Government, eSafety Commissioner, 2023).

For victims, the impact of this technologically facilitated violence is not only harm in the moment but also deep, enduring consequences for mental health, social connection, financial stability, and person-

al autonomy. This makes this type of violence that runs within family and/or intimate relationships a growing area of concern for criminology, law enforcement, and victim support services, requiring new protective measures, legal reforms, and specialised responses.

RELEVANT INTERNATIONAL FRAMEWORK

International legal and policy bodies have increasingly recognised the digital dimension of gender-based violence and expanded protections accordingly. In 2017, **CEDAW General Recommendation No. 35** explicitly extended the Convention's scope to technology-mediated environments, affirming that contemporary forms of violence also occur online and in other digital environments (General Recommendation No. 35 on Gender-Based Violence against Women, Updating General Recommendation No. 19, 2017). Similarly, **GREVIO's General Recommendation No. 1** introduced the term "digital dimension of violence against women" and set out concrete protection measures, including accessible information on legal remedies, online and offline complaint mechanisms, and specialised support services such as psychological and legal counselling for victims of technology-facilitated abuse. GREVIO further emphasised that national helplines and service providers must be trained and equipped to respond to digital forms of violence, ensuring equal access for all victims, including those with disabilities (GREVIO General Recommendation No. 1 on the digital dimension of violence against women, 2021). The **Istanbul Convention** (Council of Europe Convention on preventing and combating violence against women and domestic violence, 2011)**,** although drafted before today's digital expansion, requires states to criminalise psychological violence, stalking, and sexual harassment – all of which include digital forms. GREVIO has clarified that digital stalking, online harassment, and image-based abuse fall under the Convention's obligations.

In 2024, the **European Union adopted the Directive on combating violence against women and domestic violence**, which uses the term *cyber violence* and defines specific offences such as cyberstalking, cyber harassment, non-consensual sharing of intimate material, and online incitement to hatred or violence. The Directive also requires Member States to allow victims to submit complaints through secure digital channels for cybercrime-related offences and to ensure access to protection and support services (DIRECTIVE (EU) 2024 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on combating violence against women and domestic violence, 2024). Also, several **EU legal instruments** contribute to the protection of victims of digital abuse, including the **Victims' Rights Directive (2012/29/EU)**, the **Directive on combating sexual abuse and sexual exploitation of children (2011/93/EU)**, the **General Data Protection Regulation (GDPR)**, the **Audiovisual Media Services Directive**, and the **Directive on preventing and combating trafficking in human beings (2011/36/EU)**.

The European Commission's **Advisory Committee on Equal Opportunities for Women and Men** (Advisory Committee on Equal Opportunities for Women and Men, 2020) additionally recommends the term *cyber violence against women*, defining it as gender-based violence committed directly or indirectly through digital technologies and encompassing psychological, physical, sexual, or economic harm, as well as threats, privacy violations, image-based abuse, hacking, identity theft, and harassment. Critically, cyber violence is recognised as part of a broader continuum of violence against women and not as a separate phenomenon.

Together, these frameworks recognise digital/online forms of violence as part of GBV and impose obligations on states to criminalise intentional digital violence and address forms of online psychological abuse, digital stalking, and technology-facilitated sexual harassment, ensuring that responses to gender-based violence are comprehensive in both offline and online environments.

ABOUT NORTH MACEDONIA

As in many countries, the spread of smartphones, social media, and encrypted messaging has extended coercive control beyond the home. In North Macedonia, policy and monitoring bodies now explicitly recognise a *digital dimension* of violence against women, and service-provision gaps have been flagged (e.g., training and equipping helplines and specialist services to handle digital abuse). North Macedonia still lacks a consolidated, publicly accessible, official dataset isolating TF-IPV incidents specifically; most figures are embedded in broader cybercrime, VAW, or media-safety reporting. This is also reflected in GREVIO's calls to reinforce service coverage for the digital dimension of violence.

A UNICEF U-Report poll of youth in North Macedonia found that, in 2022, 24% felt under threat online, and 1 in 3 reported being victims of cyberbullying – most often via social media and chats. While youth-focused, these data illustrate the scale of tech-enabled harms in the population that later transitions into adult relationships (Unicef, 2023). An online survey conducted by UNDP (UNDP, 2018) on 311 people (95% women, 4% men, and 1% transgender, 55% aged 31 to 45, 40% aged 18 to 30, 3% aged 16 to 18, 2% over 46) showed that of the total number of participants, 186 people, or 60%, had faced some or several forms of technologically enabled gender-based violence. Of these, 96% were women, 3% were men, and 1% were transgender. However, the survey was not conducted on a representative sample, and the majority of participants filled out the questionnaire via Facebook, which is most often used by people aged 31 to 45 and is not entirely adequate for our research topic. According to a survey by the Helsinki Committee (2021) of 300 respondents in three cities, 78% were victims of cyberbullying. In certain situations, such cases end in suicide, because victims of this violence, where images, content, and personal data are shared without consent, feel powerless to prevent it (Anastasovska & Mitov). In 2019, high exposure to online harassment among women (notably women journalists) was detected by some regional surveys helped by the OSCE mission (OSCE, 2019), aligning with local findings and underscoring the need for stronger institutional responses.

