THE DARK SIDE OF DIGITALIZATION:

Technology-facilitated violence against women in Eastern Europe and Central Asia

October 2023

UN Women is the UN organization dedicated to gender equality and the empowerment of women. A global champion for women and girls, UN Women was established to accelerate progress on meeting their needs worldwide. UN Women supports UN Member States as they set global standards for achieving gender equality and works with the Governments and civil society to design laws, policies, programmes and services needed to implement these standards.

ACKNOWLEDGEMENTS

This publication was developed by the UN Women Europe and Central Asia Regional Office.

We would like to express our appreciation for all those who contributed to the development of this research report.

Research team: Marija Babović, the author and lead researcher, worked tirelessly throughout the process, with the support of Kelly Litz as research assistant and Erol Ohtamis providing logistical assistance.

Special thanks also go to our colleagues from UN Women offices in all countries included in the research, who peer-reviewed the research and offered their guidance, insights, and expertise throughout the process. A particular note of thanks goes to the UN Women Regional Gender Statistics Specialist for Europe and Central Asia.

Our word of appreciation goes to the UN Women EVAW Unit, particularly Raphaëlle Rafin, UN Women Programme Specialist on VAW Data on Research, whose technical expertise elevated the report.

Our recognition goes to our Technical Advisory Board that reviewed and validated the preliminary findings and enriched the recommendations of the research. The board included:

Elmaja Bavcic, OSCE
Anca Ciupa, Women against Violence Europe (WAVE)
Eleonora Esposito, European Commission
Cristina Fabre and Diogo Costa, EIGE
Loly Gaitan, Fanny Rotino and Carla Licciardello, ITU
Rachel Grant, FCDO UK
Katja Tiilikainen and Liisa Ketolainen, MFA Finland

This research was also possible thanks to vision and guidance of Alia El-Yassir, former UN Women Regional Director for Europe and Central Asia.

Lastly, and most importantly, we are grateful to all the individuals, organizations and institutions that participated in interviews and focus group discussions. This includes human rights institutions, civil society and women's rights organizations, survivors of technology-facilitated violence, justice and security institutions, gender equality mechanisms, and others. They graciously gave their time and knowledge to shed light on this important issue, and we deeply value their partnership, not only in the context of this research but also in our shared vision of a world where women and girls live free from violence.

The report was coordinated by Yolanda Iriarte with communications support from Victoria Puiu.

ACRONYMS

BiH	Bosnia and Herzegovina
CSO	Civil society organization
CSW	Commission on the Status of Women
ECA	Europe and Central Asia
EIGE	European Institute for Gender Equality
EU	European Union
EVAW	Ending violence against women
FGD	Focus group discussion
GBV	Gender-based violence
GDPR	General Data Protection Regulation
IC	Istanbul Convention
IDP	Internally displaced person
TF	Technology-facilitated
VAW(G)	Violence against women (and girls)
ICT	Information and communication technologies
GREVIO	Group of Experts on Action against Violence against Women and Domestic Violence
UNSRVAW	United Nations Special Rapporteur on Violence Against Women

CONTENT

LIST OF TABLES

LIST OF FIGURES

HeForShe Summit 2023. Photo: © UN Women/Ryan Brown

EXECUTIVE SUMMARY

BACKGROUND AND OBJECTIVES

Digital advancements offer significant means for empowering women, granting them greater access to information, fostering connections, and enabling them to champion their rights and interests. Nevertheless, in an environment marked by prevalent gender inequalities and deeply rooted patriarchal views, these same technologies can be weaponized to commit and escalate violence against women (VAW). The rapid evolution of technology and its misuse for gender-based violence against women outpaces the capacity of governments and civil society organizations to effectively respond. This lag in response, coupled with inadequate victim support, has amplified the scope and intensity of technology-facilitated violence against women, contributing to women's reluctance to participate in online spaces and jeopardizing their ability to fully seize the benefits of digitalization.

To shed light on technology-facilitated forms and dimensions of VAW, the UN Women Europe and Central Asia (ECA) Regional Office conducted comprehensive research in 13 countries of the ECA region: Albania, Bosnia and Herzegovina, Georgia, Kazakhstan, Kosovo,[1] Kyrgyzstan, Moldova, Montenegro,[2] North Macedonia, Serbia, Tajikistan, Türkiye, and Ukraine.

With this research, UN Women ECA intended to better understand the types and prevalence of technology-facilitated (TF) VAW in the region and its consequences on women and women's attitudes, experiences and access to services, while at the same time exploring the existing normative and institutional context and role and perspective of relevant stakeholders in providing prevention and support services to survivors of such violence.

RESEARCH METHODOLOGY

Rigorous ethical standards were applied to data access and storage, as well as presentation of findings.

Research components

1. Mapping of relevant normative and policy frameworks at global, regional and national levels

Aim: To provide basic insights into processes focused on the development of legal and policy frameworks and inclusion of technology-facilitated violence in key conventions, laws and strategies/action plans at global, regional, and national levels.
Over 50 legal and policy documents were reviewed directly, and not through secondary sources.

2. Large scale web-based survey with the participation of over 12,000 women across the region

Aim: To assess the prevalence, characteristics, consequences and support services related to TF VAW.
From January-June 2023, at least 1,000 women (aged 18+) were surveyed in each country. National samples are not representative of national populations but rather the population of women present online, which on average is younger, more urban and with higher education.

3. Qualitative research with governmental and non-governmental stakeholders

Aim: To delve deeper into stakeholders' awareness, understanding, capacities, challenges and experiences related to handling cases of TF VAW.
Over 80 stakeholders across the region participated in interviews and focus group discussions.
Research captured perspectives of governmental gender equality mechanisms, human rights oversight institutions, police (including cybercrime police), CSOs, activists, gender experts and women with experience of TF VAW.

1 References to Kosovo shall be understood to be in the context of UN Security Council Resolution 1244 (1999).

2 Montenegro was not included in the web-based survey due to the cost of web-based randomized research in the context of a small population. However, Montenegro was included in the qualitative research, and having in mind similarities in the technology facilitated VAW and more broadly women's situation in the Western Balkan countries, the findings obtained from the web-based survey for neighbouring countries are very much valid for Montenegro as well.

CONCEPTUAL APPROACH AND DEFINITION

The conceptual framework adopted for the purpose of this research, including the definition of technology-facilitated VAW, were informed by the ongoing discussion coordinated by UN Women and the WHO.[3] Per this discussion, TF VAW is understood as an expression of gender-based violence and discrimination that exists online and offline. Offline and technology-facilitated VAW are not separate forms, but rather could be understood as a continuum in which some forms occur only offline, some occur only through the use of digital technologies, and many include both offline and technology-facilitated components. Regardless, the risk factors, consequences and underlying causes – such as structural gender inequalities, misogyny and unequal power between women and men – remain the same. Violence and fear of violence can lead to self-censorship and the withdrawal of women, restricting their access to the internet and technologies which are of crucial importance for many aspects of social inclusion and participation, including in education, employment, politics and social life.

> ***Technology-facilitated violence against women is 'any act that is committed, assisted, aggravated or amplified by the use of 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.'***
>
> Expert Group Meeting report
> Technology-facilitated violence against women:
> Towards a common definition (2023)

Operational definition of TF VAW. To adequately measure experiences of technology facilitated violence in the web-based survey, the questionnaire utilized act-based definitions. It provided a list of acts of TF VAW from which respondents could select, allowing for multiple responses. The questionnaire also included an "other" option for respondents who felt the list wasn't comprehensive and wanted to report an act of violence not mentioned, as well as a "none of the above" option for those who had not experienced TF VAW. Those who selected any of the listed acts were categorized as women who have experienced technology-facilitated violence.

KEY FINDINGS ON NORMATIVE AND POLICY FRAMEWORK

International, regional and national actors are still in the early stages of addressing technology-facilitated violence against women (TF VAW), and the countries included in this research are no exception.

Global processes have intensified during the last several years, driven by the concurrent processes undertaken by the UN General Assembly, Secretary General, UNSRVAW and Commission on the Status of Women (CSW), which have been supported by the work of UN Statistical Commission,[4] WHO and UN Women. These processes advance the development of a common understanding to enable further progress regarding legal frameworks, data collection, research and statistics and other initiatives. Gender mainstreaming of the International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes adds to the number of ongoing processes related to developing legal instruments to prevent and combat TF VAW.

European regional processes are marked by various initiatives of the Council of Europe and EU. One of the crucial milestones is the effort to reaffirm the Istanbul Convention and its relevance for TF VAW in GREVIO recommendation No. 1.

3 UN Women, WHO, Technology-facilitated Violence against Women: Towards a common definition. Report of the meeting of the Expert Group 15-16 November 2022, New York, USA, https://www.unwomen.org/sites/default/files/2023-03/Expert-Group-Meeting-report-Technology-facilitated-violence-against-women-en.pdf

4 At the 54th Session (2023) of the UN Statistical Commission, the need for methodological work to measure technology – facilitated was recognized: https://unstats.un.org/UNSDWebsite/statcom/54

As with most countries worldwide, countries in the ECA region do not have adequate legal and policy frameworks to address TF VAW. This mapping exercise showed that only in a few cases key laws address TF VAW directly, at least to some extent. The same is found for current gender equality and EVAW policies.

Overview of national legislation and strategies that directly address TF VAW

Country	Criminal code	Specialized law on GE, VAW/DV	Gender Equality Strategy	Specialized VAW/ DV strategy
Western Balkans				
Albania	↓	↓	↓	–
BiH – state level	↓	↓	–	–
BiH – FBiH	↓	↓	–	–
BiH – Republika Srpska	↓	↓	–	–
Kosovo	↓	↓	↓	↗
Montenegro	↗	↓	↓	–
North Macedonia	↗	↗	↓	–
Serbia	↗	↓	↓	↗
Türkiye				
Türkiye	↗	↗	↓	↗
Eastern Europe				
Georgia	↗	↓	↓	↓
Moldova	↓	↓	↓	–
Ukraine	↓	↓	–	–
Central Asia				
Kazakhstan	↓	↓	–	–
Kyrgyzstan	↓	↓	↓	–
Tajikistan	↓	↓	↓	↓

Legend

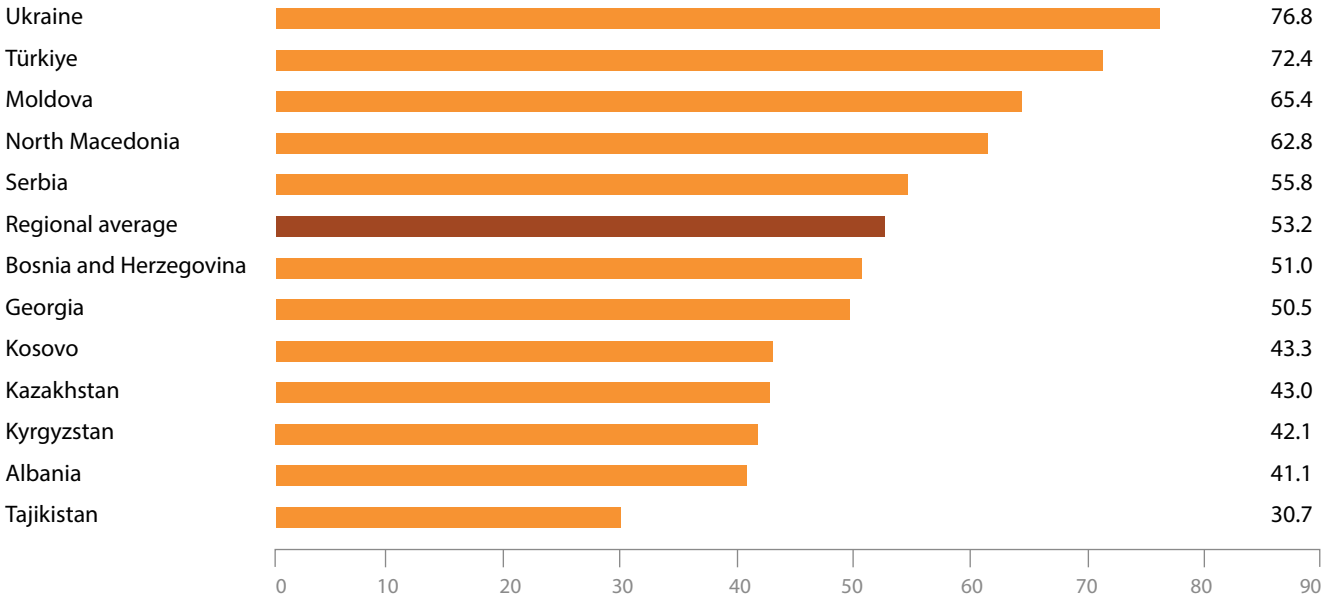
↑	Law/policy **directly** addresses TF VAW as defined by UN Women in **majority** of forms
↗	Law/policy **directly** addresses **some** forms of TF VAW as defined by UN Women
↓	Law/policy at best **only indirectly** addresses some forms of TF VAW
–	There is no such law or strategy

KEY FINDINGS FROM WEB-BASED SURVEY

Prevalence. More than half of women (18+) present online in the region have experienced some form of technology-facilitated violence in their lifetime.

The cross-country differences are significant, with the highest prevalence in Ukraine and lowest in Tajikistan. By subregion, the highest prevalence is in Türkiye and Eastern Partnership countries, while prevalence is lower in the Western Balkans and lowest in Central Asia.

Proportion of women who experienced at least one form of technology-facilitated violence, regional average and by country (%) (N=12,526)



Forms of violence. Among women who had experienced TF VAW, the most prevalent forms include receiving unwanted or offensive content or messages (39.7%), receiving inappropriate sexual advances or content on social networking (30%) and hacking women's accounts and web pages (25.4%). A large proportion of women experienced TF violence once (40.4%), while one in four women experiences such violence daily or weekly.

Virtual 'places' of violence. Facebook and Instagram are the platforms most reported by women as places where they experienced violence, as every third woman who experienced technology-facilitated violence had that experience on one of these two platforms. One in ten women experienced TF VAW on TikTok, e-mail or messaging applications such as Skype, Snapchat, Messenger, Viber or similar. The platforms on which women experienced TF violence differed by country and region, with Western Balkan women having more violent experiences on Facebook than women in other countries, women from Albania and Türkiye pointing more to Instagram, and women from Central Asia pointing more to WhatsApp and Telegram.

Perpetrators. The majority of technology-facilitated VAW is perpetrated by unknown persons (50.3%) or persons known only on the internet (17.5%). However, almost one third (32.1%) of technology-facilitated violence is perpetrated by persons in women's social proximity, such as partners, family members, friends, acquaintances, colleagues, bosses or co-students, and therefore may represent an extension of offline violence. While unknown perpetrators and those only known to women on the internet are more inclined to commit violence in the forms of hacking women's accounts and sharing offensive or other unwanted content or messages, partners are more likely to use threats or controlling acts, while family members combine controlling acts with sexual harassment, and bosses are more linked to acts in the forms of sexual harassment. Although all forms

of violence regardless of perpetrator occur mainly on Facebook and Instagram, there are certain differences between perpetrators related to types of platforms they use in acts of violence: partners more often use Twitter, WhatsApp, and meeting tools; friends and acquaintances more often use Telegram, TikTok, and online gaming platforms; while persons only known to women online more often use Facebook, Instagram and dating platforms.

Risk factors. The risks of TF VAW are not evenly distributed among women with different socio-demographic backgrounds.

- Younger women are at higher risk of TF VAW than older women: the probability of experiencing TF VAW is 4 times higher for women aged 18-24 than for those over age 65.
- Women with education beyond primary level are at higher risk than women with primary school education, and the risk is highest for women with secondary technical training.
- LGBTQ+ women, women from bigger cities and divorced women also face a higher risk of TF VAW.
- Employment status has no influence on the risk of TF VAW.

Some risk factors are related to online activities and communication-related practices and behaviours:

- Women who spend more time on the internet are at higher risk of being exposed to violence.
- The risk is highest for women participating in online gaming, followed by women who most often use social media messaging applications, such as Snapchat, Viber, Facebook or Instagram, and then women who use Telegram.
- Having a public profile on internet platforms, particularly across multiple sites, and having a larger number of friends and followers also increase the risk of experiencing violence.

Consequences of TF VAW. Two thirds of women subjected to TF VAW reported feeling emotional consequences, unsafety or embarrassment as a result. One in ten women reported that violence damaged their personal social relations with others. The consequences are more prevalent among women who were exposed to repeated violence compared to women with one-off experiences of TF VAW, with the exception of embarrassment, which is more present among women who experienced a single violent incident. Women whose perpetrators were current or former partners were more likely to suffer psychological consequences, while those whose perpetrators were bosses were more likely to feel unsafe, and those whose perpetrators were persons only known on the internet were more likely to feelembarrassed.

Women who have experienced any form of technology-facilitated violence feel less safe online. They are also more cautious in digital communication and more often utilize various precautionary measures, such as turning off webcams and location sharing, using different passwords for different accounts, customizing privacy settings on platforms, and only communicating with persons they know offline.

Experiences of violence discourage women from expressing themselves on the internet, and a significant proportion becomes accustomed to violent attacks, potentially leading to increased tolerance for violence and a less proactive approach to combat it.

Reporting and combating TF VAW. After experiencing TF VAW, the majority of women took steps to increase their safety on the internet, such as to block, mute or unfriend the person who caused harm (36.6%). Women rarely report cases of violence to the police (7.1%) or other institutions (4.5% to human rights institution, 2.6% to educational facility), and even less so to non-governmental organizations (2.5%); less than half of women reported their experience to friends or family (43.8%). The reasons for not reporting are the belief that nothing will be done, lack of trust in institutions, fear that confidentiality will not be respected and fear that they will be blamed for the experience.

Women who asked for support from their partner, family or friends often received support. A high proportion of all women participating in the survey (70.4%) would like stronger accountability and responsibility from companies that own internet platforms and apps, more effective protection from institutions (66.5%), and more awareness raising in order to empower women to prevent, report or counter TF VAW (69.7%).

KEY FINDINGS FROM QUALITATIVE RESEARCH

Governmental stakeholders. There is a consensus among interviewed representatives of governmental gender equality mechanisms and institutions engaged in response to violence against women – e.g., police (including cybercrime police), judiciary, social protection – that technology-facilitated violence against women has increased in frequency and intensity since the outbreak of the COVID-19 pandemic. At the same time, they are aware of their limited capacities to adequately respond to these new trends, and they have proposed ways to further improve legislation, policies, measures, instruments, and practices in response to TF VAW. A systematic lack of statistical data and administrative evidence on TF VAW was noted across the countries.

Multisectoral mechanisms are established to varying extents in the countries of the region, but they are often ineffective even for offline dimensions of VAW, for which they are mainly responsible. Meanwhile, TF VAW is mostly under the responsibility of cybercrime police. However, according to testimonies, cybercrime police are not sufficiently equipped to effectively address the growing issue of TF violence against women, are often more focused on TF violence against children, and are not integrated into multisectoral cooperation mechanisms.

Cooperation with the internet platforms on which violence occurs and between stakeholders in the region or in the broader international community is crucial, as TF VAW has no borders. However, qualitative research reveals that cooperation is limited and that there are still obstacles in identifying perpetrators and processing cases in cross-border situations.

Civil society perceptions and response. Similar to governmental stakeholders, civil society organizations, whether they are direct service providers, advocacy-oriented activists in the area of women's rights, or gender equality experts, are much more engaged in the 'traditional' areas of gender-based violence and VAW. Only a few are particularly focused on technology-facilitated violence. During focus group discussions and interviews, they often emphasized that technology-facilitated dimensions of violence are increasingly present in their work. They also described various forms of technology-facilitated violence they face in their work and highlighted categories of women who are at higher risk of being exposed to such violence. This includes women in divorce procedures, women in public positions (e.g., politicians, journalists, activists), women from ethnic minorities, young women, women in rural areas, women living with disabilities, LGBTQI+ women, women with HIV, and women affected by earthquakes or war (such as refugees, IDPs, and victims of conflict-related sexual violence).

Research found very innovative approaches among CSOs that specialize in addressing TF VAW. Unfortunately, there aren't many such organizations. The majority of organizations lack knowledge and skills to engage with TF VAW, even when it comes to adequately addressing technology-facilitated dimensions of cases of domestic and partner violence, which are often a focus of their work. Regarding the main challenges in addressing TF VAW, organizations reported inadequate legal frameworks, lack of awareness and underreporting, problems in referrals and cooperation with public service providers, the weak role of the education sector in preventing and screening for TF violence among children and young people, difficulties related to cross-border cases, and a lack of knowledge and tools. As one of the conclusions, participants emphasized the need to create new alliances with IT organizations in order to develop new capacities and approaches in preventing and combating TF VAW. Some innovative solutions were uncovered during the research which can be used as good practices that can be further replicated or inspire other organizations to transform their practices.

RECOMMENDATIONS

Based on the research findings and proposals of governmental and non-governmental stakeholders participating in the qualitative survey, as well as the suggestions and recommendations provided by UN Women offices and members of the Technical Advisory Board, sets of recommendations are proposed for relevant stakeholders.

Improving legal and policy instruments

In consultation with relevant stakeholders, including victims of TF VAW and women's organizations, **state actors** should develop, amend and expand legislation and policies to address digital dimensions of VAW, strengthen their implementation, and fast-track processes to prevent, eliminate and respond to TF VAW. Laws and policies should also ensure the responsibility of perpetrators, including in the case of transborder acts of violence, and accountability of the technology sector, including through a firmer control over digital and communication technologies and online media to prevent and address TF VAW, hate speech, gender stereotypes, and sexual abuse.

