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

Assoc. Prof. Elena Maksimova

Faculty of Law,

Goce Delcev University, Stip, North Macedonia

GOCE DELCHEV
UNIVERSITY
FACULTY OF LAW

Introduction: About The Technologically Facilitated Violence

Digitalisation

- process of constant change → definitions as to what counts as crime, what is criminalised and in need of regulation are under constant development, too

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

Technology-facilitated abuse (TFA)

- misuse or repurposing of digital systems to harass, coerce, or abuse, involving both existing and emerging technologies (Koukopoulos, Janickyj, & Tanczer, 2025)

At greater risk

- within a family and/or intimate relationship -e women and LGBTQI+ people - Migrant women, women in religious, rural or remote areas, women with disability

Reasons

- driven by the same reasons: misogyny, sexism and male domination

Definitions

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.

UN Special Rapporteur on violence against women (2018) – an act of GBV 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.

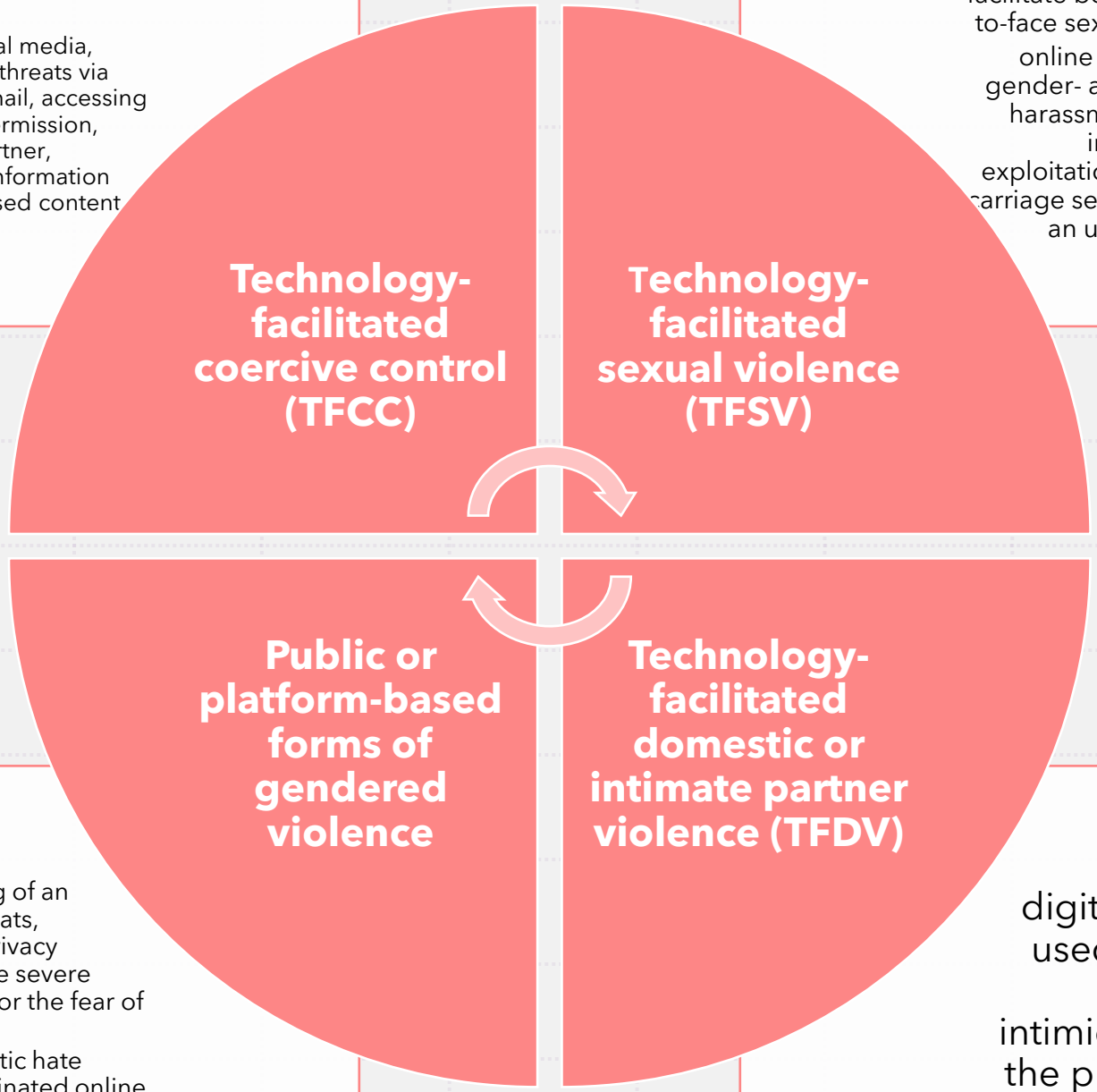
UN Women and World Health Organization, TFV against women (as the most common domestic violence victim) is any act that is committed, assisted, aggravated or amplified by the use of information and communications technologies (ICTs) or other digital tools, that results in or is likely to result in physical, sexual, psychological, social, political or economic harm, or other infringements of rights and freedoms