Due to the ratification of the Istanbul Convention and Criminal Code amendments in 2023, for the first time, stalking (article 144-a) and sexual harassment (190-a), which can be done by using electronic devices for communication, were explicitly recognised as crimes, strengthening the basis for prosecuting TF-IPV behaviours (e.g., persistent unwanted digital contact, monitoring, harassment) (Criminal Code, 2023). The definition of gender-based violence in the Criminal Code recognises physical, psychological, and economic gender-based violence but does not specifically mention technology-facilitated GBV as a distinct form of gender-based violence (UNDP, 2018). Article 144 regulates the criminal offence of threatening the safety, paragraph 5 – whoever, through an information system, threatens to commit a criminal offence for which imprisonment of five years or a more severe punishment is prescribed, against a person due to their gender, shall be punished with imprisonment from one to five years. Article 193 criminalises the act of displaying pornographic material to a child, and paragraph two stipulates that if the act is committed through means of public information, the perpetrator shall be punished with imprisonment from three to five years.

The Law on Prevention and Protection from Violence against Women and Domestic Violence from 2021 is a landmark framework law that aligns with the Istanbul Convention, introducing key definitions (including stalking and sexual harassment), and mandating comprehensive victim protection and coordinated services – intended to cover online/technology-mediated contexts as well (Law on Prevention and Protection from Violence against Women and Domestic Violence, 2021). The Law, however, lacks specific protective measures and specific services tailored to technology-facilitated GBV (UNDP, 2018).

CONCLUSION

Technology-facilitated domestic and intimate partner violence represents an evolving dimension of gender-based violence, where digital tools extend the reach of coercion and control beyond physical proximity. Through surveillance, harassment, image-based abuse, impersonation, and digital monitoring, perpetrators can exert continuous pressure on victims, generating fear, dependency, isolation, and long-term psychological harm. Research consistently shows that digital abuse does not replace traditional forms of violence but functions as a continuation of them, allowing intimate partner violence to persist across spaces, relationships, and time – even after separation.

International legal instruments have increasingly responded to this reality. CEDAW General Recommendation No. 35, GREVIO General Recommendation No. 1, the Istanbul Convention, and most recently the 2024 EU Directive on combating violence against women and domestic violence all recognise the digital dimension of abuse and impose obligations on states to criminalise cyberstalking, cyber-harassment, non-consensual sharing of intimate material, and other forms of cyber violence. They further emphasise accessible reporting mechanisms, specialised support services, and training of institutions to properly address online victimisation.

North Macedonia has begun to align with these standards. The Law on Prevention and Protection from Violence against Women and Domestic Violence (2021) and Criminal Code amendments (2023) explicitly recognise stalking and online harassment as criminal acts, creating a legal foundation for addressing technology-facilitated abuse. High-profile cases such as *Public Room* revealed both the scale of online victimisation and the urgent need for more effective institutional responses.

Despite progress, significant challenges remain. North Macedonia still lacks systematic data collection on TF-IPV, institutional capacity for rapid response, and specialised training for police, prosecutors, social workers, and support services. Many victims continue to face barriers when reporting online abuse, while offenders exploit gaps in technology oversight, digital evidence procedures, and platform cooperation.

In this context, future policy must focus on implementing the existing legal framework, strengthening victim protection mechanisms, and ensuring that support services are equipped to address digital forms of violence with the same seriousness as offline abuse. As technology continues to shape intimate relationships, North Macedonia – like other countries – must adapt its criminal justice, social services, and prevention measures to ensure that the digital sphere does not become a space where violence is invisible, unregulated, or unpunished.

REFERENCES

Advisory Committee on Equal Opportunities for Women and Men. (2020). *Opinion on combatting online violence against women.* European Commision.

Anastasovska, S., & Mitov, O. (n.d.). *Annual report on the situation with hate speech at the local level in the cities of Tetovo, Bitola and Shtip for 2021.* 2021: Helsinki Committee for Human Rights.

Anayiotou, E. (2024, May 1). *Online Domestic Abuse: Redefining the law and protecting victims in long-distance intimate relationships.* Retrieved from London School of Economics Law Review: https://blog.lselawreview.com/2024/05/01/online-domestic-abuse-redefining-the-law-and-protecting-victims-in-long-distance-intimate-relationships/

ASSEMBLY OF THE REPUBLIC OF NORTH MACEDONIA. (2021). Law on Prevention and Protection from Violence against Women and Domestic Violence.

Australian Government, eSafety Commissioner. (2023). *Technology-facilitated abuse: family, domestic and sexual violence.*

Bond, E., & Tyrrell, K. (2018). *Journal of Interpersonal Violence*, 2166-2181.

Citron, D. K., & Penney, J. (2018). WHEN LAW FREES US TO SPEAK. *FORDHAM LAW REVIEW* , 2317 - 2335.

Committee on the Elimination of Discrimination against Women. (2017, July 26). General Recommendation No. 35 on Gender-Based Violence against Women, Updating General Recommendation No. 19. *Convention on Elimination of All Forms of Discrimination against WOmen*. United Nations.