International and regional organizations should advance and promote international and regional frameworks on TF VAW, produce guidance on states' alignment with such frameworks, and ensure that relevant frameworks under preparation are gender-sensitive and sufficiently address TF VAW. Furthermore, EU institutions should leverage EU accession processes to encourage and support EU candidates and potential candidate countries to align national legislation with the EU legal framework related to TF VAW.

The technology sector, including social media, online gaming and IT companies, should closely monitor the development of the international and national legal frameworks for protection from TF VAW and align their 'community guidelines' to international norms.

Improving multistakeholder coordination on TF VAW

At national level, all stakeholders must strengthen their cooperation and coordination in order to achieve a robust multisectoral approach to prevent and respond to TF VAW.

At international level, all stakeholders, with an emphasis on **state actors**, should ensure more effective cooperation among national police forces and allow victims to report violence to the police in their own countries rather than in perpetrators' countries. All stakeholders should also engage in regional and bilateral knowledge exchanges to learn from other countries and establish more coordinated efforts.

International coalitions and networks such as the multistakeholder Generation Equality Action Coalitions on Technology and Innovation for Gender Equality and on Gender-Based Violence which share TF VAW as a common priority and the Global Partnership for Action on Gender-Based Online Harassment and Abuse can leverage their commitments and goals to accelerate progress towards ending TF VAW and engaging more state and non-state partners to participate in these global efforts.

Conducting whole-of-society prevention strategies

All stakeholders, state and non-state, should raise awareness among relevant professionals on the magnitude, manifestations and consequences of TF VAW, as well as encourage a more proactive role of the education system in raising student and teacher awareness on TF VAW. Digital literacy and knowledge should be advanced among the general population to improve personal security while using digital and communication technologies, which should also be reflected in national gender equality policies and programmes. Finally, men and boys should be educated on the forms, dimensions, severity and consequences of TF VAW, with a particular focus on the forms and dimensions that may already be normalized or are at risk of being normalized, as well as more generally on equitable masculinities and non-violent communication.

The **technology sector** has an important role to play, by its outreach, to contribute to prevention efforts to change social norms and attitudes and should develop educational resources to raise awareness on TF VAW and the importance of nonviolent and safe communication and use of technologies.

Media outlets should improve their awareness and understanding of TF VAW, and journalistic standards and codes should be revised to include ethical considerations related to TF VAW. Further, the media should raise awareness about TF VAW and accurately report on cases of TF VAW rather than minimizing or romanticizing the actions and their impact on victims.

Improving multistakeholder response to TF VAW

State actors should ensure that general and specialized services address TF VAW and meet the needs of particularly vulnerable women. In countries where cybercrime police are mandated with investigating TF VAW, they should be more systematically integrated into multisectoral mechanisms, and their roles in responding to TF VAW should be defined more clearly in bylaws or protocols. Specific protection mechanisms should be developed to protect women in the public eye as they are more often exposed to TF VAW.

Civil society organizations should expand their services to cover dimensions and forms of TF VAW as well as strengthen cooperation and coordination among CSOs to more effectively and cohesively counter TF VAW.

The technology sector should proactively, promptly and effectively monitor and remove hate speech, sexist and misogynistic content and incidents of TF VAW, including by improving response to platform-based reporting mechanisms. They should also enhance their cooperation with law enforcement to improve response time to cases of TF VAW and more rapidly lock or remove offenders' accounts.

Empowering CSOs and women's rights organizations

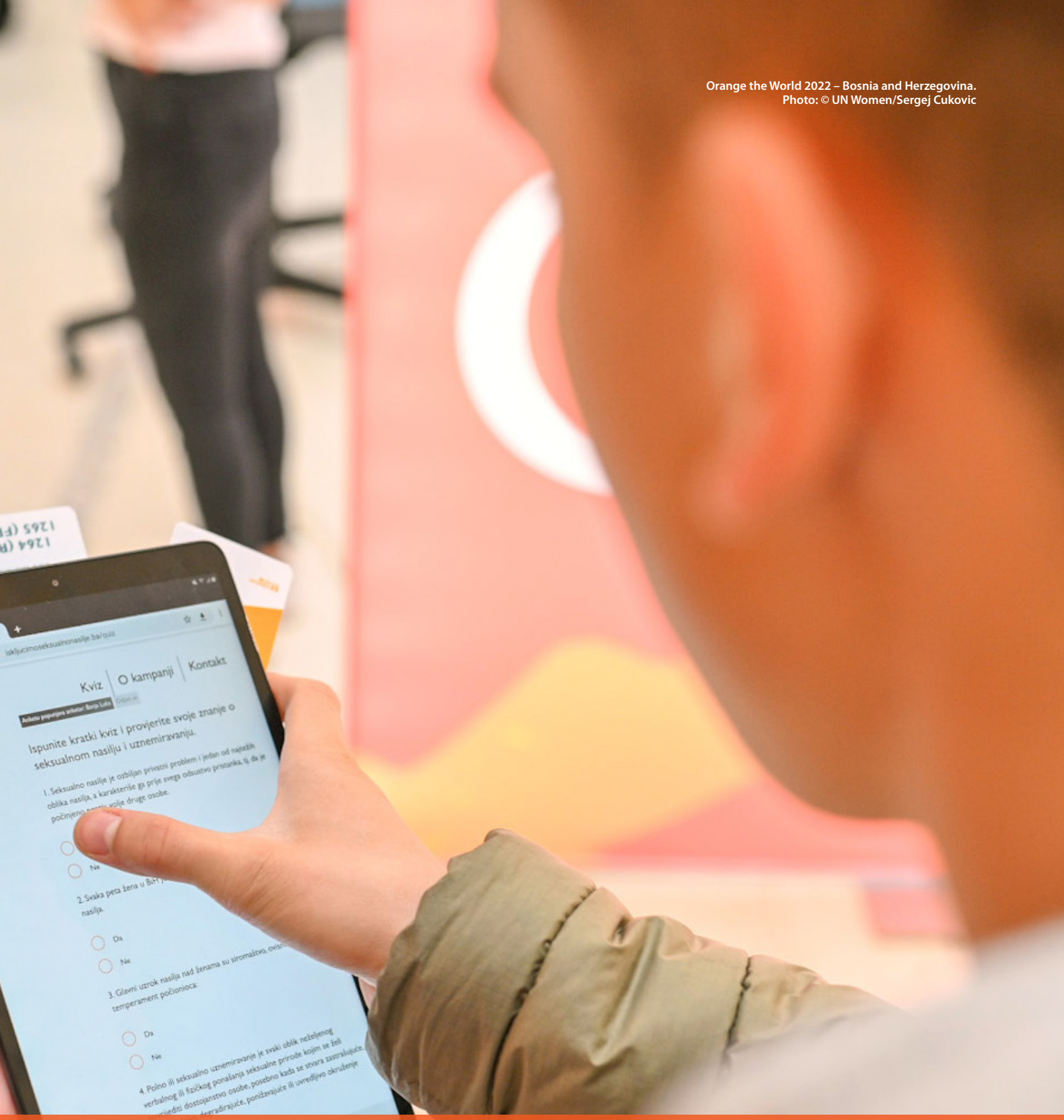
State actors, as well as **international and regional organizations**, should support CSOs to strengthen their capacities to fully understand and provide services for TF VAW, as well as include CSOs as key partners in the development of programmes, policies and legislation related to TF VAW. They should also ensure sustainable funding for CSO services providers, outside of project-based funding.

Improving data and evidence

International and regional organizations are well positioned to lead the way on improving data collection on TF VAW, particularly through the development of global standards and guidance on the collection of data on TF VAW. Further, statistical surveys on VAW should encompass technology-facilitated dimensions. In the European region, learnings from methodologies to collect survey and administrative data on TF VAW developed by Eurostat, EIGE and FRA should feed and inform further regional and global methodological developments in this area.

State actors should also strengthen and better coordinate administrative data systems on TF VAW, and administrative data reports should be regularly shared and should clearly present (anonymized) findings. State actors should also fund and produce research on TF VAW to serve as an evidence base for designing campaigns to counter it. Finally, states should monitor the proportion of funds from public budgets or international aid allocated to prevention and response to TF VAW to ensure sufficient allocation.

Civil society organizations that provide services to victims of VAW should develop and improve their internal collection of administrative service data to screen for and document incidents of TF VAW.



Orange the World 2022 – Bosnia and Herzegovina.
Photo: © UN Women/Sergej Cukovic

1· INTRODUCTION

BACKGROUND

Technology and digitalization undoubtfully provide powerful tools for women's empowerment. They expand women's opportunities to access information, knowledge and services; to connect with others; and to pursue their interests and advocate for their rights, among other benefits. However, in a context of rampant gender-based violence against women grounded in structural gender-based inequalities and widespread patriarchal norms, technology also provides powerful tools for perpetrators to commit and intensify violence against women. At the same time, advancements in technology and their subsequent appropriation for gender-based violence against women occur at a much faster pace than the state or civil society is able to respond. Due to the latency of responses and insufficient support for victims, the forms, intensity and spaces of violence against women have been expanding, contributing to growing feelings of unsafety, discouragement and withdrawal from online public spaces.

In line with UN Women's commitment to end violence against women, as emphasized in the Strategic plan 2021-2025, the UN Women Europe and Central Asia (ECA) Office has implemented comprehensive research on technology facilitated violence against women (TF VAW) in 13 countries of the ECA region: Albania, Bosnia and Herzegovina, Georgia, Kazakhstan, Kosovo,[5] Kyrgyzstan, Moldova, Montenegro,[6] North Macedonia, Serbia, Tajikistan, Türkiye, and Ukraine.

In 2023, UN Women produced a scoping review on the state of data and evidence on technology-facilitated VAW to review availability of data and highlight data gaps.[7] The comprehensive research presented in this report was designed based on the findings of that scoping review, with the aim to fill critical gaps and provide methodological lessons that can inform the further development of global standards for the measurement of technology-facilitated VAW.

PURPOSE AND OBJECTIVES

With this research, UN Women ECA intended to better understand the types and prevalence of TF VAW in the region and its consequences on women and women's attitudes, experiences and access to services, while at the same time exploring the existing normative and institutional context and role and perspective of relevant stakeholders in providing prevention and support services to survivors of such violence.

The importance of this research is multi-fold:

It provides insights in an area of VAW where there are still **critical data gaps and a lack of precise and systematic insights**.

It examines how various **key stakeholders perceive technology-facilitated VAW**, how they work with or around them, and their roles and capacities to address them adequately.

It offers **recommendations for global, regional and national processes** aiming at improving legislation, policies and institutional responses toward more effective prevention and protection related to TF VAW.

5 References to Kosovo shall be understood to be in the context of UN Security Council Resolution 1244 (1999).

6 Montenegro was not included in the web-based survey due to the cost of web-based randomized research in the context of a small population. However, Montenegro was included in the qualitative research, and having in mind similarities in the technology facilitated VAW and more broadly women's situation in the Western Balkan countries, the findings obtained from the web-based survey for neighbouring countries are very much valid for Montenegro as well.

7 Un Women, WHO, The state of evidence and data collection on technology-facilitated violence against women (2023), https://www.unwomen.org/en/digital-library/publications/2023/04/brief-the-state-of-evidence-and-data-collection-on-technology-facilitated-violence-against-women

RESEARCH COMPONENTS

The research included several components:

1. **Mapping of relevant normative and policy frameworks** at global, regional and national levels
2. Large scale web-based survey with the participation of over **12,000 women** across the region
3. **Qualitative research** aimed at capturing the perspective of governmental and non-governmental stakeholders and women's experiences with different forms of TF VAW.

Structure of the report

1. **Conceptual framework and research methodology**
2. **Normative and policy framework**
3. **Women's experiences with TF VAW**
4. **Stakeholder's engagement**
5. **Conclusions and recommendations**

Orange the World 2021 – Bosnia and Herzegovina.
Photo: © UN Women/Adis Novic

2 · CONCEPTUAL FRAMEWORK AND METHODOLOGY

2.1 CONCEPTUAL FRAMEWORK

One of the obstacles noted globally by various stakeholders is the lack of a unified, broadly agreed definition of technology-facilitated violence. Different organizations use different terms. For example, the EU uses the term cyber violence, while academic literature often references digital violence, etc. These differences are important because they reflect differences in the conceptual approach in understanding TF VAW and its scope – which specific forms it encompasses (for example, whether it encompasses only online violence or also offline forms that are linked to the use of technology in intimate partner, domestic or other form of violence perpetrated by persons from women's networks and environment).

The conceptual framework that was adopted for the purpose of this research, including the definition of technology-facilitated VAW, are informed by the ongoing discussion coordinated by UN Women and the WHO.[8] According to this discussion, TF VAW is understood as an expression of the gender-based discrimination that exists online and offline.[9] Offline and technology-facilitated VAW are not separate forms, but rather could be understood as a continuum in which some forms occur only offline, some occur only through the use of digital technologies, and many include both offline and technology-facilitated components.[10] Regardless, the risk factors, consequences and underlying causes – such as structural gender inequalities, misogyny and unequal power between women and men – remain the same. Violence and fear of violence can lead to self-censorship and the withdrawal of women, restricting their access to the internet and technologies which are of crucial importance for many aspects of social inclusion and participation, including in education, employment, politics and social life.

There are two main categories of technology-facilitated VAW, which are often overlapping rather than mutually exclusive:[11]

1) VAW that is committed using technology and that targets victims/survivors in digital spaces and online platforms (e.g., social media, dating apps through their digital devices);
2) VAW that occurs offline, such as domestic violence or sexual assault, that is aggravated by using technology, for example extending controlling behaviour through electronic tracking and surveillance of the victim/survivor.

While TF VAW has forms and characteristics similar to those of other forms of VAW, it has also some distinct features:

- Reach, transmission and speed: easy and rapid dissemination of information and content through multiple platforms comprised of vast networks;
- Lack of inhibition: enhanced anonymity offered by digital and virtual spaces through encryption and privacy protocols allows users to be uninhibited and to behave with impunity. It also presents particular challenges in identifying perpetrators;[12]
- Hard to eliminate: violent content becomes persistent, difficult to remove and therefore, re-traumatizing.

As with the basic definition of gender-based VAW, existing conceptualizations of technology-facilitated VAW are rooted in the ideology of men's entitlement and privilege over women, social norms regarding masculinity and the need to assert male control or power, enforce gender roles.[13] Additionally, technology-facilitated VAW often includes several key elements as emphasized by UN Women and the WHO in discussion on the definition of TF VAW:

- **Privacy**. Unauthorized access to and dissemination of data cause distress and damage. Personal information and data retrieved by a perpetrator made public with malicious intent clearly violates the right to privacy.[14] Further, breaches of privacy based on gender, gender identity and expression are a systemic form of denying human rights, frequently reflecting and perpetuating unequal social, economic, cultural and political structures and norms, with consequences for society as a whole.[15]
- **Consent** is an important element, particularly regarding the re-sharing of intimate sexual content originally intended solely for a specific individual recipient. Consent should be informed, active and ongoing. It may also be conditional and temporal (e.g., photos shared with intimate partners for the duration of the relationship).
- **Freedom of expression** is not restricted by the initiatives to eliminate TF VAW. Contrary to that, the elimination of TF VAW enhances freedom of expression by ensuring that women and girls are able to exercise their right to freedom of expression without fear of harassment and violence.

8 UN Women, WHO, joint programme on violence against women data, Foundational Expert Group Meeting (EGM) on Online and technology-facilitated violence against women and girls: Towards a common definition. Background Note. New York, USA, 15-16 November 2022.
9 Ibid.
10 Ibid, see also EIGE, Combating Cyber Violence against Women and Girls, 2022. https://eige.europa.eu/publications-resources/publications/combating-cyber-violence-against-women-and-girls?language_content_entity=en
11 Ibid.
12 On the other hand, anonymity is critical to protect privacy.
13 CEDAW, General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19.
14 UNSR VAW Report, para. 36.
15 Report of the Special Rapporteur on the right to privacy, 2018, https://digitallibrary.un.org/record/1656178

- **Harm** caused by TF VAW is real and diverse, affecting the mental and physical health of those targeted, undermining their confidence and autonomy, stigmatizing them and generating fear, shame, and professional and reputational damage.[16] The effect is also to silence women's voices by denying equal access to technology and the internet.
- **Perpetrators** may be primary (the person from whom the TF VAW content originates), or secondary (others who view, download and/or re-share the material). [17]
- **Victims/survivors** could be specific targets, groups of women and women in general, in the case of broader symbolic violence, such as misogyny spread through internet discourses and messages. Particularly vulnerable are adolescents (girls but also boys). Targets could be public figures, such as women politicians, journalists, celebrities and civil society advocates, who are often exposed to violence in order to be silenced. In some cases, victims are women and girls who are exposed to certain materials without their consent (such as rape videos or similar).
- **ICT intermediaries** are platforms, apps and other intermediaries that bring together or facilitate transactions between third parties online or in digital spaces. They give access to, host, transmit and index content, products and services originated by third parties on the internet or provide internet-based services to third parties. Their role in eliminating TF VAW is critical.

2.2 DEFINITION OF TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN

Until recently, the international community has lacked a shared definition of TF VAW, which has been one of the foremost challenges to collecting data and producing comparable research on this type of gender-based violence. Recognizing this key barrier, as a part of the Joint Programme on Violence against Women Data of UN Women and World Health Organization (WHO), an expert group meeting was convened in November 2022 with the aim to develop a common, comprehensive definition of TF VAW that could be used as the basis for developing tools to begin to fill the data gap around the prevalence and characteristics of TF VAW. The resulting definition builds on the work from academics, governments, national statistical offices, feminist movements, international organizations and other gender equality advocates.

Technology-facilitated violence against women is *'any act that is committed, assisted, aggravated or amplified by the use of 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.'*

Expert Group Meeting report
Technology-facilitated violence against women:
Towards a common definition (2023)[18]

In this definition, 'ICT' is an umbrella term that includes mobile phones, the internet, social media platforms, computer games, text messaging, email and other related technologies. In addition, the definition includes other digital tools, such as GPS, navigation systems and similar. In line with the guidance of the Report of the Special Rapporteur on violence against women and girls, its causes and consequences, this definition uses the term 'women' to include girls, whenever applicable, recognizing that young women and girls are often targets of technology-facilitated violence.[19] The definition also acknowledges that perpetrators of TF VAW use a variety of technology-based tactics to enact harm. Some of these are unique to digital contexts, including: doxing, gender-based trolling, hacking, cyber grooming, using fake accounts and image-based abuse.

TF VAW also includes behaviours that are not unique to digital contexts (e.g., harassment, stalking and exploitation) but may be assisted, aggravated or amplified by the use of ICTs or other digital tools. Essentially, this framing acknowledges that while TF VAW has its own distinct features, it is "part of the continuum of multiple, recurring and interrelated forms of gender-based violence."[20] It is also noted that while UN Women and WHO employ the term TF VAW, others may refer to technology-facilitated gender-based violence, but the common definition describing the phenomenon remains the same.

16 Irene Khan, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, A/76/258, 30 July 2021.
17 Aziz, Due Diligence and Accountability for Online Violence against Women (2017). https://duediligenceproject.org/wp-content/uploads/2019/05/Paper-on-Due-Diligence-and-Accountability-for-Online-Violence-against-Women-make-this-active-link.pdf
18 https://www.unwomen.org/sites/default/files/2023-03/Expert-Group-Meeting-report-Technology-facilitated-violence-against-women-en.pdf
19 UN Women, WHO, Technology-facilitated violence against women: taking stock of evidence and data collection, https://www.unwomen.org/en/digital-library/publications/2023/04/technology-facilitated-violence-against-women-taking-stock-of-evidence-and-data-collection
20 Ibid

Forms of TF VAW: a short indicative selection of commonly researched forms

'Sextortion' – use of ICT to blackmail a victim. In such cases, the perpetrator threatens to release intimate pictures of the victim in order to extort additional explicit photos, videos, sexual acts or sex from the victim.

'Doxing' – publication of private information, such as contact details, on the internet with malicious intent, usually with the insinuation that the victim is soliciting sex (researching and broadcasting personally identifiable information about an individual without consent, sometimes with the intention of exposing the woman to the "real" world for harassment and/or other purposes). It includes situations where personal information and data retrieved by a perpetrator is made public with malicious intent, clearly violating the right to privacy.

'Trolling' – posting of messages, the uploading of images or videos and the creation of hashtags for the purpose of annoying, provoking or inciting violence against women and girls. Many "trolls" are anonymous and use false accounts to generate hate speech.

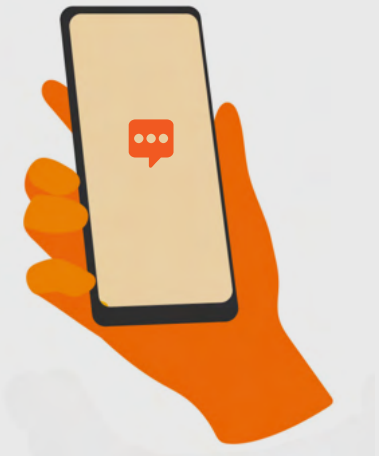
'Online mobbing and harassment' – online equivalents of mobbing or harassment on social platforms, the Internet, in chat rooms, instant messaging and mobile communications.