Modus operandi

1. Perpetrators of technology-facilitated violence against women (TF VAW) use a variety of technology-based tactics to enact harm:
    1. Some are unique to digital contexts (doxing, gender trolling, hacking, cybergrooming, using fake accounts and image-based abuse),
    2. TF VAW also includes behaviours that are not unique to digital contexts (harassment, stalking and exploitation) but may be assisted, aggravated or amplified using ICTs or other digital tools.
    3. **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**

The technology facilitates violence against women in domestic and intimate relationships

main divisions of technologically facilitated violence:



Technology-facilitated domestic or intimate partner violence (TFDV)

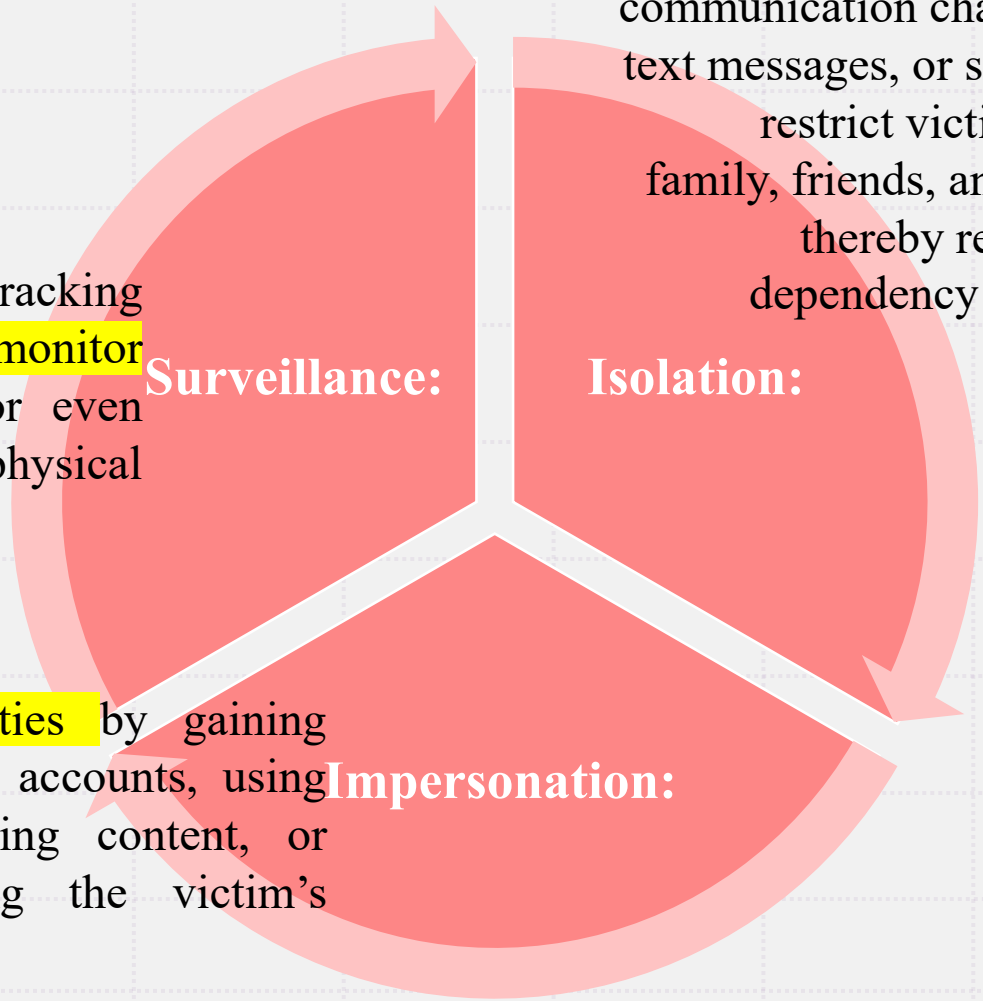
digital means are used to maintain control and intimidation within the private sphere