Councile of Europe. (2011). Council of Europe Convention on preventing and combating violence against women and domestic violence. *Council of Europe Treaty Series - No. 210*. Istanbul .

Crisis House. (2023, July 20). *The Role of Technology in Domestic Violence: Digital Abuse and Cyberstalking*. Retrieved from Crisis House: https://crisishouse.org/blog/the-role-of-technology-in-domestic-violence-digital-abuse-and-cyberstalking/

Douglas, H., Harris, B. A., & Dragiewicz, M. (2019). *British Journal of Criminology*, 551-570.

Douglas, H., Harris, B. A., & Dragiewicz, M. (2019). Technology-facilitated domestic and family violence: Women's experiences. *British Journal of Criminology*, 551–570.

Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N., Woodlock, D., & Harris, B. (2018). Technology facilitated coercive control: domestic violence and the competing roles of digital media platforms. *Feminist Media Studies* .

Dragiewicz, M., O'Leary, P., & Ackerman, J. (2020). *Children and technology-facilitated abuse in domestic and family violence situations.* Retrieved from https://www.esafety.gov.au/research/children-and-technology-facilitated-abuse-in-domestic-and-family-violence-situations

GREVIO. (2021, OCtober 20). GREVIO General Recommendation No. 1 on the digital dimension of violence against women. Council of Europe.

Harris, B., & Woodlock, D. (2019). Digital coercive control: Insights from two landmark domestic violence studies. *British Journal of Criminology*, 530-550.

Henry, N., & Powell, A. (2018). Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research. *Trauma Violence Abuse, National Library of Medicine*.

Kaufmann, M., & Lomell, H. M. (2025). An introduction to digital criminology. In *De Gruyter Handbook of Digital Criminology.* De Gruyter.

Koukopoulos, N., Janickyj, M., & Tanczer, L. (2025). Defining and Conceptualizing Technology-Facilitated Abuse ("Tech Abuse"): Findings of a Global Delphi Study. *Journal of Interpersonal Violence,Sage Journals*.

MacDonald, J., Truong, M., Willoughby, M., & March, E. (2023, June). *Technology-facilitated coercive control*. Retrieved from Australian Government: https://aifs.gov.au/sites/default/files/2023-06/cfca-practice-guide-technology-facilitated-coercive-control.pdf

OSCE. (2019). *New OSCE-led survey reveals violence against women in South-Eastern and Eastern Europe*. Retrieved from https://www.osce.org/secretary-general/413423?utm_source=chatgpt.com

PARLIAMENT OF THE REPUBLIC OF NORTH MACEDONIA. (2023). Criminal Code. *Criminal Code of the Republic of North Macedonia, Official Gazzet 80/1999; 48/2001; 4/2002; 16/2002; 43/2003; 19/2004; 40/2004; 81/2005; 50/2006; 60/2006; 73/2006; 87/2007; 7/2008; 139/2008; 114/2009; 51/2011; 51/2011; 135/2011; 185/2011*.

Rogers, M., Fisher, C., Ali, P., Allmark, P., & Frontes, L. (2023). Technology-Facilitated Abuse in Intimate Relationships: A Scoping Review. *TRAUMA, VIOLENCE, & ABUSE, SAGE publication*, 2210 - 2226.

Stanojoska, A. (2025). A guide to tackling gender misinformation and gender-based violence in the digital space. Association for Equal Opportunities - Stella Network, Skopje.

Stratton, G., Powell, A., & Cameron, R. (2017). Crime and Justice in Digital Society: Towards a 'Digital Criminology'? *International journal for Crime, Justice and Social Democracy*, 17 - 33.

Sugiura, L., Buttom, M. B., Nurse, J., Saglam, R., Hawkins, C., & Frederick, B. (2024). The technification of domestic abuse: Methods, tools and criminal justice responses. *Criminology and Criminal Justice*.

Tanczer, L. M., Parkin, S., & López-Neira, I. (2021). 'I feel like we're really behind the game': Perspectives of the united kingdom's intimate pattern violence support sector on the rise of technology-facilitated abuse. *Journal of Gender-Based Violence,*, 431–450.

The European Parlament. (2024, April 25). DIRECTIVE (EU) 2024 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on combating violence against women and domestic violence. *DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on combating violence against women and domestic violence*. European Union.

UN Women; World Health Organization. (2023, March). TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN: TAKING STOCK OF EVIDENCE AND DATA COLLECTION.

UNDP. (2018). *Analysis of the legislation related to Technology Facilitated Gender Based Violence.*

Unicef. (2023). *"Cyberbullying Bye! Bye!" UNICEF and Telekom Foundation for Macedonia campaign against cyberbullying and online hate speech co-created with youth.* Retrieved from https://www.unicef.org/northmacedonia/cyberbullying-bye-bye?utm_source=chatgpt.com

Vogels, E. A. (2021). *The State of Online Harassment.* Pew Research Center.

Woodlock, D., Salter, M., Dragiewicz, M., & Harris, B. (2022). "Living in the Darkness": Technology-Facilitated Coercive Control, Disenfranchised Grief, and Institutional Betrayal. *Violence against women*.