'Online stalking' – repeated harassment of individuals, perpetrated by means of mobile phones or messaging applications, in the form of crank calls or private conversations on online applications (such as WhatsApp) or in online chat groups.

'Online sexual harassment' – any form of online unwanted verbal or non-verbal conduct of a sexual nature with the purpose or effect of violating the dignity of a person, in particular by creating an intimidating, hostile, degrading, humiliating or offensive environment.

Non-consensual intimate image (NCII) abuse (often mischaracterized as 'revenge porn'[21]) – the non-consensual online dissemination of intimate images, obtained with or without consent, with the purpose of shaming, stigmatizing or harming the victim.

Report of the special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective.



21 The term 'revenge porn' is often used in discussions. However, the term should be avoided, as it minimizes the impact of this crime on people's lives. The term 'pornography' does not denote the non-consensual nature of the act, and the term 'revenge' only focuses on the presumed motive of the perpetrator, excluding the experience and rights of the victim. Moreover, many perpetrators are not motivated by revenge or by any personal feelings towards the victim and not all content may be understood popularly as pornographic.

2.3 RESEARCH METHODOLOGY

As noted, the research involved several components:

- Desk review of relevant documents and existing research on TF VAW
- Mapping of normative and policy framework relevant for TF VAW
- Large scale web-based survey
- Qualitative research

Desk review of relevant documents and existing research on TF VAW

A desk review was conducted during the preparatory stage of the research to conceptualize and design the methodology as well as to collect insights from existing literature and research on TF VAW conducted by UN Women, academia and other research organizations. The list of reviewed literature is provided in the references section.

Mapping of normative and policy framework

Because of resource constraints, the mapping was designed as a 'light mapping' and not an in-depth legal analysis. As such, it provides basic insights into processes focused on the development of legal and policy frameworks and the recognition and inclusion of online and technology facilitated violence in key conventions, laws and strategies/action plans at global, regional, and national levels. More detailed information on mapping methodology and documents reviewed can be found in Annex 1.

All legal and policy documents (listed in Annex 1) were reviewed directly, and not through secondary sources or policy analyses. In some countries with more elaborate frameworks, additional insights were provided, but still not in the form of thorough legislative and policy analysis.

The mapping was conducted with valuable linguistic and translation assistance from UN Women teams.

Web-based survey

A web-based survey was conducted from January to June 2023 by the independent research agency RIWI, which specializes in web-based surveys using a methodology particularly suited for sensitive topics such as violence against women (more on RIWI Methodology in Annex 1). The sample included 12,527 women aged 18 years and above, with at least 1,000 from each participating country: Albania (1,000), Bosnia and Herzegovina (1,106), Georgia (1,002), Kazakhstan (1,011), Kyrgyzstan (1,006), Kosovo (1,007), Moldova (1,001), North Macedonia (1,006), Serbia (1,200), Tajikistan (1,008), Türkiye (1,180), and Ukraine (1,000). The survey was offered in local languages and included 22 questions for all respondents and an additional 12 questions for those with experience of online and technology- facilitated violence.

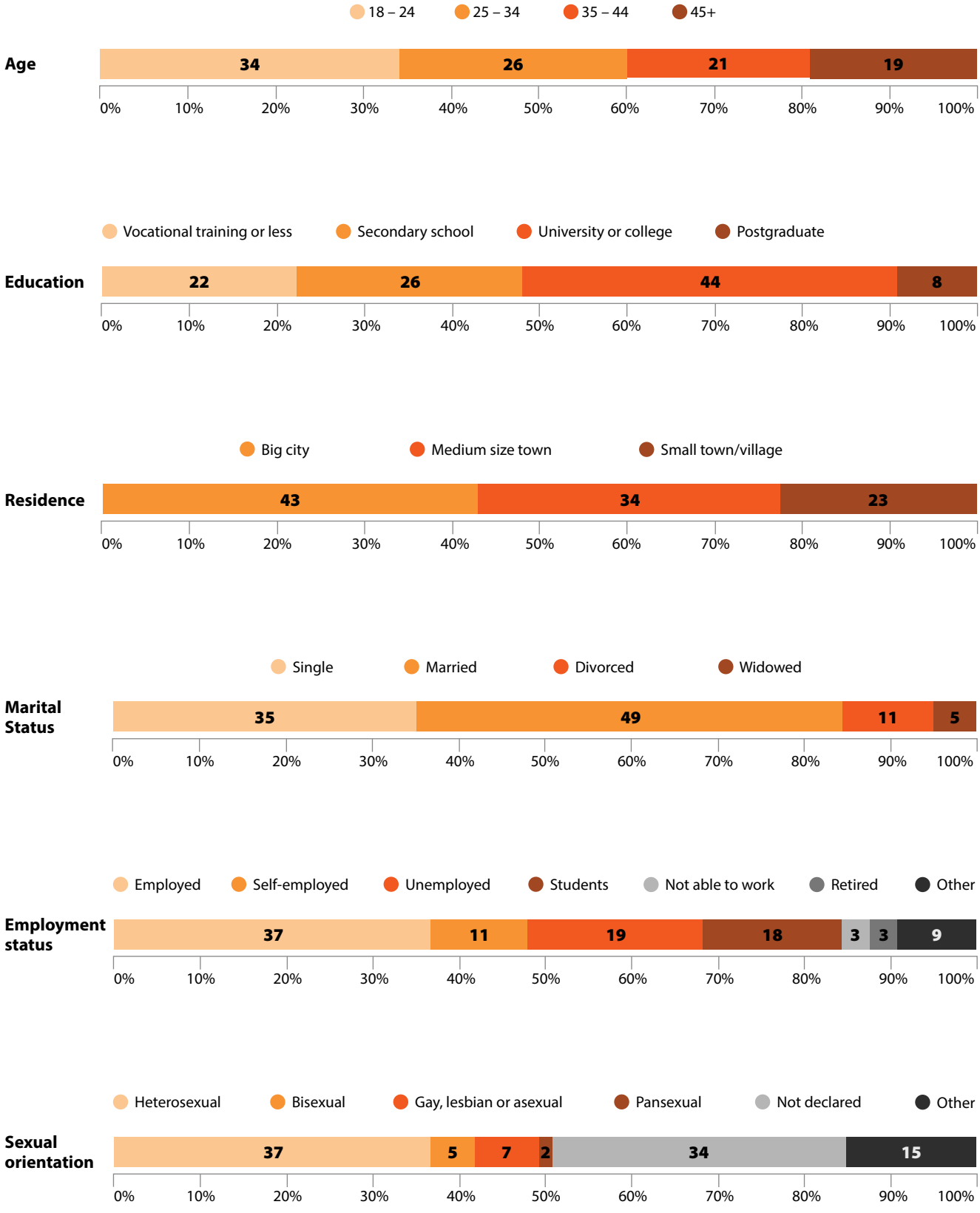
Operational definition of TF VAW. To adequately measure experiences of technology-facilitated violence (both overall prevalence and prevalence of specific forms), the questionnaire utilized act-based definitions. It provided a list of acts of TF VAW from which respondents could select, allowing for multiple responses. The questionnaire also included an "Other" option for respondents who felt the list wasn't comprehensive and wanted to report an act of violence not mentioned, as well as a "None of the above" option for those who hadn't experienced TF VAW. Those who selected any of the listed acts were categorized as **women who have experienced technology-facilitated VAW**:

a. Received inappropriate sexual advances or sexual content on social networking websites;
b. Been pressured to share sexually suggestive or explicit images / messages;
c. Had someone threaten to reveal / share personal information without their consent (such as images, contact information, sexually explicit content);
d. Private information was revealed without their consent (such as images, contact information, sexually explicit content);
e. Received unwanted or offensive content and/or messages;
f. Had someone monitor their phone calls, messages or posts to see who they are communicating with;
g. Had someone monitor their location in a way that made them feel controlled;
h. Their private accounts and web pages were hacked;
i. Received threats (e.g., of violence, towards family, etc.);
j. Photos manipulated and/or electronic defamation;
k. 'Others, please specify'.

Similarly, those who picked "None of the above" were grouped as **women who did not report having experienced TF VAW**.

Characteristics of the sample. As shown in Figure 1, the sample consisted of women of a variety of socio-demographic profiles, with a higher proportion of respondents who are young adults and middle aged, have secondary or tertiary education and live in larger cities. Respondents also tended to be married, employed and of heterosexual or undeclared sexual orientation.

Figure 1: Socio-demographic profile of women participating in the survey, regional level data



More details on the methodology of the web-based survey are available in Annex 1.

#orangetheworld – Kosovo. Photo: © UN Women and Office of the Development Coordinator, Arben Llapashtica

Qualitative research

Qualitative research was informed by the preliminary findings of the web-based survey. It was conducted with various stakeholders across all the 13 countries included in the research. The objective of this research component was to delve deeper into awareness and understanding, experiences related to handling cases of TF VAW, capacities, and challenges in addressing TF VAW in each country through targeted focus group discussions and semi-structured interviews. This component included:

- Focus groups and interviews with 57 representatives of civil society organizations (women's rights organizations, service providers for women survivors of VAW, activists, feminists, and gender experts);
- Focus group discussions and interviews with 20 representatives of state institutions and service providers in response to VAW, including representatives of cybercrime units;
- Interviews with 5 representatives of national gender equality mechanisms; and
- Interviews with 5 representatives of national human right independent (governmental) institutions.

Research design envisaged conducting the qualitative research activities with same stakeholders in each country, including representatives of CSOs, representatives of state service providers, a representative of the national gender equality mechanism, and a representative of human rights oversight institutions. However, the response rate varied: in some countries, all types of stakeholders were responsive, while in others only certain stakeholders participated. A detailed list of participants is presented in Annex 1.

The qualitative research encompassed several in-depth interviews with young women who had diverse experiences of TF VAW, who were identified with the assistance of CSOs. It also included media-based research and analysis of specific cases of TF VAW, offering more detailed insights or showcasing particular examples of TF VAW.

Ethical principles

The research was designed and its components implemented with strict ethical protocols, ensuring the highest standards pertinent to the sensitive research topic. This was done to prevent any harm to respondents, including potential secondary victimization for individuals with experience of GBV, and to ensure voluntary participation, confidentiality, and anonymity. The ethical protocols were crafted in accordance with UN Women's principles on research ethics[22] and programming and WHO ethical and safety recommendations for intervention research on VAW.[23]

Rigorous ethical standards were also applied to data access and storage, as well as presentation of findings. The original dataset is fully anonymized to ensure that no data could be used to reveal the identity of respondents. Data protection protocols, designed according to the highest standards by the data collection company, established data safety in storage and transfer and in later stages of analysis (more details in Annex 1). While anonymity and confidentiality were relatively easy to ensure for quantitative data, the qualitative research required more careful data management. Despite the fact that qualitative research encompassed a diversity of stakeholders, some are unique and could be easily identified if their institution and country were specified. Given the research's commitment to confidentiality and anonymity for all respondents, the qualitative component of the report consistently avoids references that might disclose their identities. Thus, when sources are cited, only one background characteristic is mentioned – either the type of institution/organization or the country/sub-region.

22 UN Women, Principles of research ethics, https://wrd.unwomen.org/practice/resources/principles-research-ethics

23 WHO, Ethical and safety recommendations for intervention research on violence against women, https://www.who.int/publications/i/item/9789241510189

Women rebuild lives, advocate for each other.
Photo: © UN Women/Norman Gorecho

3 · NORMATIVE AND POLICY FRAMEWORK

KEY FINDINGS:

- International, regional and national actors are still in the early stages of addressing technology-facilitated violence against women (TF VAW), and the countries included in this research are no exception.
- Global processes have intensified during the last several years, driven by the concurrent processes undertaken by the UN General Assembly, Secretary General, UNSRVAW and Commission on the Status of Women (CSW), which have been supported by the work of UN Statistical Commission,[24] WHO and UN Women. These processes advance the development of a common understanding to enable further progress regarding legal frameworks, data collection, research and statistics and other initiatives. Gender mainstreaming of the International Convention on countering the use of information and communications technologies for criminal purposes adds to the number of ongoing processes related to developing legal instruments to prevent and combat TF VAW.
- European regional processes are marked by various initiatives of the Council of Europe and EU. One of the crucial milestones is the effort to reaffirm the Istanbul Convention and its relevance for TF VAW in GREVIO recommendation No. 1.
- As with most countries worldwide, countries in the ECA region do not have an adequate legal and policy framework to address TF VAW. This mapping exercise showed that only in a few cases key laws address TF VAW directly, at least to some extent. The same is found for current gender equality and EVAW policies.

Technology-facilitated violence against women is not a new phenomenon, having developed jointly with information and communication technologies and globalizations processes. However, attention to this form of violence increased during the COVID-19 pandemic when the use of the internet and other ICT communications increased in response to anti-COVID measures that restricted in-person communication. In this chapter, we provide an overview of processes that initiated or contributed to increased attention and work on this issue in the areas of conceptualization, data collection, research, as well as to the improvement of international legislative and policy framework in response to it. The chapter also provides an overview of the current positioning of TF VAW in key global human rights conventions and platforms. The EU framework is also included as relevant for ECA countries, whether through EU enlargement or EU neighbourhood policies, which influence the framework and response to VAW.

3.1 GLOBAL INSTRUMENTS AND INITIATIVES

3.1.1 Key processes

Until recent years, the focus on gender equality and women's rights in the context of technology was more directed towards areas such as education, employment and empowerment, and less on the issue of VAW. To inform the negotiations of the 67th session of CSW, UN Women conducted in 2022 an analysis of normative frameworks on gender perspectives in technology and innovation.[25] The overview of initiatives and milestones presented in that analysis shows that since the Fourth World Conference on Women in 1995, the **Commission on the Status of Women has adopted agreed conclusions related to gender equality in the context of technology twice** – in its 47th session (2003) related to ICT and media-based violence against women and in its 55th session (2011) related to women's and girl's access to technology with a focus on education and training in the field of science and technology and their employment in these sectors. Otherwise, the number of references related to technology in agreed conclusions of sessions have been minimal, and the primary focus has remained on access to technology, the digital gender divide, innovation and technology in education and employment.[26]

Since then, the UN General Assembly, the Human Rights Council and the Committee on the Elimination of Discrimination against Women have drawn attention to the issue of TF VAW. In its **2014 resolution 68/181, the General Assembly** expressed concerns regarding technology-related violations and abuses against women human rights defenders.[27] The **CEDAW Committee included mention of TF VAW in its General recommendation No. 36 (2017)**.[28]

24 At the 54th Session (2023) of the UN Statistical Commission, the need for methodological work to measure technology – facilitated was recognized: https://unstats.un.org/UNSDWebsite/statcom/54

25 UN Women (2022). Normative frameworks on gender perspectives in technology and innovation.

26 Ibid.

27 https://digitallibrary.un.org/record/764453

28 https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-recommendation-no-36-2017-right-girls-and

The **Human Rights Council issued a resolution 38/5 (2018)** on preventing and responding to violence against women and girls in digital contexts.[29]

One of the cornerstones of UN global initiatives to improve the international framework in response to GBV and VAW was the 2018 **Report of the Special rapporteur on violence against women, its causes and consequences (UNSRVAW) on online violence against women and girls from a human rights perspective**.[30] The report noted that *'even though the core international human rights instruments, including those on women's rights, were drafted before the advent of ICT, they provide a global and dynamic set of rights and obligations with transformative potential, and have a key role to play in promotion and protection of fundamental human rights, including a woman's rights to live a life free from violence, to freedom of expression, to privacy, to have access to information shared through ICT and other rights'* (Para 13). The UNSRVAW recommended that the relevant UN treaty bodies should coordinate with the support of OHCHR and UN Women to tackle human right violations in general and online, particularly related to online violence against women, in their work, reports and recommendations (Para 92). States were recommended to implement the principle that the human rights and women's rights protected offline should be protected online by the ratification and implementation of all core human rights treaties (Para 94), and that States should, in accordance with the principle of due diligence, enact new laws and measures to prohibit new emerging forms of online GBV (Para 95).

The resolution on countering the use of information and communications technologies for criminal purposes, adopted by the General Assembly in 2019 (A/RES/74/247),[31] launched the establishment of an open-ended ad hoc intergovernmental committee of experts and representatives of all regions to elaborate a comprehensive international convention on countering the use of information and communications technologies for criminal purposes, taking into full consideration existing international instruments and efforts at the national, regional and international levels (Para 2). The ad-hoc group was established in May 2021 and as of April 2023 had organized five sessions. The last working version of the document reflects the efforts to mainstream gender and address gender-based violence against women and girls.

In **December 2020, UN General Assembly adopted Resolution on Intensification of efforts to prevent and eliminate all forms of violence against women and girls** (A/RES/75/161), demonstrating increased commitment to this cause.[32] In the Resolution, the General Assembly *'calls upon all United Nations bodies, entities, funds and programmes and the specialized agencies and invites the Bretton Woods institutions to intensify their efforts at all levels to eliminate all forms of violence against women and girls and to better coordinate their work, with a view to increasing effective support for national efforts to prevent and eliminate sexual harassment'* (Para 24). The Resolution requested a report from the Secretary General based on information from UN bodies, funds, programmes and special agencies and on information provided by States.

The global framework was further developed with **Council's resolution on Right to privacy in the digital age (48/4)** (2021),[33] and corresponding **General Assembly resolution (A/RES/75/176) which recognizes the importance of the right to privacy to prevent gender-based violence** and calls for implementing and strengthening gender-responsive policies on privacy.[34] The action against technology-facilitated violence is also becoming increasingly significant for child protection. The Committee on the Rights of the Child in its General Comment No. 25 (2021) calls for the protection of children against technology-facilitated violence and online sexual exploitation and abuse.[35]

All these efforts are further strengthened by global advocacy efforts led by **multistakeholder initiatives** for catalytic action to address TF VAW, including through two of the **Generation Equality Action Coalitions** convened by UN Women: the Action Coalition on Gender-Based Violence and the Action Coalition on Technology and Innovation for Gender Equality, and the **Global Partnership on Action on Gender-Based Online Harassment and Abuse,** for which UN Women is the Technical and Policy Lead.

In August 2022, pursuant to the General Assembly Resolution on Intensification of efforts to prevent and eliminate all forms of violence against women and girls, **the Secretary General submitted a report on Intensification of efforts to eliminate all forms of violence against women and girls** (A/77/302).[36] The Report, for which UN Women analyzed data and coordinated information submitted by 35 Member States and around 10 UN agencies, was focused on the urgent need to address VAW in digital contexts and contains information on measures taken by Member States and entities of the UN system to address VAW and contains conclusions and specific recommendations for future action.

29 https://www.ohchr.org/en/hr-bodies/hrc/regular-sessions/session38/res-dec-stat
30 https://digitallibrary.un.org/record/1641160?ln=en#record-files-collapse-header
31 https://documents-dds-ny.un.org/doc/UNDOC/GEN/N19/440/28/PDF/N1944028.pdf?OpenElement
32 https://digitallibrary.un.org/record/3896021?ln=en
33 https://daccess-ods.un.org/tmp/7922586.79866791.html
34 https://digitallibrary.un.org/record/3896430?ln=en
35 https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation
36 https://digitallibrary.un.org/record/3988297?ln=en

As already noted, in November 2022, UN Women convened 29 diverse stakeholders from 26 inter-governmental organizations, government agencies, civil society, and the academia, including gender policy specialists, researchers, academics and statisticians to develop a shared definition which builds on previous work from academics, governments, national statistical offices, feminist movements, international organizations and other gender equality advocates. As an outcome, an agreement on a common definition was reached, as presented in the previous chapter.[37] Following the dissemination of the proposed common definition, in early March 2023, the UN Statistical Commission in its 54th session called for the inclusion of measurement of TF VAW in the agenda of the 55th session.[38]

The 67th session of the Commission on the Status of Women, convened in March 2023, as a priority theme had "Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls." In the agreed conclusions, the Commission *'recognizes the need to ensure that human rights are promoted, respected and fulfilled in the conception, design, development, deployment, evaluation and regulation of technologies and to ensure that they are subject to adequate safeguards in order to promote an open, secure, stable, accessible and affordable information and communications technology environment for all women and girls'* (Para 15). The Commission further recognizes that *'while technology can be used to promote women's and girls' full realization of civil, political, economic, social and cultural rights, it can also be used to perpetuate gender stereotypes and negative social norms and create vicious cycles, in which inequalities are amplified and perpetuated through digital tools, and also recognizes the need to address the impact of structural barriers to the realization of those rights'* (Para 17). The agreed conclusions propose concrete recommendations for governments, intergovernmental bodies and other institutions, civil society actors and other relevant stakeholders, to be implemented at the international, national, regional, and local level.[39]

3.1.2 Key conventions

International human rights instruments set out States' obligations to combat all forms of discrimination against women, including technology-facilitated violence against women, and to protect their human rights, including every woman's right to be free from violence. As pointed out in the Report of the UNSRVAW on technology-facilitated violence against women and girls from a human rights perspective, core women's human right instruments, such as the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), the Declaration on the Elimination of Violence against Women and the Beijing Declaration and Platform for Action, predate the development of the Internet and ICT, and consequently the emerging forms and modes of perpetration of technology-facilitated violence against women.

The Convention on the Elimination of All Forms of Discrimination against Women has been progressively analyzed by the Committee on the Elimination of Discrimination against Women, which has addressed technology-facilitated violence against women in several general recommendations and concluding observations.