- 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
- particularly evident in relationships between partners who maintain long-distance intimate relationships → much of the emotional connection is relocated into online environments, where interaction occurs primarily through digital communication (regular messaging, video calls, sharing personal experiences, and planning future visits are common practices that foster closeness, attachment, and mutual vulnerability)
- 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

Technology-facilitated domestic or intimate partner violence (TFDV)

digital means are used to maintain control and intimidation within the private sphere

Transforms the domestic sphere into a digital environment of constant surveillance and coercion:



- 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.

- 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.

- 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.

sleep disturbances, depression, emotional exhaustion, and **long-term trauma harms to the mental health**

Psychological

Physical

increased risk of **self-harm**

isolation from family and friends
dependency on the perpetrator →
restricts a victim-survivor's ability to seek assistance from police, healthcare professionals, or social supports

Social

Economical

lack of **access to banking** (and therefore money) - perpetrator changes passwords for the internet banking of a victim/survivor or destroys her devices
negative impact in terms of **job prospects** and other aspects of daily living

Relevant international framework

- 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
- **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.
- The **Istanbul Convention,** although drafted before today's digital expansion, requires states to criminalise psychological violence, stalking, and sexual harassment - all of which include digital forms
- 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
- The European Commission's **Advisory Committee on Equal Opportunities for Women and Men** in 2020 additionally recommends the term *cyber violence against women*. Critically, cyber violence is recognised as part of a broader continuum of violence against women and not as a separate phenomenon.

North Macedonia

A **UNICEF U-Report** poll of youth in North Macedonia found (2022) - 24% felt under threat online, and 1 in 3 reported being victims of cyberbullying - most often via social media and chats.

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.

In 2019, high exposure to online harassment among women (notably women journalists) was detected by some regional surveys helped by the **OSCE mission, aligning with local findings** and underscoring the need for stronger institutional responses.

North Macedonia – legislation

Due to the ratification of the Istanbul Convention, the **Criminal Code** amendments in 2023

stalking, sexual harassment, threatening the Safety, Displaying Pornographic Material to a Child

Law on Prevention and Protection from Violence against Women and Domestic Violence from 2021

introducing key definitions (including stalking and sexual harassment), and mandates comprehensive victim protection and coordinated services - intended to cover online/technology-mediated contexts as well, however, lacks specific protective measures and specific services tailored to technology-facilitated GBV

Conclusion

•**Technology extends abuse beyond physical space**, enabling continuous surveillance, harassment, image-based abuse and digital monitoring.
•TF-IPV does not replace traditional violence – it **expands and sustains** coercive control, even after relationship separation.
•**International frameworks** (CEDAW GR No. 35, GREVIO GR No. 1, Istanbul Convention, EU Directive 2024) recognise cyber violence and require states to **criminalise cyberstalking, cyber-harassment** and **non-consensual sharing of intimate material.**
•**North Macedonia** has taken important steps:
•Law on Prevention and Protection from Violence against Women & Domestic Violence (2021)
•Criminal Code amendments (2023) – stalking & online harassment recognised as crimes
•High-profile cases (e.g., **Public Room**) reveal the **scale of digital victimisation** and need for a stronger institutional response.
•**Challenges remain**: limited data, slow reporting mechanisms, insufficient training of police and service providers, lack of rapid digital protection.
•**Future priority**: effective implementation of law, stronger victim support, digital evidence procedures, platform accountability, and institutional training.

THANK YOU FOR YOUR ATTENTION

Assoc. Prof. Elena Maksimova

Elena.Maksimova@ugd.edu.mk

Faculty of Law,

Goce Delcev University, Stip, North Macedonia

GOCE DELCHEV
UNIVERSITY
FACULTY OF LAW