In its general recommendation No. 35 (2017), which complements and updates the guidance to States parties set out in general recommendation No. 19, the Committee made clear that the Convention was fully applicable to technology-mediated environments. The Committee notes that *'… gender based violence against women remains pervasive in all countries, with high levels of impunity. It manifests itself on a continuum of multiple, interrelated and recurring forms, in a range of settings, from private to public, including technology-mediated settings and in the contemporary globalized world it transcends national boundaries' (Para 6). It is also noted that 'Gender-based violence against women occurs in all spaces and spheres of human interaction, whether public or private, including in the contexts of the family, the community, public spaces, the workplace, leisure, politics, sport, health services and educational settings, and the redefinition of public and private through technology-mediated environments, such as contemporary forms of* ***violence occurring online and in other digital environments****.'* (Para 20).

The Human Rights Council:
'All forms of discrimination, intimidation, harassment and violence in digital contexts prevent women and girls from fully enjoying their human rights and fundamental freedoms…'

37 UN Women, WHO, The state of evidence and data collection on technology-facilitated violence against women (2023), https://www.unwomen.org/en/digital-library/publications/2023/04/brief-the-state-of-evidence-and-data-collection-on-technology-facilitated-violence-against-women

38 https://unstats.un.org/UNSDWebsite/statcom/54

39 https://www.undocs.org/E/CN.6/2023/L.3

Jonada and her team believe their app can make a difference.
Photo: © UN Women/ Eduard Pagria

The Recommendation emphasized the overarching obligation of State parties to pursue a policy of eliminating discrimination against women, including gender-based violence against women. States are required to adopt legislation prohibiting all forms of gender-based violence against women and girls, harmonizing national law with the Convention.

In its general recommendation No. 34, the Committee highlighted the important role of ICT in transforming social and cultural stereotypes about women, as well as its potential in ensuring effectiveness and efficiency of women in their access to justice. In its general recommendation No. 36 (2017) on the right of girls and women to education, the Committee also recognized how girls are affected by cyberbullying, particularly in relation to their right to education.

The Human Rights Council has adopted various resolutions that are relevant for combating TF VAW. HR Council Resolution 38/5 (2018) is fully focused on accelerating efforts to eliminate violence against women and girls and prevent and respond to violence against women and girls in digital contexts. Condemning all forms of VAW and expressing deep concern that *'all forms of discrimination, intimidation, harassment and violence in digital contexts prevent women and girls from fully enjoying their human rights and fundamental freedoms…',* the Council calls upon States to take immediate and effective action to prevent all forms of VAW, including in digital contexts, by developing inclusive policies; integrating gender perspective in legislation, programmes, projects, strategies and regulatory and technical instruments in the area of digital technologies; and supporting initiatives undertaken by other stakeholders, such as international and non-governmental organizations, business enterprises, faith and community groups, religious leaders, journalists and human right institutions. The Council calls upon states to take immediate and effective action to respond to all forms of VAW, including in digital contexts by holding perpetrators to account and combating impunity, ensuring that legislation allows for timely and effective investigation, prosecution, sanction and redress of VAW in digital contexts.[40]

The International Convention on countering the use of information and communications technologies for criminal purposes is still under development. The latest version, which resulted from the April 2023 ad-hoc working group meeting, contains revisions that clearly point to gender mainstreaming within the Convention and recognizing the specific gender dimension of cybercrime.

40 https://documents-dds-ny.un.org/doc/UNDOC/GEN/G18/214/82/PDF/G1821482.pdf?OpenElement

3.2 EUROPEAN NORMATIVE AND POLICY FRAMEWORK

The regional European framework is relevant for the 13 ECA countries which are in the focus of this research for several reasons: nine out of 13 ECA countries[41] are members of the Council of Europe, and eight are EU candidate countries[42] while two are potential candidates.[43] Moldova, Ukraine and Georgia are part of the Eastern Partnership countries. Therefore, the Council of Europe and EU legal and policy instruments are relevant for the majority of countries within this research, whether due to their obligation to synchronize legislation as requested by the EU accession processes or because they are affected by the European framework through external action, cooperation initiatives and access to funds.

3.2.1 Council of Europe

The Council of Europe has been active in addressing TF VAW. A review of its legal instruments indicates that some treaties directly target TF VAW, while others may be indirectly applicable.

The main legal instrument in the European region addressing VAW is the **Council of Europe Convention on preventing and combating violence against women and domestic violence** (Istanbul Convention). Signatories among countries included in this research are Albania (signed 2011, ratified 2013), Bosnia and Herzegovina (signed and ratified in 2013), Georgia (signed 2014, ratified 2017), Moldova (signed 2017, ratified 2022), Montenegro (signed 2011, ratified 2013), North Macedonia (signed 2011, ratified 2017), Serbia (signed 2012, ratified 2013), and Ukraine (signed 2011, ratified 2022). Türkiye is former signatory which withdrew from the Convention in 2021.[44] Kosovo is not a signatory but has included in its national Constitution the principles of the Istanbul Convention, making them directly applicable in national legislation.

The Istanbul Convention applies to all forms of violence against women, including domestic violence, and shall apply in every situation in which women are targeted by violence (Article 2). While the Convention's original text does not contain an explicit reference to technology facilitated violence against women, its scope as defined in the Article 2 extends to violence committed in online spaces and through ICTs. Analysis of the applicability of the Istanbul Convention to TF VAW reveals that several articles of the Convention are applicable in the digital context, specifically those related to sexual harassment and stalking. It is also noted that the application of Article 34 in online spaces is affirmed in the explanatory text of the Convention, which explicitly classifies 'the pursuit of any active contact with the victim through any available means of communication, including modern communication tools and ICTs' as unwanted contact. In view of the serious psychological consequences that many forms of TF VAW can have, the Istanbul Convention's requirements to criminalize psychological violence (Article 33) hold great importance.[45]

The monitoring body of the implementation of the Istanbul Convention is the Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO). In October 2021, GREVIO issued **Recommendation No. 1**[46] to highlight the digital dimension of VAW, noting that *'information and communication technology has enabled the perpetration of violence against women on a scale previously unknown'* (Para. 10). It is noted that digital forms of GBV against women can be particularly pronounced for women and girls at risk of or exposed to intersecting forms of discrimination. It is also mentioned that some State Parties have taken steps to introduce new criminal offences to capture specific harm perpetrated online, and where these steps are taken, the emphasis is placed on ensuring a person's safety, reputation or property. *'Many domestic laws fail to reflect other important impacts of acts of such violence, including social, economic, psychological and participatory harms. Very few consider and specifically address the compound experiences of women and girls and do not place it in the context of a continuum of violence against women that women and girls are exposed to in all spheres of life, including the digital sphere'* (Para. 16). With this recommendation, GREVIO intends to position manifestations of violence against women and girls in the digital sphere as expressions of gender-based violence against women covered by Istanbul Convention. This interpretation of the Istanbul Convention clarifies the relevance of this treaty in relation to the digital dimension of VAW.

The Council of Europe Convention on Cybercrime (the Budapest Convention) is the first and most relevant regional legally binding treaty focusing on cybercrime and electronic evidence.[47] Among ECA countries taking part in this research, the signatories include Albania, Bosnia and Herzegovina, Georgia, North Macedonia, Montenegro, Moldova, Serbia, and Ukraine.

41 Albania, Bosnia and Herzegovina, Georgia, Moldova, North Macedonia, Serbia, Türkiye and Ukraine
42 Albania, Bosnia and Herzegovina, Moldova, Montenegro, North Macedonia, Serbia, Türkiye and Ukraine
43 Georgia and Kosovo
44 https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=210
45 Adriane van der Wilk, Protecting Women and Girls from Violence in the Digital Age. The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women, Council of Europe, 2021, https://rm.coe.int/the-relevance-of-the-ic-and-the-budapest-convention-on-cybercrime-in-a/1680a5eba3
46 https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147
47 https://www.coe.int/en/web/cybercrime/the-budapest-convention

The convention requires parties to criminalize offences perpetrated against or by means of computer data and systems, content-related offences pertaining to the production, distribution or possession of child sexual abuse material (CSAM) as well as infringements of copyright and related rights. Parties to the convention are required to strengthen their domestic criminal procedural laws and equip judicial systems with the means to secure electronic evidence in relation to any offence, as well as to effectively facilitate international cooperation and mutual legal assistance regarding investigation and prosecution of cybercrime and other offences involving electronic evidence.[48]

The Budapest Convention does not refer explicitly to GBV or VAW in the context of cybercrime. However, the analysis of the applicability of the Convention to VAW concluded that the Budapest Convention through a number of substantive criminal law provisions addresses directly and indirectly some types of TF VAW, while other provisions address acts facilitating these types of violence.[49]

The Council of Europe recommendation on preventing and combating sexism was adopted in 2019. This document contains the first regionally agreed definition of sexism, including online and via new technologies, and reaffirms the existence of a continuum of violence affecting women and girls. Sexism is defined as *'any act, gesture, visual representation, spoken or written words, practice or behaviour based upon the idea that a person or a group of persons is inferior because of their sex, which occurs in the public or private sphere, whether online or offline, with the purpose or effect of violating dignity or rights of person, resulting in physical, sexual, psychological or socio-economic harm or suffering, creating an intimidating, hostile, degrading, humiliating or offensive environment, constituting a barrier to the autonomy… maintaining and reinforcing gender stereotypes.'*[50]

The Council of Europe Convention 108+ aims at data protection. The scope of application of the protection includes both automated and non-automated processing of personal data and guarantees the protection of sensitive data such as genetic and biometric data as well as a "right to erasure."

The Council of Europe Convention on the Protection of Children against sexual exploitation and sexual abuse (Lanzarote Convention) was adopted in 2007.[51] This is the first regional treaty specifically dedicated to the protection of children from sexual violence. The Convention requires states to offer a holistic response to sexual violence against children through the '4 Ps approach': prevention, protection, prosecution and promotion of national and international cooperation. The Lanzarote Committee is the body established to monitor how the State parties to the Convention are effectively putting it into practice in legislation and policy.

The Council of Europe Gender Equality Strategy 2018-2023 reaffirms the existence of forms of discrimination and violence affecting women's rights, safety and security online and offline. The Strategy highlights the idea of a continuum of VAW online and offline.

3.2.2 European Union

In the EU, several directives and regulations are directly or indirectly applicable to technology facilitated violence against women. However, there is not yet a harmonized definition or legal instrument.[52] The EU framework uses the term 'cyber violence against women' (CVAW).

The European Commission recently adopted a **Proposal for a directive on combating VAW and domestic violence**. The proposal includes a harmonized definition of cyber violence as 'any act of violence covered by this Directive that is committed, assisted or aggravated in part or fully by the use of information and communication technologies.' The proposal includes the criminalization of some common forms of cyber violence, including cyber stalking, cyber harassment, non-consensual sharing of intimate images and cyber incitement to violence or hatred.[53]

The proposal of the Directive is still under discussion. Meanwhile, several other EU directives and regulations are directly or indirectly applicable to 'cyber VAW.'

Victim's rights directive (Directive 2012/29/EU)[54] aims to ensure victims of all forms of crime across the EU are well informed of their rights, know where they can seek recourse and protection, are able to participate in criminal proceedings, and are acknowledged and treated equally and respectfully. The directive protects victims of crime as defined under national laws. It is therefore applicable to forms of cyber VAW that are criminalized in a Member State.[55]

48 Ibid.
49 Ibid, p. 19.
50 Ibid, p. 21
51 Signatory countries among 12 ECA countries included in the research: Albania, Bosnia and Herzegovina, Georgia, Moldova, North Macedonia, Serbia, Türkiye and Ukraine. More information available at https://www.coe.int/en/web/children/lanzarote-convention
52 EIGE, Combating Cyber Violence against Women and Girls, 2022, https://eige.europa.eu/publications-resources/publications/combating-cyber-violence-against-women-and-girls
53 Ibid, p. 19
54 Currently under revision by the European Commission.
55 Ibid, p. 20

EU definition

'Cyber-violence against women is an act of gender-based violence perpetrated directly or indirectly through information and communication technologies 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 hindrances to the use of their fundamental rights and freedoms.
Cyber-violence against women is not limited to but includes violations of privacy, stalking, harassment, gender-based hate speech, personal content sharing without consent, image-based sexual abuse, hacking, identity theft, and direct violence.
Cyber-violence is part of the continuum of violence against women: it does not exist in a vacuum; rather, it both stems from and sustains multiple forms of offline violence.'

European Commission
Advisory Committee on Equal Opportunities
for Women and Men, 2020

Directive on combating sexual abuse and exploitation of children and child pornography (Directive 2011/93/EU)[56] covers both offline and online forms of child sexual abuse. It protects minors from non-consensual intimate image abuse and obliges Member States to promptly remove child abuse materials within their territory and to endeavour to secure the removal of materials hosted elsewhere. Directive mentions girls as recipients of specific gender-based forms of cyber violence.

The European Union's General Data Protection Regulation (GDPR) regulates the collection and processing by individuals, companies or organizations of personal data from individuals in the EU.[57] The regulation improves individuals' rights towards the control, the erasure, the rectification, the restriction or the objection to personal data processing and facilitates their access to and transfer of their personal data, including image data such as non-consensual intimate images. The regulation also obliges companies and entities that process data to request explicit consent from the users.

The Regulation offers the potential to cover some aspects of TF VAW, as it demands, for example, that companies integrate privacy by design into their products or that individuals responsible for uploading image-based sexual abuse material as well as publishers of such material are considered joint data controllers and hence fall under the obligations and sanctions imposed by the GDPR. Moreover, the GDPR also contains a "right to erasure," better known as the right to be forgotten.[58]

The Directive on the implementation of the principle of equal opportunities and equal treatment of men and women in matters of employment and occupation (recast) (Directive 2006/54/EC) replaces a series of previous EU directives that constituted the foundation of the framework for equal treatment of men and women.[59] The directive is applicable to some forms of TF VAW, such as cyber harassment, but does not explicitly mention the online aspects and it is limited to matters of employment and occupation.

Directive on certain legal aspects of information society services, in particular electronic commerce, the Internal Market ('Directive on electronic commerce) (Directive 2000/31/EC), among other things, obliges service providers to remove or disable access to illegal content hosted on their platforms.[60]

The Directive on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual media services directive) (Directive 2010/13/EU) aims to protect minors from inappropriate content and all users from content 'containing incitement to violence or hatred directed against a group of persons or a member of such a group defined by reference to sex, race, colour, religion, descent or national or ethnic origin'.[61] It also contains provisions for reporting and flagging illegal and hateful content. This applies to television programmes, video-on-demand services and video-sharing platforms, including social media essentially devoted to video sharing.[62]

56 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32011L0093
57 Regulation (EU) 2016/679, available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj
58 Van der Wilk, 2021, p: 23
59 Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32006L0054
60 Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32000L0031
61 Available at: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32010L0013
62 Van der Wilk, 2021, p. 20

The EU Gender Equality Strategy acknowledges technology-facilitated violence against women. The Strategy states that TF violence targeting women has become pervasive and results in unacceptable consequences for women and girls. *'Bullying, harassment and abuse on social media have far-reaching effects on women's and girls' daily lives.'*

Having entered into force in November 2022, the **Digital Services Act (DSA)** [63] aims to create a safer digital space in which the fundamental rights of all users of digital services are protected.[64] The DSA defines clear responsibilities and accountability for providers of intermediary services, such as social media and online marketplaces. The rules are designed asymmetrically, which means that larger intermediary services with significant societal impact are subject to stricter rules.[65] The Digital Services Act is a step towards ensuring that women and girls have safer and more equal experiences online. In particular, the inclusion of GBV as a systemic risk within the DSA aligns with the EU's aim to criminalize certain forms of technology-facilitated GBV within the aforementioned Proposal for a directive on combating violence against women and domestic violence, published in March 2022.

The Directive on preventing and combating trafficking in human beings and protecting its victims (Directive 2011/36/EU) is indirectly relevant because of its strong gender dimension and the use of digital networks to commit these crimes.[66]

Two additional relevant legislative initiatives are currently ongoing: the ePrivacy regulation[67] and the Artificial Intelligence (AI) Act .[68] The former aims at improving online privacy, particularly considering online interactions between citizens and businesses, while the latter contains some instruments to address gender-based discrimination in AI systems and creates special rules for AI technologies that pose high risk to the health, safety and fundamental rights of individuals.[69]

The EU Strategy on Victim's Rights defines cybercrime as 'any type of a criminal offence that is committed online or with a use of computer or online tools.' The Strategy proposes remedies such as protection of privacy, liability of intermediaries and securing of digital evidence.[70]

The EU Code of conduct on countering illegal hate speech online was signed between the European Commission and Facebook, Microsoft, Twitter, YouTube (2016), Instagram, Snapchat, Dailymotion (2018), Jeuxvideo.com (2019) and TikTok (2020). The signatories to the code of conduct have committed to reviewing reports of hate speech on their platforms and to responding to unlawful content within 24 hours. The Code is being updated in the light of the DSA, which provides comprehensive rules for platforms' responsibilities and will further support co-regulatory frameworks. The most common ground for hate speech online in 2020 was sexual orientation, accounting for 33% of reports. This is explained partially by the fact that "organizations working on LGBTQI rights have been more active in flagging content." The major flaw of this monitoring activity is the lack of data disaggregation and the lack of overall transparency on reports and removals. Intersectional attacks are not accounted for, making it complicated to fully understand the phenomenon of hate speech online that contains a strong intersectional dimension and thus trivializing the experience of many women users.[71] The most recent evaluation of the Code of Conduct released by the European Commission in 2022 showed a decrease in companies' notice-and-action results.[72]

UN Women launches a STEM School in Kazakhstan. Photo: © Caravan of Knowledge

63 EUR-Lex – 32022R2065 – EN – EUR-Lex (europa.eu)
64 Available at: https://eur-lex.europa.eu/eli/reg/2022/2065
65 See also: https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package
66 Ibid, p. 20.
67 More information available at: https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation
68 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206
69 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021PC0206
70 Van der Wilk, 2021, p. 22
71 Ibid, p. 24.
72 More information available at https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7109

3.3 NATIONAL FRAMEWORKS IN ECA COUNTRIES

National legislation in ECA countries does not provide an adequate framework for combating technology facilitated violence against women. Only in a few countries do criminal codes include provisions that directly address some form of TF VAW, but in almost all cases, these provisions are not gender sensitive or designed to address gender-based violence (such in the case of identity theft, account hacking, abuse of personal data, etc.). Even specialized laws fully dedicated to prohibiting and sanctioning VAW do not recognize specific forms of TF VAW. Only North Macedonia has some provisions that directly recognize use of ICT in the perpetration of violence. Besides, where such laws exist, they are mostly limited to domestic violence. National overarching policies for gender equality do not address the issue of TF VAW, while in several countries this violence is at least partly addressed through specialized action plans for preventing and combating violence against women and domestic violence (Table 1).

Table 1: Overview of national legislation and strategies that directly address TF VAW

Country	Criminal code	Specialized law on GE, VAW/DV	Gender Equality Strategy	Specialized VAW/ DV strategy
Western Balkans				
Albania	↓	↓	↓	–
BiH – state level	↓	↓	–	–
BiH – FBiH	↓	↓	–	–
BiH – Republika Srpska	↓	↓	–	–
Kosovo	↓	↓	↓	↗
Montenegro	↗	↓	↓	–
North Macedonia	↗	↗	↓	–
Serbia	↗	↓	↓	↗
Türkiye				
Türkiye	↗	↗	↓	↗
Eastern Europe				
Georgia	↗	↓	↓	↓
Moldova	↓	↓	↓	–
Ukraine	↓	↓	–	–
Central Asia				
Kazakhstan	↓	↓	–	–
Kyrgyzstan	↓	↓	↓	–
Tajikistan	↓	↓	↓	↓
Legend				
↑	Law/policy **directly** addresses TF VAW as defined by UN Women in **majority** of forms			
↗	Law/policy **directly** addresses **some** forms of TF VAW as defined by UN Women			
↓	Law/policy at best **only indirectly** addresses some forms of TF VAW			
–	There is no such law or strategy			

3.3.1 Western Balkans

Western Balkan countries are at different stages of aligning their Criminal Codes to the Istanbul Convention, and all have special laws addressing domestic violence. Only in North Macedonia the special law more broadly includes gender-based violence against women, while in other countries the special law is limited to domestic violence and is not gender specific. All countries except Bosnia and Herzegovina[73] have active Gender Equality Strategies. While in Albania and North Macedonia, gender-based violence against women is included in the main Gender Equality Strategy, in Serbia and Kosovo there are separate Strategies for prevention and combating gender-based violence against women and domestic violence.

The legal and policy framework is currently not adequate for the prevention and protection of women from TF VAW. Except in North Macedonia and Serbia, criminal codes do not directly address any forms of TF VAW. Even specialized laws do not directly address TF VAW, except in North Macedonia.

The mapping results indicate following:

- When elements of technology-facilitated crimes are included in criminal codes, they systematically lack a gender perspective as well as specific reference to gender-based violence (for example identity theft; unauthorized taking of photos, videos, recording; breach of data privacy, etc.).
- When there is more direct focus on gender-based violence, it is only in the context of child pornography and does not target the protection of adult women from sexual abuse and exploitation in pornographic materials.
- The law can be indirectly applied to prevention and protection from different forms of VAW, such as threats, psychological violence, stalking, sexual harassment, but currently the protection in relation to these forms of violence is not explicitly linked to TF VAW.
- When there are references to TF VAW in policies, this is mainly related to prevention and awareness-raising on the dangers of technology-facilitated violence rather than protection, improvement of security or sanctioning.
- As the implementation of laws and policies in the region is often ineffective, such indirect references to TF VAW are far from sufficient to provide adequate prevention and protection.

Indirect legal provisions are not enough

It appears that one of the most common forms of TF VAW in the region is shaming women by publishing their intimate photos or videos without their consent. The Criminal Code of Montenegro (similarly to that of other countries) stipulates that the offender who publishes anything from private or family life of a person that can harm their honor and reputation will be punished with a fee of 3,000 – 10,000 euros (Article 197). However, the implementation of this legal provision is far from effective, and women in the region often report victimization from 'revenge porn' or similar attacks in digital spaces.

Evidence from qualitative research

3.3.2 Türkiye

In Türkiye, there has been some progress in revising the Criminal code and Law to Protect Family and Prevent Violence against Women to address at least some forms of TF VAW. The specialized national Action Plan on Combatting Violence against Women (2021-2025) also addresses to a certain extent TF VAW, while the Law to Protect Family and Prevent Violence against Women and national Strategy and Action Plan on Women's Empowerment (2018-2023) do not address directly this TF VAW (Table 1). In addition, a commission established by the Turkish Grand National Assembly on the causes and prevention of VAW considered cyber/digital violence as a separate form of violence in its report in March 2022.[74]

In the Criminal Code, there are several provisions that refer to some forms of TF VAW, but they are not gender sensitive. Some other provisions are indirectly applicable to TF VAW, although they have not been specifically designed to prevent,

73 The new strategy is in the process of being adopted.

74 Report available at: https://mgm.adalet.gov.tr/Home/SayfaDetay/kadina-yonelik-siddetin-sebeplerinin-arastirilarak-alinmasi-gereken-onlemlerin-belirlenmesi-amaciyla-kurulan-meclis-arastirma-komisyonunun-717-sira-sayili-raporu

protect from and sanction TF VAW. For example, the disruption of individuals' peace and order (Article 123) includes calling another person incessantly and thus can be applied to TF VAW, despite not specifically referencing women or defining this behaviour as a form of gender-based harassment. On the other hand, the newly introduced Article 123/A on stalking specifically refers to the use of technology as a means of perpetrating violence. The Article considers perpetration against children and ex-spouses as well as against people who have standing restraining orders for protection purposes as aggravating grounds. While the Law's formulation is not gender-sensitive, some gendered impacts of the act of stalking are reflected in legislation.

Violation of communicational secrecy (Article 132) includes recording communication between persons (Article 133), unlawful disclosure of communication content and broadcasting of data. Again, these provisions are not gender sensitive. The criminal code also addresses violations of privacy, including disclosure of images or sounds of one's private life (Article 134). The definition of threatening includes making threats through social media (Article 106), which is considered in aggravated form if the victim is a woman, and defamation (Article 125), but without gender sensitive references. The code recognizes sexual harassment as a specific crime, including through 'electronic communication tools' (Article 105). Furthermore, recording, breaching or destroying personal data (Articles 135- 138) also covers ICT storage and transfer of data, but again, these provisions are not gender sensitive.[75]

The Law to Protect Family and Prevent Violence against Women mainly defines types of violence, protective and preventive measures, referrals and obligations of various institutions and organizations in the system for protection. Although the Law makes no explicit mention of TF VAW, it includes a specific preventive measure in Art. 5/1-f "not to cause distress to the protected person by means of communication instruments or alternative channels."The implementation regulation of the Law also further clarifies that such "communications instruments" include visual, auditory, written, internet or similar other means, in a way that addresses TF VAW.

The National Action Plan (NAP) on Combating Violence against Women (2021-2025) explicitly recognizes cyber violence (*siber şiddet*) as a form of VAW. The NAP outlines various activities to improve the response to this VAW, including revision of the criminal code and diverse awareness-raising activities. A table overview is in Annex 2.

3.3.3 Eastern European countries

Of the three Eastern European countries included in the research, Georgia's criminal code contains the highest number of provisions directly addressing certain forms of TF VAW. Article 151 of the Georgia Criminal Code defines stalking as *'an illegal monitoring, personally or through a third person, of a person, his/her family member or a close relative, or establishment of an undesirable communication by a telephone, an electronic or other means, or any other international action conducted regularly and causing mental torture to a person….'* There are also provisions related to disclosure of information on private life or of personal data and disclosure of secrets of personal life (Article 157), including through the internet and social networks. The provisions related to violating the secrecy of private communication or correspondence (Articles 158, 159) also include the unauthorized acquisition of computer data or electromagnetic waves, transmission from computer system using technical means or unlawful storage of recordings. However, these provisions are not gender sensitive and not necessarily related to VAW. Chapter XXXV of the Criminal Code is dedicated to cybercrime, but with no specific references to gender-based violence against women.

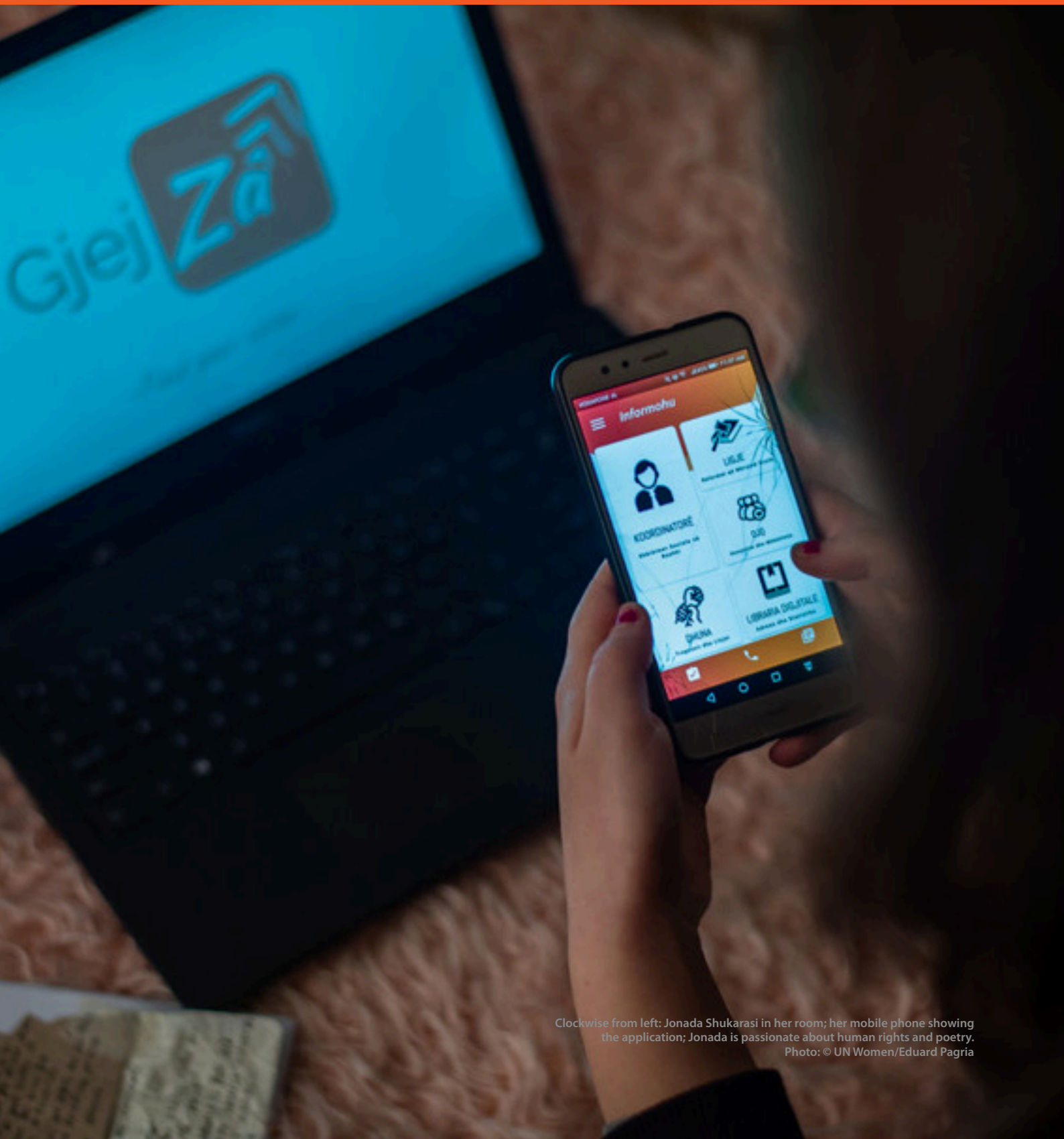
Chapter XI of the criminal code of Moldova addresses computer crimes and crimes in the telecommunications sphere, but the provisions are not related to VAW. The criminal code of Ukraine does not refer directly to any form of TF VAW. There are some provisions related to violations of privacy in communications that might apply to some forms of TF VAW, but they are not formulated to address gender-based violence against women.

3.3.4 Central Asia

The three countries included in the research from the sub-region of Central Asia – Kazakhstan, Kyrgyzstan and Tajikistan – do not have legal provisions in criminal codes or other legislation that would directly address any forms of TF VAW. Additionally, only a few provisions are indirectly applicable, mainly covering forms of TF VAW that are close to doxing and trolling. Kyrgyzstan and Kazakhstan have Laws on State Guarantees of Equal Rights and Equal Opportunities of Men and Women, but these laws do not refer to the issues of prevention and protection of GBV against women, including online and through technology. Kyrgyzstan and Kazakhstan also have specific laws on prevention and protection from domestic violence, but they do not refer to TF VAW. Similarly, Kyrgyzstan's national Gender Equality Strategy addresses the issue of VAW, but not online and through technology.

75 A Guide to fight digital gender-based violence, https://ekitap.alternatifbilisim.org/pdf/cinsiyetci-dijital-siddetle-mucadele-rehberi-en.pdf

4 · WOMEN'S EXPERIENCES WITH TECHNOLOGY-FACILITATED VIOLENCE



Clockwise from left: Jonada Shukarasi in her room; her mobile phone showing the application; Jonada is passionate about human rights and poetry.
Photo: © UN Women/Eduard Pagria

This chapter presents research findings on the prevalence of TF VAW and some of its characteristics, including main forms and manifestations, incidence or frequency, the most common platforms and applications used to induce harm to women and girls, and characteristics of perpetrators. The findings from the web-based survey with women across the region are complemented by qualitative insights from personal experiences of women survivors as well as a presentation of cases reconstructed based on information published in the media.

4.1 PREVALENCE OF TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN

KEY QUESTIONS:

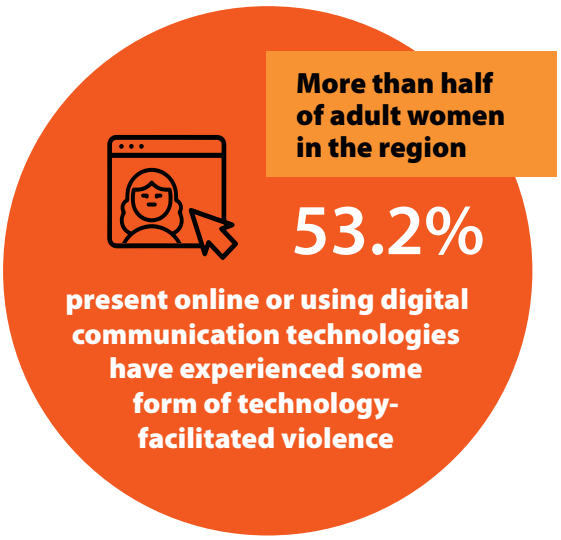
- Among women using ICT in their everyday lives, how many have experienced technology-facilitated violence?
- Are trends common across countries or are there differences between countries and sub-regions?
- How frequent is technology-facilitated violence? Are the harmful incidents isolated cases or is there systematic harassment and abuse?

KEY FINDINGS:

- More than half of women present online in the region have experienced some form of technology-facilitated violence at least once.
- The cross-country differences are significant, with the highest prevalence rate in Ukraine and lowest in Tajikistan.
- By subregion, the highest prevalence is in Türkiye and Eastern Partnership countries, while prevalence is lower in the Western Balkans and lowest in Central Asia.

Survey data tell us that **more than half of adult women in the region (53.2%) present online or using digital communication technologies have experienced some form of technology-facilitated (TF) violence against women at least once in their lifetime**. Forms of TF VAW in the survey included receiving inappropriate sexual advances or sexual content on social networking websites, pressure to share sexually suggestive or explicit images or messages, sharing or threatening to share personal or intimate content without their consent, monitoring their digital communication or location, and other acts (see Methodology section for a complete list). Insights into prevalence disaggregated by age, education and other background characteristics of women are presented in Chapter 4.5 on risk factors.

It is important to keep in mind that the prevalence of TF VAW does not suffice to measure the overall prevalence of VAW in the surveyed countries, as TF VAW is only a portion of the diverse forms and manifestations of VAW. Besides, the prevalence of TF VAW is closely linked to the availability of digital technologies and internet penetration in each country (more on that in the chapter on risk factors of TF VAW) as well as the cultural context which may discourage women from disclosing their experiences through the survey.



Prevalence among the online female population

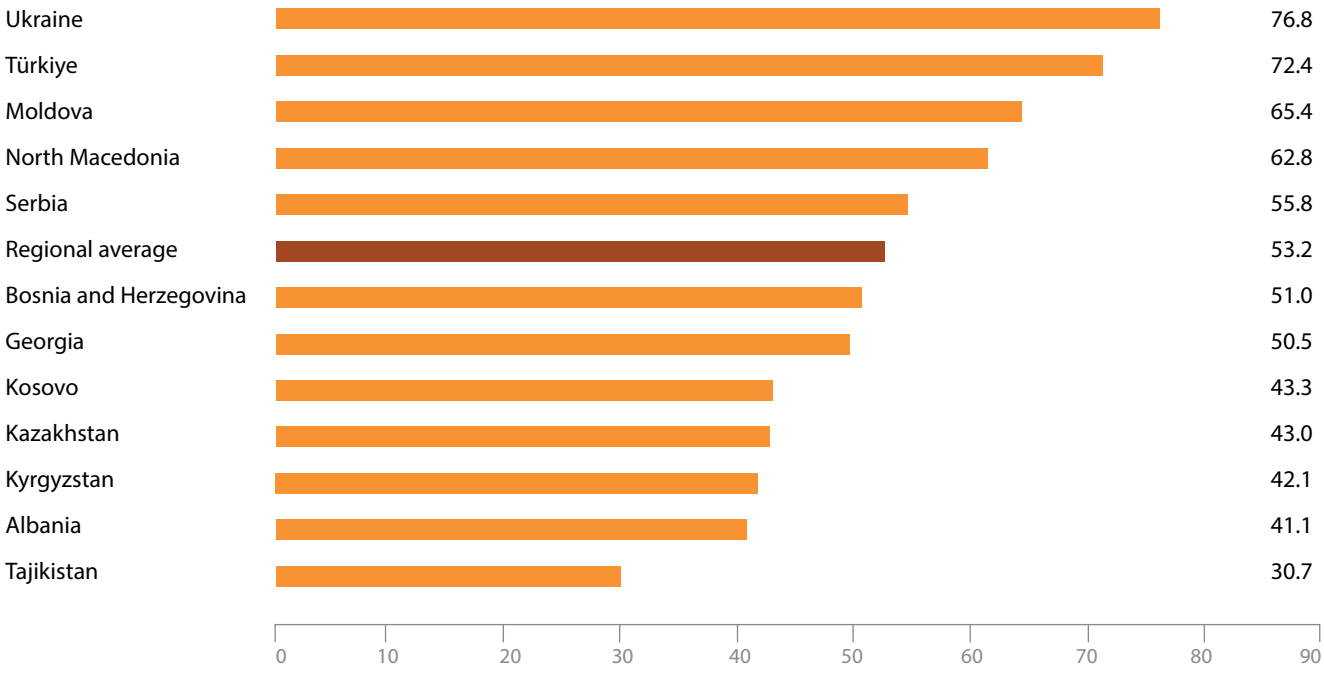
Prevalence measures the proportion of women in a certain population or group who were exposed to violence during a certain timeframe (e.g., lifetime or past 12 months). As the web-based survey was not conducted with a nationally representative sample of women, it does not reflect the prevalence of technology-facilitated violence against women within a country or region.

Instead, the web-based survey provides insight into how many women who are present online have experienced some forms of technology facilitated violence. Therefore, the survey measures the prevalence among women who are using information and communication technologies and are present in online/virtual/cyber space. The sampling methodology used provides a representative picture of women who are present online.

The highest prevalence of TF VAW was found in Ukraine (76.8%) and the lowest in Tajikistan (30.7%) (Figure 1). Countries above the average regional prevalence rate (53.2%) include Türkiye, Moldova, North Macedonia and Serbia, while countries with rates below the regional average, in addition to Tajikistan, include Bosnia and Herzegovina, Georgia, Kosovo, Kazakhstan, Kyrgyzstan, and Albania. Although the survey did not assess the reasons for country-level differences, it is important to bear in mind that reported prevalence is only the 'tip of the iceberg,' as many women are reluctant to share their experience of violence, and reporting personal experiences of violence in a survey is strongly linked to awareness about violence, level of tolerance and attitudes that influence women's perceptions and readiness to share experiences.

Prevalence should be considered in the context of cross-country differences in internet penetration. While low internet penetration rates did not influence prevalence rates since survey respondents were women who participate in online spaces or use digital technologies to communicate, lower internet use in a country might also influence less 'dense' online communication and less 'spill over' of gender-based violence from offline to online space.

Figure 2: Proportion of women who experienced at least one form of technology-facilitated violence, regional average and by country (%) (N=12,526)

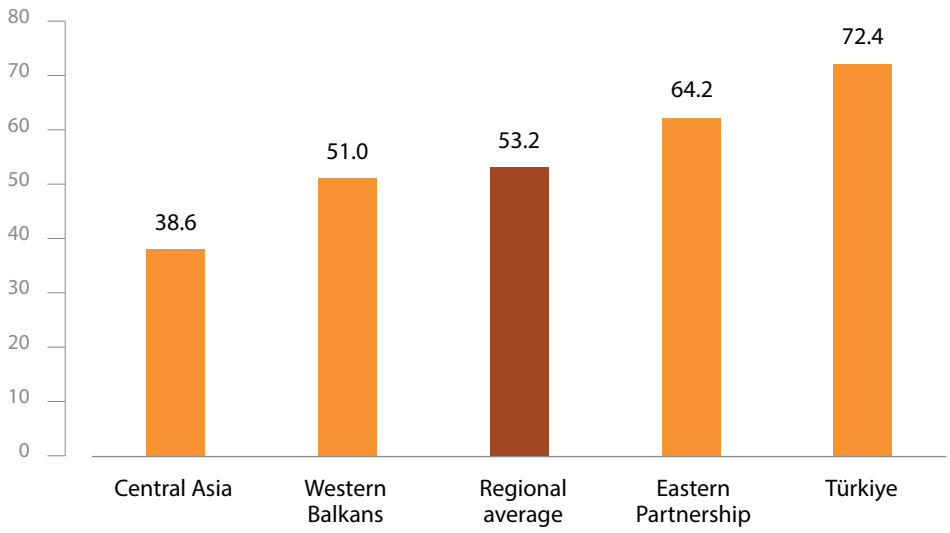


Source: UN Women ECA regional survey 2023

Uliana Pcholkina, a social activist and the head of the "Active Rehabilitation Group" in Kyiv, Ukraine, an NGO dedicated to the rehabilitation of people with spinal cord injuries, was featured in a series of videos titled #нестерпиться #noexcuse launched during the 16 Days of Activism against Gender-Based Violence in Ukraine.

Data also indicate significant sub-regional differences (Figure 2). Sub-regional average prevalence rates are highest in Türkiye and Eastern Partnership countries, lower than average for the Western Balkans region and lowest in Central Asia.

Figure 3: Proportion of women who experienced at least one form of technology-facilitated violence, regional average and by sub-region (%) (N=12,526)



Source: UN Women ECA regional survey 2023

4.2 FORMS AND FREQUENCY OF TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN

KEY QUESTIONS:

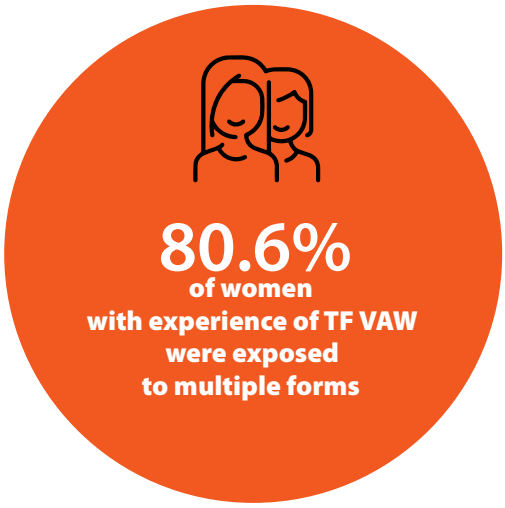
- Which forms of technology-facilitated violence against women are the most prevalent?
- Are women exposed to multiple forms of TF violence?
- How frequently do women experience TF violence?
- Are there cross-country or subregional differences that might indicate specific patterns of online and TF violence against women?

KEY FINDINGS:

- The most prevalent forms of online and TF violence include receiving unwanted or offensive content or messages, receiving inappropriate sexual advances or content on social networking and hacking women's accounts and web pages.
- The highest proportion of women experienced one single form of online and TF violence, but one woman in four experienced multiple forms (three or more).
- A large proportion of women experienced TF violence once (40.4%), while one in seven women experiences such violence daily or weekly.
- There are remarkable differences between countries and subregions, with women in Türkiye being exposed in the highest proportion to repeated experiences of violence compared to women in other countries.

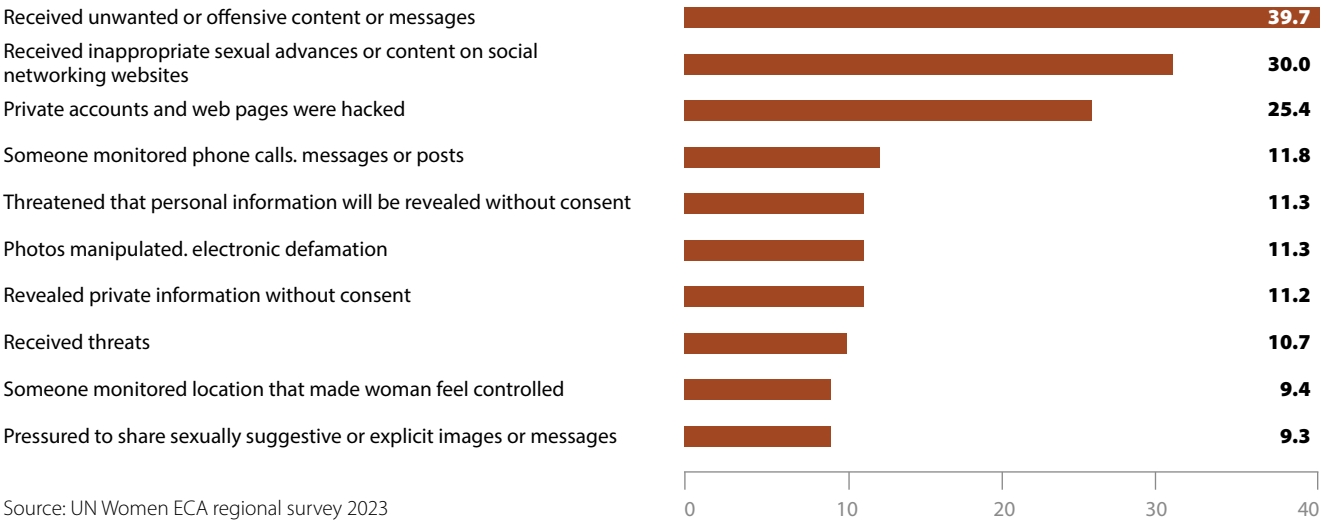
4.2.1 Forms of technology-facilitated violence against women

Analysis within this chapter covers women who experienced technology-facilitated violence at least once (N=6662, or 53.2% of the total sample). The most prevalent form of tech nolo-gy-facilitated violence against women is manifested as unwanted or offensive content or messages, which were received by almost 40% of women, followed by inappropriate sexual advances or sexual content on social networking websites, which were experienced by almost every third woman (Figure 3). Every fourth woman has had their internet accounts or web pages hacked. One woman in eight had her phone calls, messages or posts monitored by a perpetrator in order to see with whom she was communicating. In the same proportion, women experienced abuse by manipulation of their photos, electronic defamation, threats to reveal their private information without their consent, having their private information published without their consent, or threats of violence to themselves or their family. One woman in ten had her location monitored for the purpose of control and one in ten was pressured to share sexually suggestive or explicit images or messages (Figure 3).



Despite diversity within these forms of violence, their motivation and aim are the same – to harm women by controlling, frightening, or humiliating them, thus reproducing unbalanced gender power relations.

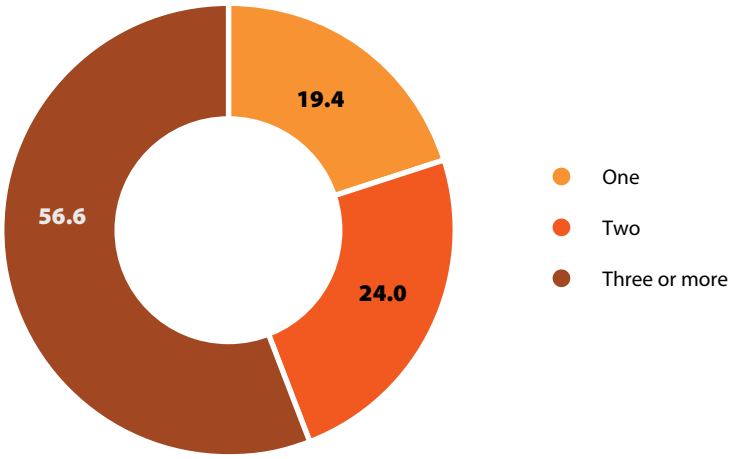
Figure 4: Women with experience of at least one form of technology-facilitated violence by form of violence they experienced, multiple choices (%) (N=6662)



Source: UN Women ECA regional survey 2023

Another question is related to the multiplicity of forms of violence experienced by individual women. Survey data show that more than half of women have experienced one single form of TF VAW, while every fourth woman has experienced two forms and every fifth has experienced three or more forms of TF VAW (Figure 4).

Figure 5: Women who experienced at least one form of technology-facilitated violence, by number of different forms of violent acts they experienced (%) (N= 6662)



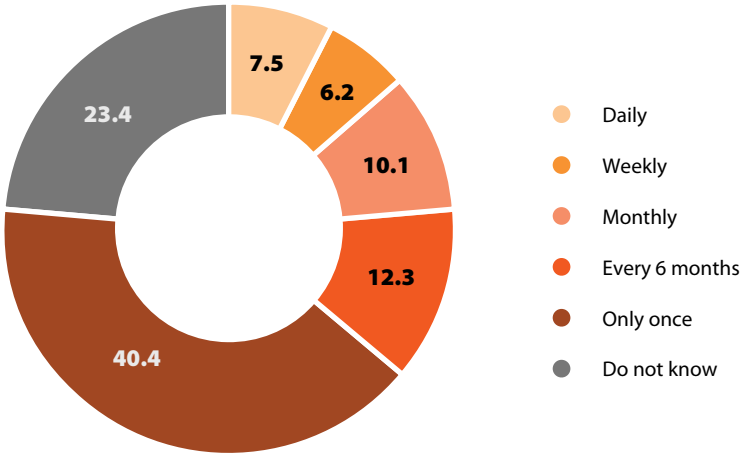
Source: UN Women ECA regional survey 2023

Women are generally aware of the possibilities new technologies provide in controlling their lives. In the overall sample of women, 44.1% think that their partner or family members can control their activities or location through mobile technologies. Within that proportion, not all women had already experienced some form of TF VAW. In fact, 46.7% of these women have not experienced TF VAW, but regardless, they are concerned that might be controlled via mobile phones by their partners or family.

4.2.2 Frequency of technology-facilitated violence against women

If the frequency of violent acts women experience facilitated by digital technologies is taken as a proxy for measuring the intensity of violence, we can conclude that one in seven women (13.7%) is exposed to a high intensity of violence, defined by facing violent acts daily or weekly. A major proportion of women with experience of TF VAW (40.4%) has experienced an act of TF violence once, while 23.4% were not able to assess the frequency of TF violence to which they were exposed (Figure 5).

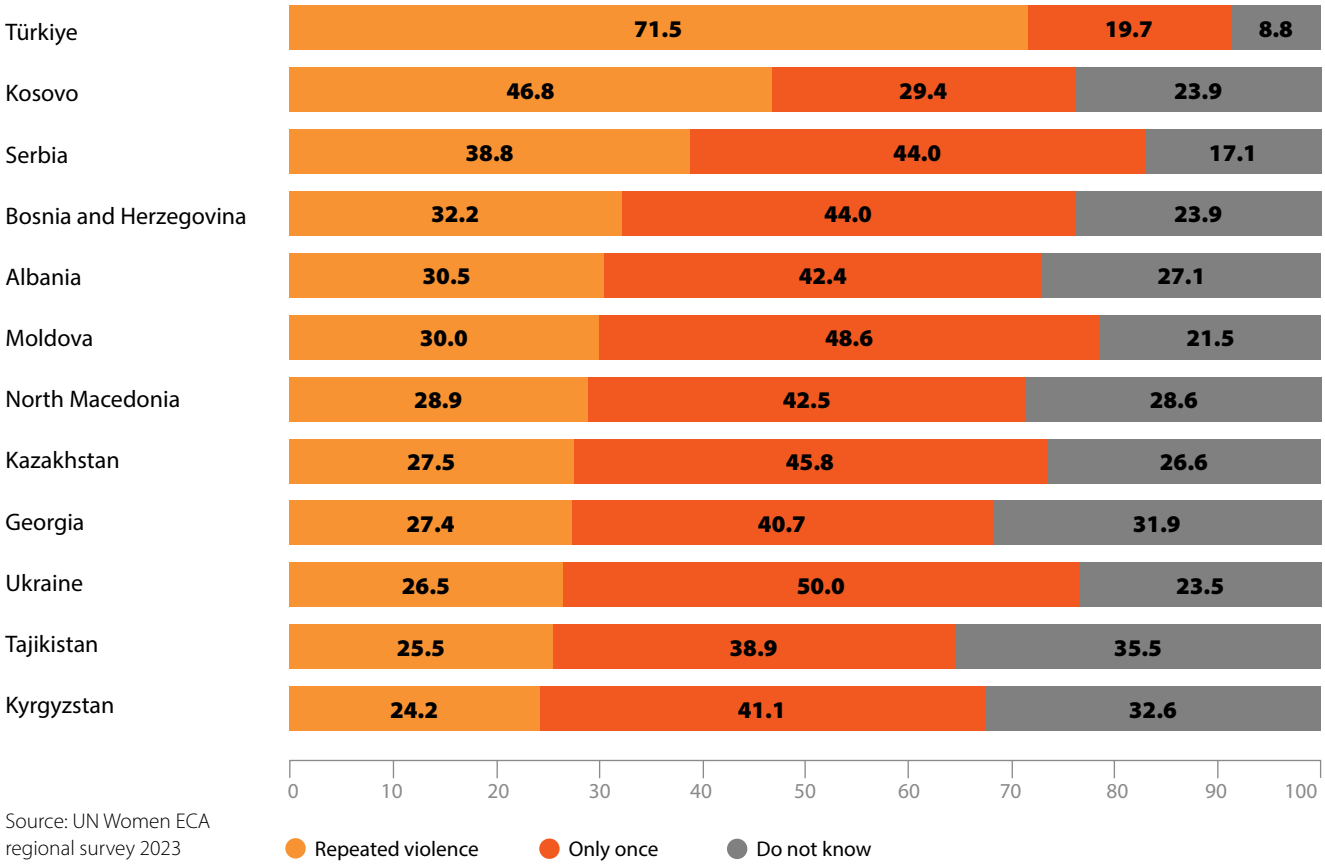
Figure 6: Women who experienced at least one form of technology facilitated VAW, by frequency of violent acts (%) (N= 6662)



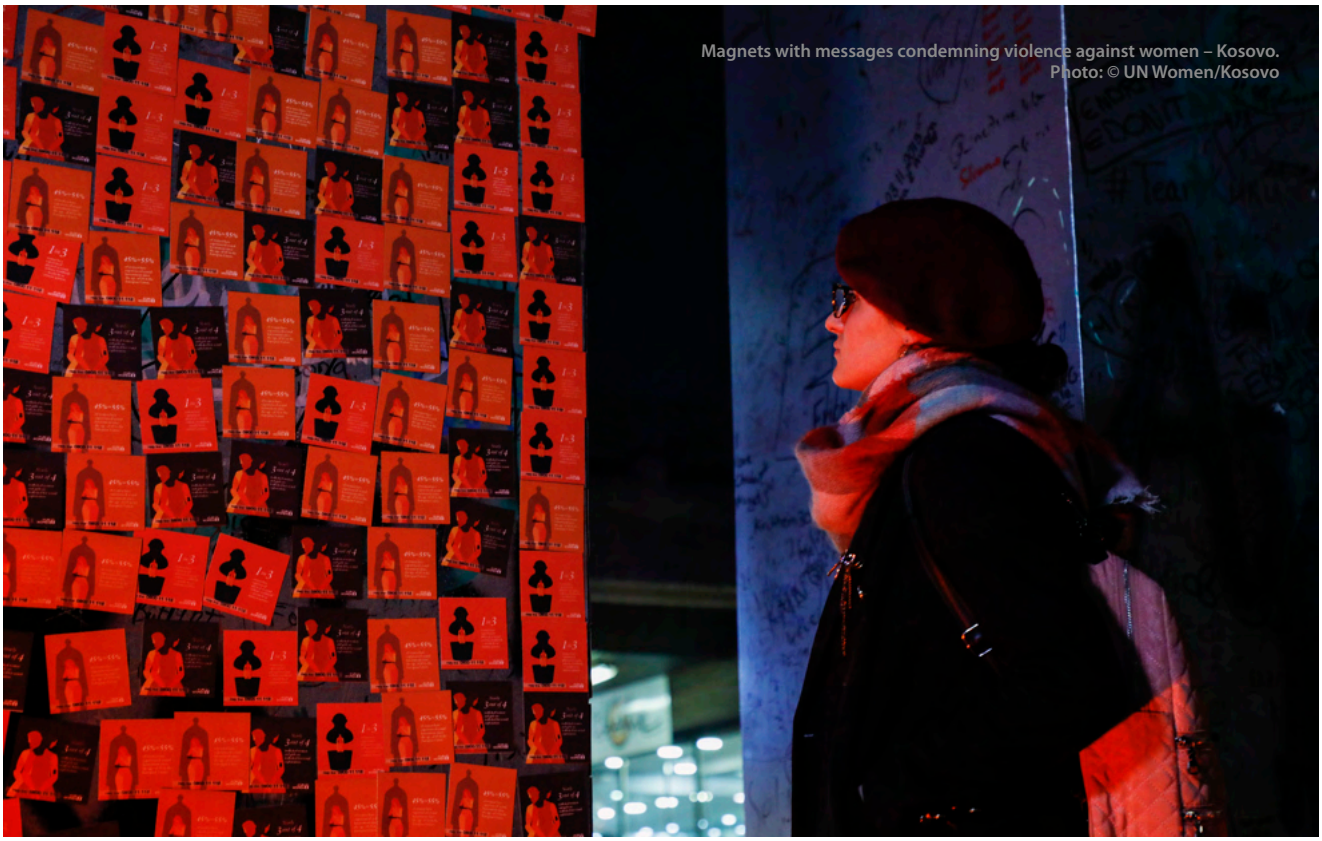
Source: UN Women ECA regional survey 2023

Differences in frequency of violence appear significant between countries and sub-regions. Türkiye has the highest share of women who reported repeated violence (daily, weekly, monthly or every six months), while Kyrgyzstan has the lowest prevalence of repeated violence (Figure 6). Cross-country data on frequency of violence provide a somewhat different picture than data on prevalence. Some countries with very high prevalence rates of TF VAW have relatively low intensity (for example Ukraine), while some countries have lower prevalence rates but higher intensity (for example when compared, Kosovo has a lower prevalence rate but higher intensity than Georgia). Some countries, such as Türkiye have high prevalence with high intensity of violence, indicating a particularly concerning situation regarding the safety and wellbeing of women online.

Figure 7: Women who experienced at least one form of technology-facilitated violence, by frequency of violent acts and country (%) (N= 6662)



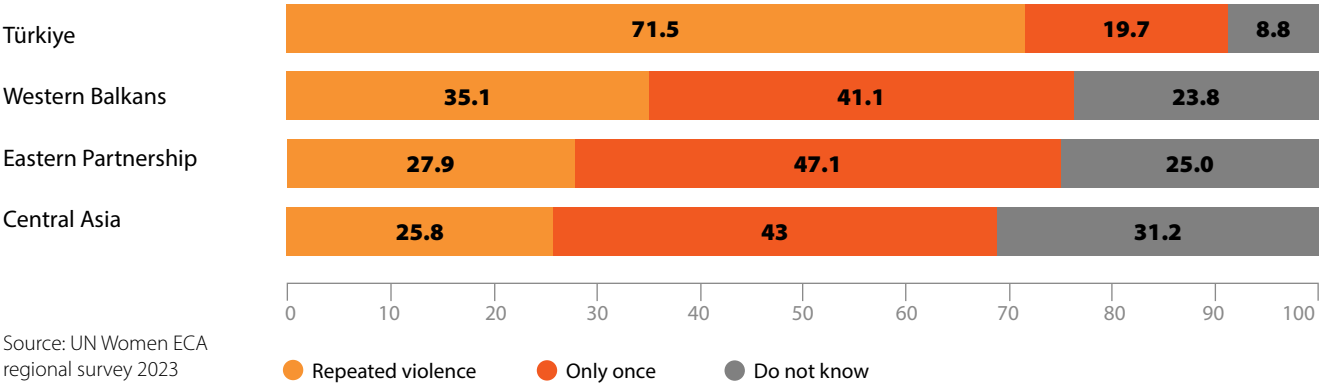
Source: UN Women ECA regional survey 2023



Magnets with messages condemning violence against women – Kosovo.
Photo: © UN Women/Kosovo

By sub-region, following Türkiye, the Western Balkans has a higher prevalence of repeated violence, where more than one in three women have been repeatedly exposed to violence by single or multiple perpetrators (Figure 7).

Figure 8: Women who experienced at least one form of technology-facilitated violence, by frequency (incidence) of violent acts and country (%) (N= 6662)



Source: UN Women ECA regional survey 2023

The frequency of technology-facilitated violence women experience varies by identity of the perpetrator. When perpetrators are unknown persons or persons women met on internet, it is most common that the violent act occurred once (in 47% of cases when the perpetrator is unknown, and 42% of cases when the perpetrator is known only on the internet). When perpetrators are persons from women's 'offline' social networks, in the majority of cases (51.2%), the violent acts are repeated. The highest proportion of repeated acts of violence is recorded among women who were violated by bosses or supervisors (66.4%, but caution is needed due to the relatively small number of cases – see the chapter on perpetrators), followed by women who identified family members as perpetrators (58.0%), then women who identified current or former partners (49.3%) and friends and acquaintances (48.7%). Differences were also found by partners' civil status – the highest proportion of repeated violence was reported by women who identified husbands as perpetrators (51.1%), followed by those who identified boyfriends, girlfriends or fiancés (50.5%), and then those who identified former partners (47.4%) (Table 6, Annex 2).

4.3 THE 'VIRTUAL' PLACES OF VIOLENCE

KEY QUESTIONS:

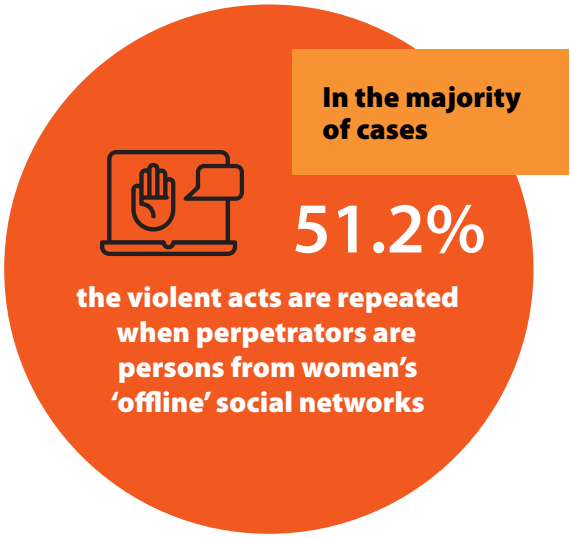
- Which places on the internet are particular 'places of fear,' where women are more likely to be exposed to violence and which often provoke harm, fear, or discomfort?
- Which other digital tools such as mobile phone apps are mainly used by perpetrators?

KEY FINDINGS:

- Facebook and Instagram are the platforms most reported by women as places where they experienced violence, as every third woman who experienced technology-facilitated (TF) violence had that experience on one of these two platforms.
- One in ten women experienced TF VAW on TikTok, e-mail or messaging applications such as Skype, Snapchat, messenger, Viber or similar.
- The platforms on which women experienced TF violence differed by country and region, with Western Balkan women having more violent experiences on Facebook than women in other countries, women from Albania and Türkiye pointing more to Instagram, and women from Central Asia pointing more than other women to WhatsApp and Telegram.

Certain **spaces can become places of fear**[76] due to the increased risks and frequency of violence against women.[77] For instance, there is a common perception that women should be afraid of violence when walking home alone at night. The internet and social media introduced new places of fear where women are exposed to higher risks of violence both publicly (e.g., via public forums and platforms) and privately (e.g., via email and private messages). Each internet platform is a specific place where women can communicate privately with other individuals, participate in exchanges with broader audiences, or join certain communities formed of static groups of individuals who meet on regular basis to have exchanges and share content, values, and opinions. The question becomes – what are these 'virtual' places in which women are more often exposed to violence? In addition to that, the question is which mobile applications are more often used by perpetrators who are close to or known by women in offline spaces.

The highest proportion of women who experienced TF violence identified Facebook and Instagram as platforms on which their experience of violence occurred (Figure 8). More than one in three women linked their experience of violence to one of these two platforms. Other platforms are far less reported: every tenth woman with experience of TF violence identified TikTok, e-mail, or messaging applications such as Skype, Snapchat, messenger, Viber, WhatsApp or similar.

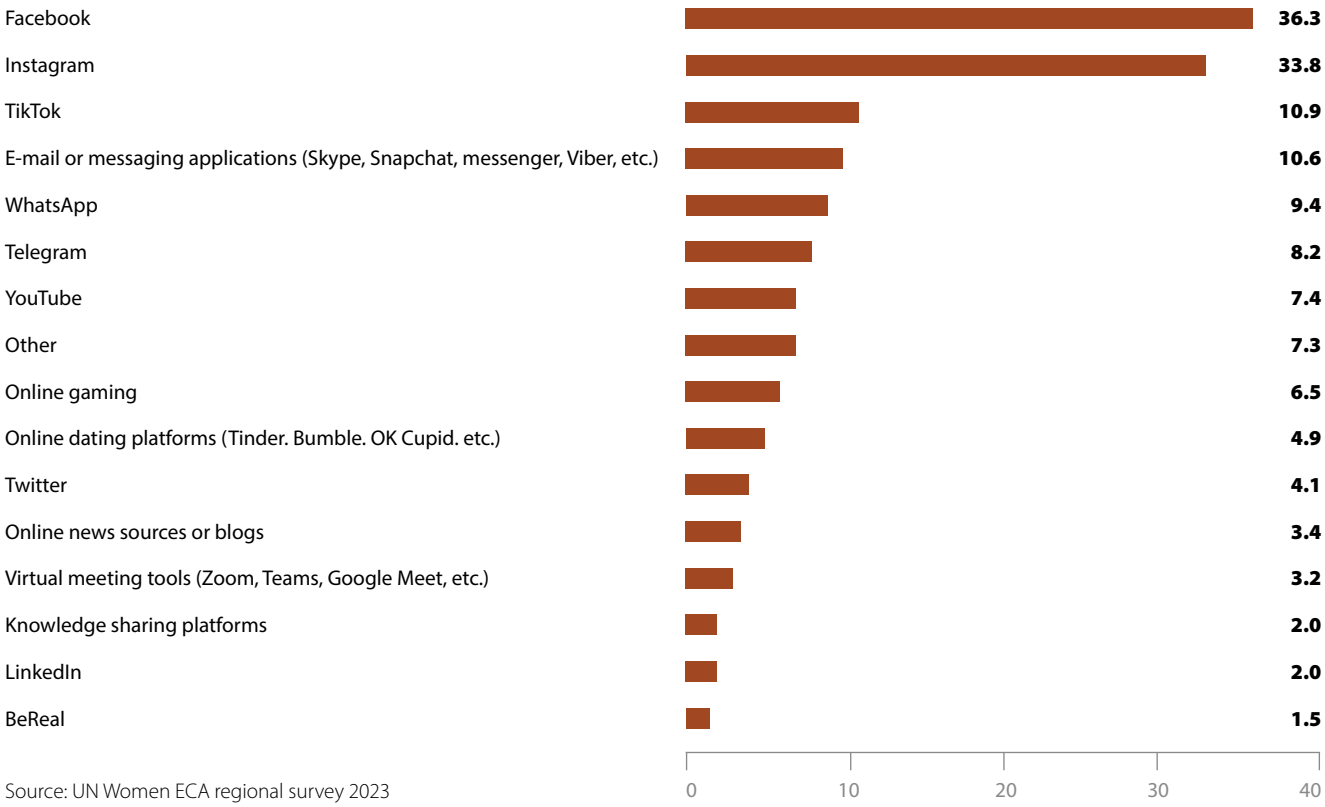


76 Renowned geographer Doreen Massey made distinction between 'space' as more 'objective' location, and 'place' as more complex, subjective as it includes socially experienced and formed environment, interactions between individuals, emotional connections and lived experiences. See more in Massey, D. (1994) *Space, place, and gender*. Minneapolis: University of Minnesota Press.

77 Sandberg, L (2011). Fear of violence and gendered power relations. Responses to threats in public space in Sweden. Umea: Gerum.

Orange the World 2019 – Bosnia and Herzegovina. Photo: © UN Women/Elmina Karic

Figure 9: Women who experienced at least one form of technology-facilitated violence by platform on which that violence was experienced (in case of multiple experiences, the most recent) (%) (N= 6651)



Source: UN Women ECA regional survey 2023

There are certain cross-country differences in this regard.[78] For example, women from Western Balkan countries and Georgia were comparatively more likely to identify Facebook as virtual place where they were exposed to violence (62.3% of women with experience of TF VAW in BiH, 51.0% in Georgia, 68.6% in North Macedonia, 55.8% in Serbia; compared to 24.1% in Türkiye, 11.1% in Kyrgyzstan, 7.6% in Kazakhstan, 12.3% in Tajikistan). Instagram is most often the place where women from Türkiye and Albania have experienced TF VAW, while Telegram and WhatsApp are more often identified by women in Kyrgyzstan and Kazakhstan compared to other countries (with exception of Ukraine in the case of Telegram) (Table 5 in Annex 2).

However, the question remains – are certain platforms more prevalent places of violence against women just because women use those platforms more than others, or there are certain platform-related features that increase the risk of TF violence against women? This question is addressed in the chapter on risks of TF violence.

Statistical analysis shows that some 'digital places' bear higher risks of VAW than others (see Annex 2, binary logistic regression model 2). **The highest risks are present in gaming communities** and when women most often use **chatting and messaging on Snapchat, Facebook and Instagram** (more about this topic in the chapter dedicated to risks).

Bosnia and Herzegovina: Livestreaming femicide

The entire Western Balkan region was shaken in August 2023 when a man livestreamed femicide on social media. The perpetrator livestreamed the torture and murder of his wife on Instagram; the video and the perpetrator's account were removed three hours after the video was posted. During these three hours he killed three persons (including his wife), wounded another three persons and then committed suicide. Radio Free Europe reported that in one hour, the number of likes on his livestream increased from 125 to 329. At one point in time, 15,000 people were watching the livestream. The femicide video went viral on other networks.

The hours-long uptime of the video revealed substantial weaknesses in Instagram's mechanisms of reporting and removing harmful content, including filters designed to automatically flag and remove violent content. The source reports that the BiH cybercrime department of the Federal Police requested removal of the video to Instagram's parent company immediately upon receiving reports of the video, but the company took two hours to remove the video.

The incident was followed by massive protests across BiH and was echoed by solidarity protests in other countries in the Western Balkans. Citizens raised the issue of how the femicide coupled with multiple murders could have happened since the perpetrator was known to police for his aggressive incidents and had previously been reported for domestic violence. The case revealed the gaps in the system for protection. Livestreaming the incident was an act of violence not only against murdered woman, but against all women who have seen or heard about this. It was intended to encourage men to use violence to discipline or punish women and to spread fear among women and send the message that they should be obedient. Another tragic aspect of the case were the comments posted on Instagram supporting the perpetrator.

78 It should be taken into account that the internet/social media penetration rate is very different between subregions. While in the Türkiye penetration of social media is 80.5%, in Eastern Europe 70.5%, in Central Asia is only 27.4%. For details see https://www.demandsage.com/social-media-users/.

79 Radio Free Europe https://www.slobodnaevropa.org/a/gradacac-ubistvo-instagram-bosna-hercegovina/32544490.html

4.4 PERPETRATORS

KEY QUESTIONS:

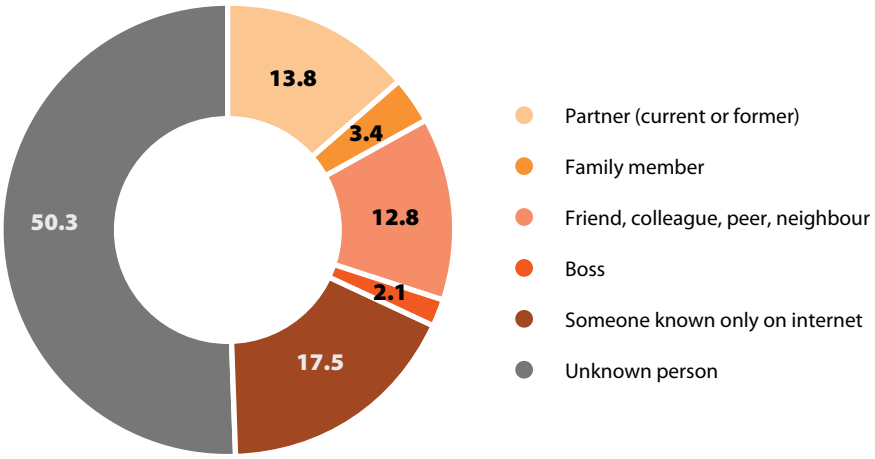
- Who are the perpetrators of technology-facilitated violence against women, in terms of their relationship to women?
- Are there noticeable differences in types of violence committed against women based on survivor-perpetrator relationship?
- Are there certain 'inclinations' of different perpetrators to use some communication channels over others?

KEY FINDINGS:

- The majority of technology-facilitated violence is perpetrated by unknown persons (50.3%) or persons known only on the internet (17.5%). However, almost one third (32.1%) of technology facilitated violence is perpetrated by persons in women's social proximity, such as partners, family members, friends, acquaintances, colleagues, bosses or co-students, and therefore may represent an extension of offline violence.
- Unknown perpetrators and those only known to women on the internet are more inclined to commit violence in the forms of hacking women's accounts and sharing offensive or other unwanted content or messages. Partners are more likely to use threats or controlling acts, while family members combine controlling acts with sexual harassment, and bosses are more linked to acts in the forms of sexual harassment.
- Although all forms of violence regardless of perpetrator occur mainly on Facebook and Instagram, there are certain differences between perpetrators related to types of platforms they use in acts of violence: partners more often use Twitter, WhatsApp, and meeting tools; friends and acquaintances more often use Telegram, TikTok, and online gaming platforms; while persons only known to women online more often use Facebook, Instagram and dating platforms.

A major portion of technology-facilitated (TF) VAW is perpetrated by persons who are either unknown to women (50.3%) or persons that women know only from the internet (17.5%) (Figure 9). One in seven women (13.8%) identified a current or former partner as a perpetrator, and one in eight (12.8%) identified a friend, colleague, co-student or neighbour. To a lesser extent, women pointed to family members or bosses (3.4% and 2.1% respectively). However, these findings should be taken with reservation, as unknown or unidentified persons may in some cases be persons known to women in the 'offline' world who have concealed their online identity through fake accounts, hidden phone numbers or other methods.

Figure 10: Perpetrators of technology-facilitated violence against women (in case of multiple experiences, the most recent) (%) (N= 6657)



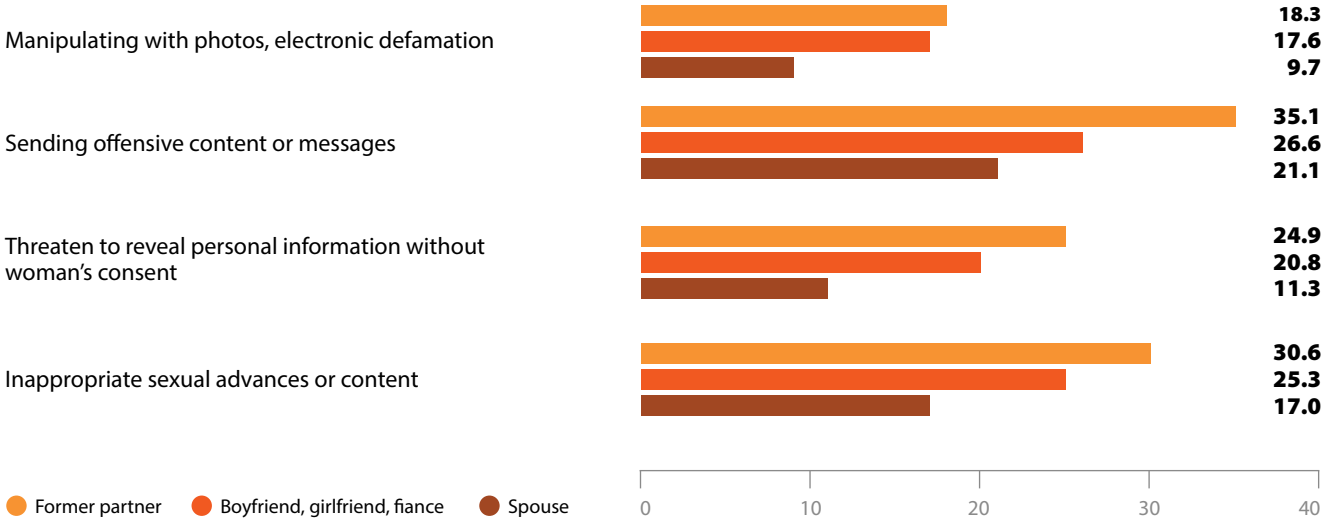
Source: UN Women ECA regional survey 2023

There are certain differences in types of TF VAW committed based on the survivor-perpetrator relationship:

- Unknown perpetrators in highest proportion compared to other perpetrators hack women's accounts (31.8% of cases committed by unknown perpetrator), but this type of violence is also present in a high proportion among partners (24.4% of all cases perpetrated by partners) and persons known to women only on the internet (22.6% of all cases committed by these persons);
- Persons only known to women on the internet in higher proportion than other perpetrators send unwanted or offensive content or messages (53.2%), although this form of violence is also present in high proportion among unknown perpetrators (47.1%);
- Partners (current or former) in higher proportion than any other perpetrator threaten to reveal women's personal information without consent (20.9%), threaten women in other ways (15.3%), and in almost the same proportion as family members, monitor women's phone calls and other digital communication (23.8%);
- Family members in higher proportion than any other perpetrator monitor women's phone calls (24.2%) and conduct acts related to photo manipulation and electronic defamation (22.3%);
- Supervisors or bosses in higher proportion than other perpetrators pressure women to share sexually implicit images or messages (17.2%), reveal private information without woman's consent (22.4%), and monitor women's location (20.1%), though the total number of bosses identified as perpetrators is relatively small (140 cases) and this finding should be taken with caution (Table 6, Annex 2).

In addition, there are significant differences between current and former, married and non-married partners in the type of TF violence they commit. When it comes to sending offensive content or messages, inappropriate sexual advances or content, threatening to release private content (often for blackmail or revenge), manipulating photos, and electronic defamation (Figure 10), former partners commit these offenses in higher proportion than current partners, and current non-married partners commit them in higher proportion than spouses.

Figure 11: Types of technology facilitated violence against women perpetrated by different partners (%) (N=918)



Source: UN Women ECA regional survey 2023

Although all forms of violence, regardless of perpetrator, occur mainly on Facebook and Instagram, there are certain differences between perpetrators related to types of platforms they use in acts of violence. As previously noted, unknown perpetrators are the most frequent perpetrators in general, so they are also the most prevalent perpetrators in every type of platform, excluding LinkedIn and educational platforms (Table 5, Annex 2). In addition to Facebook and Instagram, which are the most used platforms for all perpetrators, there are certain differences in the use of other platforms.

Compared to other perpetrators:

- Current and former partners more often use TikTok, WhatsApp and messaging applications;
- Family members more often use TikTok, YouTube and WhatsApp;
- Friends and acquaintances more often use WhatsApp, Telegram and YouTube;
- Supervisors or bosses more often use YouTube, TikTok and WhatsApp.

4.5 RISK FACTORS

In order to understand which factors increase the risk of being exposed to technology-facilitated (TF) violence, two sets of factors were examined: one related to various socio-demographic characteristics of women (such as age, education level, living area, civil status, sexual orientation, employment status) and one related to the activities on the internet or in other digital communication (such as time spent online, use of specific platforms and applications, possession of public accounts, number of friends or followers, etc.). For this purpose, binary logistic regression was conducted with a dependent dichotomous variable in which women were divided in two groups: those with any experience of TF violence (N=6662) (tested category) and those without (N=5864) (reference category). Regression models and results are presented in Annex 2.

4.5.1 Socio-demographic characteristics of women

KEY QUESTIONS:

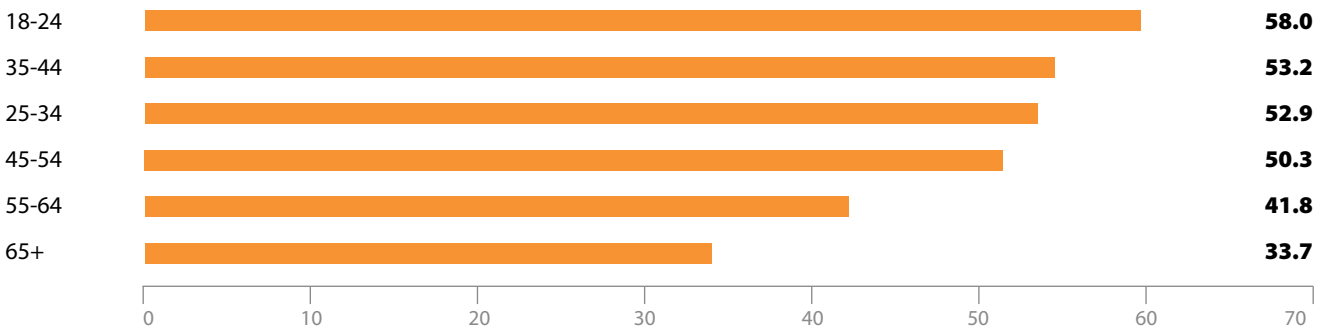
- What factors increase the risk of being exposed to TF VAW?
- Are socio-demographic characteristics related to risk of exposure to TF VAW?

KEY FINDINGS:

- The risks of TF VAW are not evenly distributed among women with different socio-demographic backgrounds.
- Younger women are at higher risk of TF VAW than older women.
- Women with more than primary education are at higher risk compared to women with only primary school education, and women with secondary technical training are at highest risk of being exposed to TF VAW.
- LGBTQI women, women from bigger cities and divorced women also face higher risk of TF VAW.
- Employment status has no influence on the risk of TF VAW.

Statistical analysis showed that among tested risk factors (age, education level, employment, civil status, sexual orientation and area of living) the strongest predictor of experiencing TF VAW is age. Young women (18-24) are at a much higher risk of TF VAW than women in the oldest age group (65+) (which was used for the reference category). Regression analysis indicates that the probability of experiencing TF VAW is 4 times higher for the youngest women than for those over 65 (see Annex 2, regression model 1).[80] Cross-tabulation data also clearly indicate that the prevalence of TF VAW decreases with age (Figure 11).

Figure 12: Percentage of women with experience of technology-facilitated VAW within each age group (N = 12526)



Source: UN Women ECA regional survey 2023

80 In the statistical logistic regression model, the difference is observed between all age categories compared to the oldest respondents of age 65+ (reference category). The odds ratio for women up to 24 years was 4,1 (Exp(B)=4,115).

4x **Women aged 18-24 are 4 times more likely to experience TF VAW than women aged 65+**

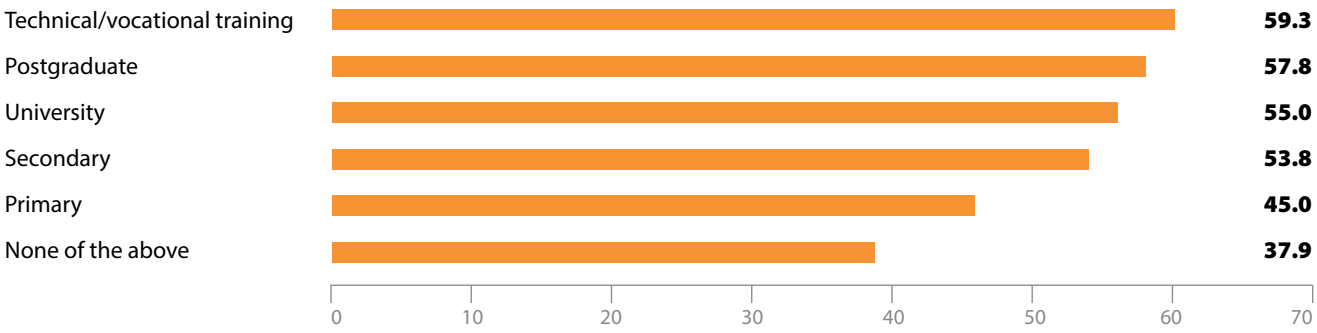
The identification of age as a significant risk factor may not be surprising, as younger women on average spend more time on the internet and social media.

Among women aged 18-24, almost half (49.4%) spend at least three hours daily on social media, online messaging, browsing and online gaming. This proportion decreases to 40.6% among women aged 25-34, 36.2% among women aged 35-44, 38.6% among women aged 45-54, 36.1% among women aged 55-64 and 24.3% among women aged 65 years or older.

That said, younger women were also found to have higher exposure to offline gender-based violence in the OSCE-led Survey on the Well-being and Safety of Women. Among young women aged 18-29, 40% experienced sexual harassment, stalking, psychological, physical or sexual violence in the 12 months preceding the survey, compared to 24% of women aged 60 years or older.[81]

Furthermore, data show that education has a significant impact on women's exposure to TF VAW. Women who completed secondary or tertiary education are more likely to experience TF VAW compared to women who completed only primary school (see regression model 1, Annex 2). This is also evidenced by cross-tabulation data presented in Figure 12.

Figure 13: Percentage of women with experience of technology-facilitated violence within each education level category, (%) (N = 12526)



Source: UN Women ECA regional survey 2023

The locality (the size of the town) also statistically significantly affects the chances of being exposed to TF VAW. Women living in cities with number of inhabitants between 30,000 and 100,000 are at greater risk of TF VAW (59.8% have reported experience of at least one form of technology facilitated violence), followed by women living in cities with 100,000-500,000 inhabitants (56.2%) and big cities with more than 500,000 inhabitants (55.4%). The lowest prevalence rates are found among women living in places with less than 30,000 inhabitants (47.6%) (see also regression model 1 in Annex 2).

59.8% **women living in cities with number of inhabitants between 30,000 and 100,000 have reported experience of at least one form of technology facilitated violence**

There is a statistically significant relationship between women who reported having experienced TF violence and sexual orientation. Bisexual and pansexual women are more exposed to TF VAW than heterosexual women (74.8% and 72.4% vs. 63.6% respectively), while lesbian and gay women are at lower risk (59.1% and 55.4% respectively) (see also regression model 1, Annex 2). There is also a relationship between civil status and TF VAW, showing that divorced women are more affected by TF VAW than unmarried and married women (59.3% vs. 55.7% and 50.8% respectively). Finally, there is no statistically significant correlation between TF VAW and current employment status.

81 OSCE, Wellbeing and Safety of Women. Main report. p. 121

4.5.2 Risk factors related to digital communication

KEY QUESTIONS:

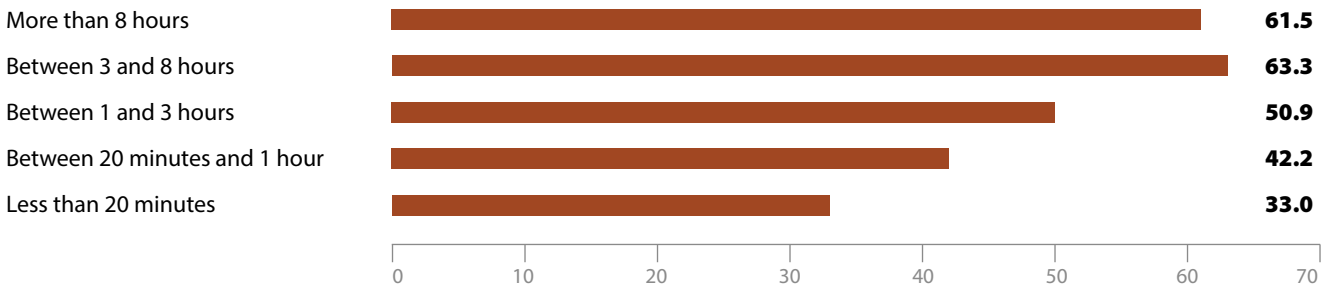
- Are there factors related to online activities and practices, such as time spent on the internet, possession of public accounts, number of connections established online, type of platform used, that increase risks of technology-facilitated (TF) violence against women?

KEY FINDINGS:

- Time spent on the internet is the strongest predictor of TF VAW – women who spend more time on the internet are at higher risk of being exposed to violence.
- The highest risks are found among women participating in online gaming, followed by women who most often use social media messaging, such as Snapchat, Viber, Facebook or Instagram, and then women who use Telegram.
- Possession of a public profile on internet platforms, particularly more than one, and a larger number of friends and followers increase also the risk of violence.

Statistical analysis shows that various characteristics of online activities and communication influence the probability of experiencing technology-facilitated (TF) VAW, including time spent on the internet,[82] type of platform or application used for communication, possession of a public profile, and number of friends or followers. The only factor that appeared insignificant is the type of device used to go online. The majority of women (78.7%) use mobile phones to communicate, while some women use a shared mobile (5.7%), shared computer (2.3%) or public computer (2.1%). However, this appears to have no influence on the risk of TF VAW. Among other tested factors, the strongest predictor is time spent on the internet. Women who spend 1-3 hours on the internet daily are at 1.5 times higher risk to become victims of TF VAW. Women who spend more than 3 hours on the internet daily are at 2 times higher risk compared to women who spend less than 20 minutes (regression model 2, Annex 3). See Figure 13.

Figure 14: Percentage of women with experience of technology facilitated VAW within each category of daily internet usage duration (%) (N = 12526)



Source: UN Women ECA regional survey 2023

Women who participate in online gaming have the highest risk of experiencing TF VAW, followed by women who most frequently use social media messaging such as Snapchat, Viber, Facebook and Instagram chats and women who most often use Telegram (regression model 2, Annex 2).

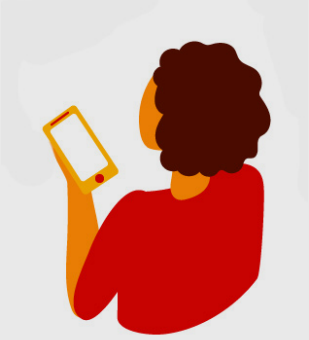
Higher risks of TF VAW are also linked to the possession of public profiles and the number of such profiles. Women with public profile are under three times higher risk of TF VAW than women without public profile. Women with more than one public profile are under higher risks than women with only one public profile (regression model 2, Annex 2).

82 Time spent on internet was measured as a categorical rather than continuous variable. The question was 'How much time do you spend on social media, online messaging, browsing and online gaming' and the categories were: less than 20 minutes, 20 minutes to 1 hour, 1 hour to 3 hours, 3 hours to 8 hours, more than 8 hours.

HeForShe Summit 2023. Photo: © UN Women/Ryan Brown

The number of friends or followers also increases the risk of violence. Women with more than 100 friends or followers are exposed to a higher risk of violence than women with less than 100 followers (regression model 2, Annex 2).

Lina's testimony* (age 16): Doxing and cyberbullying



We young people mostly use Instagram and TikTok. Instagram is for posting photos, seeing other people's photos and chatting with others, while TikTok is for watching videos when you are bored. For me, Instagram is the worst platform because anyone can find you and see your photos. I had a private Instagram account since the age of 13 [the minimum age to open an account on most platforms]. Everyone had an Instagram account, so I thought I should have it as well. All was fine until I started to receive some unwanted photos and requests to send photos. I was threatened that I would be raped and killed if I didn't send photos. It was so traumatic. Maybe they were joking, but it was very traumatic for me. I didn't know with whom to talk, so I approached a psychologist for help, and I deleted my Instagram account. This lasted for two years, and nobody did anything to stop it. After two years, one girl after another reported the same violence, and when 10 girls revealed the same experience, they finally found the perpetrator. He was a peer from school with problematic behaviour. None of the girls had told anyone out of fear.

Another harmful experience was with another boy. He asked me to send him some photos and promised that he would not show them to anyone. But this was a lie. He sent photos that I would not want to show to anyone to half the school. I am so embarrassed now that I will change schools.

I was lucky to have good parents. They showed understanding and did not blame me. Nowadays I use the internet only to browse – I don't have any social media account. Peers look at me with surprise, like 'how it is possible that she does not have an Instagram account.'

Later I joined an organization that works on raising awareness about gender-based violence.

Evidence from the qualitative research
*Not her real name

4.6 CONSEQUENCES OF TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN

4.6.1 Consequences for women's psychological wellbeing and social relations

KEY QUESTIONS:

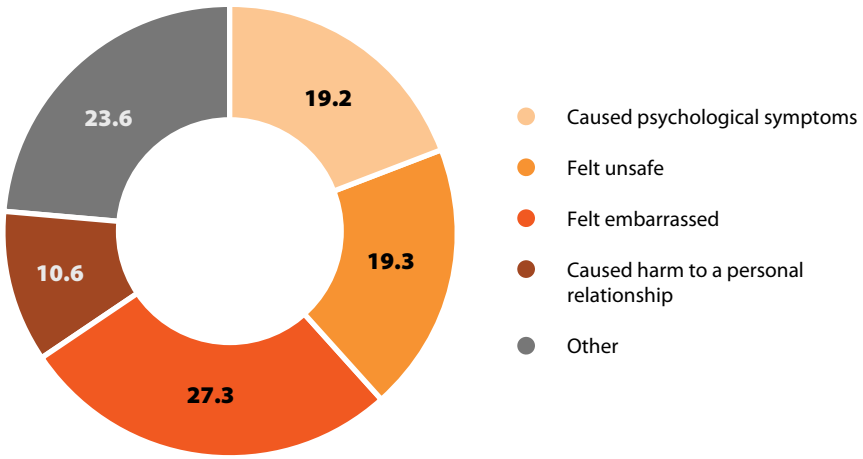
- How does technology-facilitated (TF) violence affect women's psychological wellbeing and their social relations?
- Are consequences stronger or more prevalent in the case of repeated violence compared to one-off incidents?
- Are consequences different based on survivor-perpetrator relationship?

KEY FINDINGS:

- TF VAW has noticeable consequences for women's psychological wellbeing, as two thirds of women with some experience of TF VAW reported some emotional symptoms, feelings of unsafety or embarrassment because of the exposure to TF VAW.
- One in ten women reported that violence damaged their personal social relations with others.
- The consequences are more prevalent among women who were exposed to repeated violence compared to women with one-off experience of TF VAW, except for embarrassment, which is more present among women who experienced a single violent incident.
- Women whose perpetrators were partners were more likely to suffer psychological consequences, while those whose perpetrators were bosses were more likely to feel unsafe, and those whose perpetrators were persons only known on the internet felt more embarrassed.

When asked about the most significant consequence of experiencing technology-facilitated (TF) VAW, one in five women experienced emotional and psychological symptoms such as stress, anxiety, fear, insomnia or similar. More than one in four women (27.3%) felt embarrassed, one in five women felt unsafe and one in ten said the violence caused harm to a personal relationship (Figure 14).

Figure 15: Women who experienced technology-facilitated violence by the main consequence of such violence (single choice) (%) (N= 6662)

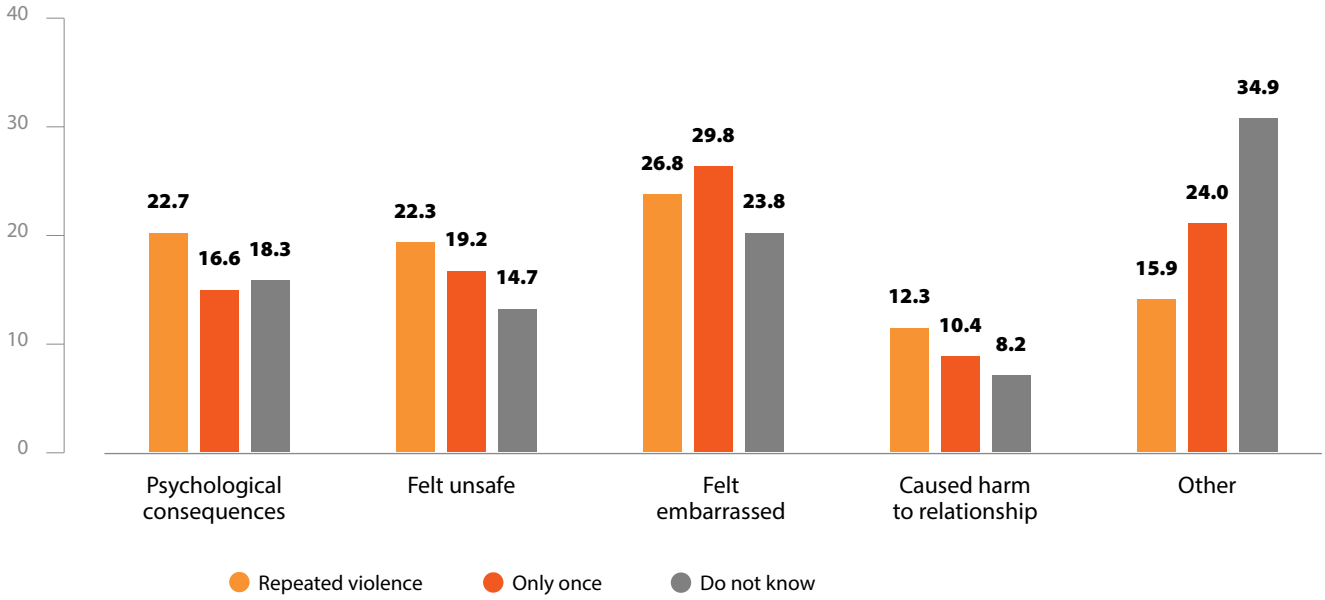


Source: UN Women ECA regional survey 2023

There are significant differences between countries and sub-regions regarding the consequences of TF violence (Tables 9 and 10 in Annex 2). Women reported psychological harm in higher proportion in Türkiye, North Macedonia and Albania (27.2%, 24.1% and 23.4% respectively), while embarrassment was the most frequent reaction among women in Moldova (42.2%). Feelings of unsafety were highest among women in Albania, North Macedonia and Ukraine, while

damage to social relationships was reported by a higher proportion of women in Türkiye, Kosovo and Bosnia and Herzegovina (14.9%, 12.2% and 11.7%, respectively). There is also a relationship between consequences and frequency of violence. For repeated acts of violence, a higher proportion of women experienced negative consequences for their psychological wellbeing and social relationships, while for one-off acts of violence, a slightly higher proportion felt embarrassment (Figure 15).

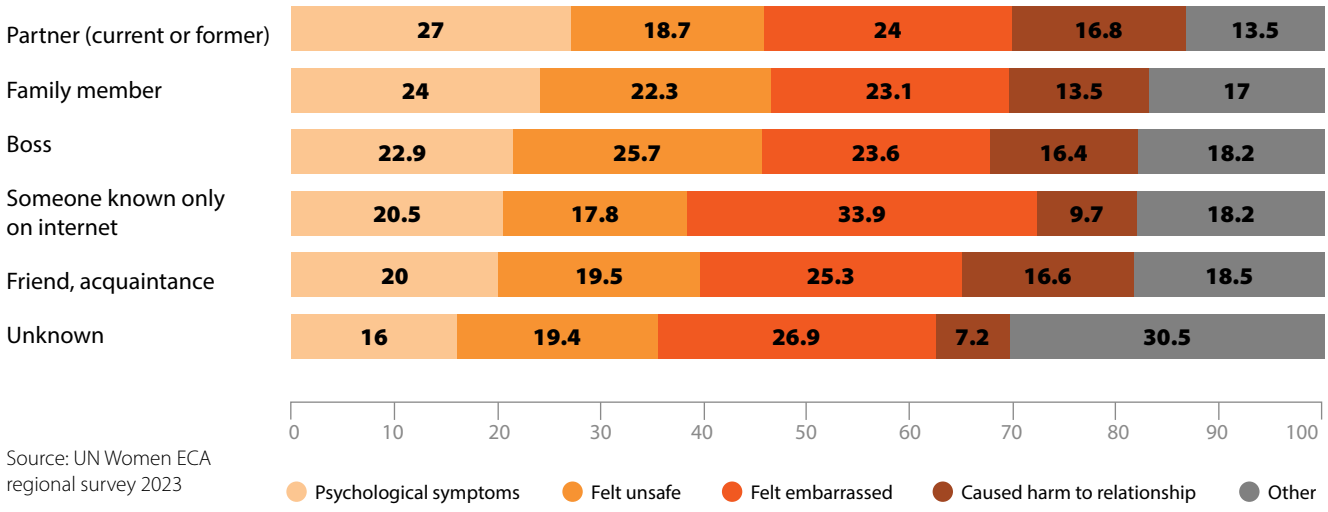
Figure 16: Consequences of technology-facilitated violence reported by women, by the frequency of the acts experienced (%) (N= 6662)



Source: UN Women ECA regional survey 2023

The consequences for women are also different depending on their relationship with the main perpetrator. More prevalent psychological damage was recorded among women who were aggressed by partners than other perpetrators, while feelings of unsafety were reported in the highest proportion among women who were abused by bosses and supervisors. Embarrassment was more often felt when perpetrators were only known to women on the internet, and other reactions (such as ignoring, ridiculing, minimizing the importance) are more present in the case of unknown perpetrators (Figure 16).

Figure 17: Consequences of technology-facilitated violence reported by women, by the perpetrator of these acts (%) (N= 6662)



Source: UN Women ECA regional survey 2023

4.6.2 Women's response to feelings of unsafety and use of precautionary measures

KEY QUESTIONS:

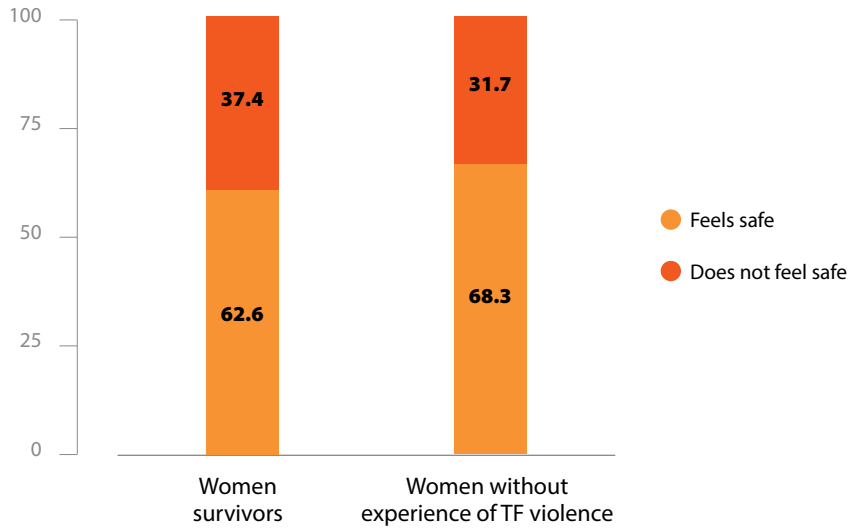
- Are there differences in feelings of safety between women with and without experience of technology-facilitated violence in regard to participating in online communication?
- Are women with experience of TF violence more cautious in their digital communication?
- Which precautionary measures do they utilize when going online?
- Do survivors of TF violence have higher expectations of violent attacks than women without such experience?

KEY FINDINGS:

- Women who have experienced any form of technology-facilitated violence feel more unsafe online.
- They are also more cautious in digital communication and more often utilize various precautionary measures, such as turning off webcams and location sharing, using different passwords for different accounts, customizing privacy settings on platforms, and only communicating with persons they know offline.
- Experiences of violence discourage women from expressing themselves on the internet, and a significant proportion becomes accustomed to violent attacks, potentially leading to increased tolerance for violence and a less proactive approach to combat it.

Experiencing technology-facilitated violence makes women feel less safe on the internet. Although the majority of women feel safe on the internet regardless of whether or not they have experienced TF violence, there are statistically significant differences in feelings of safety between women with and without experience of TF violence, with women who have experienced some form of technology-facilitated violence less likely to feel safe than women who have not (Figure 17).

Figure 18: Women's feelings of safety by experience of technology-facilitated violence (%) (N = 12526)



Source: UN Women ECA regional survey 2023

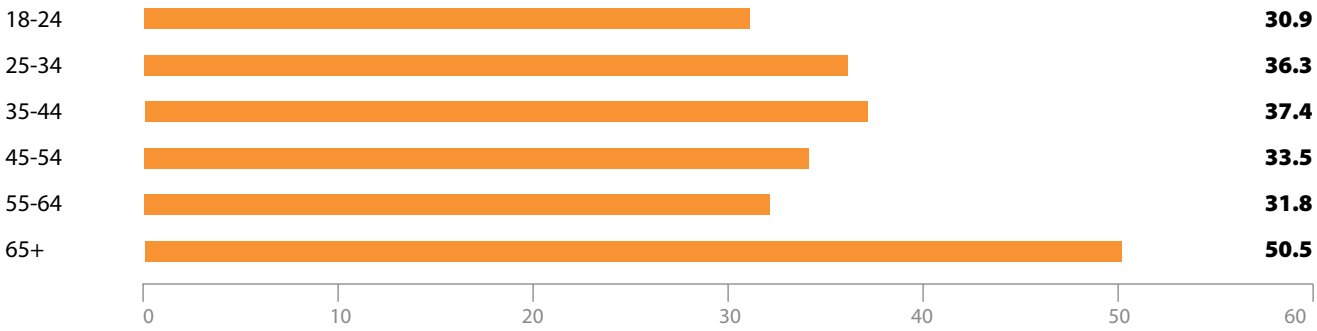
Feelings of unsafety are particularly high among women in North Macedonia (56.2%), Georgia (46.8%), Albania (45.3%), and Türkiye (38.8%), which may not only be related to experienced TF VAW but also to greater awareness of the risks of online communication. For example, among women who are accustomed to being negatively targeted online because nothing is done to prevent it, 37.2% feel unsafe, compared to 32.9% of women without such expectation (for risk awareness see figure 21).

There is also a noticeable difference between women who were exposed to TF violence repeatedly and those who ex-

perienced a one-off incident: among the former, 38.5% feel unsafe on the internet, while among the latter, 34.1% feel unsafe. There is no significant difference based on the survivor-perpetrator relationship, meaning that women's feelings of safety on the internet do not change depending on whether their experience of TF VAW was related to a partner, other known persons in the 'offline' world, persons only known on the internet, or those completely unknown.

Interestingly, while a higher proportion of younger women (18-24 years old) have been exposed to TF VAW (58% – see Figure 11), they feel safer online than older women (65+) (Figure 18). This may be connected to higher digital literacy and confidence in precautionary measures, but this assumption could neither be confirmed nor rejected based on the survey data.

Figure 19: Proportion of women who feel unsafe on the internet within each age group (%) (N = 12526)



Source: UN Women ECA regional survey 2023

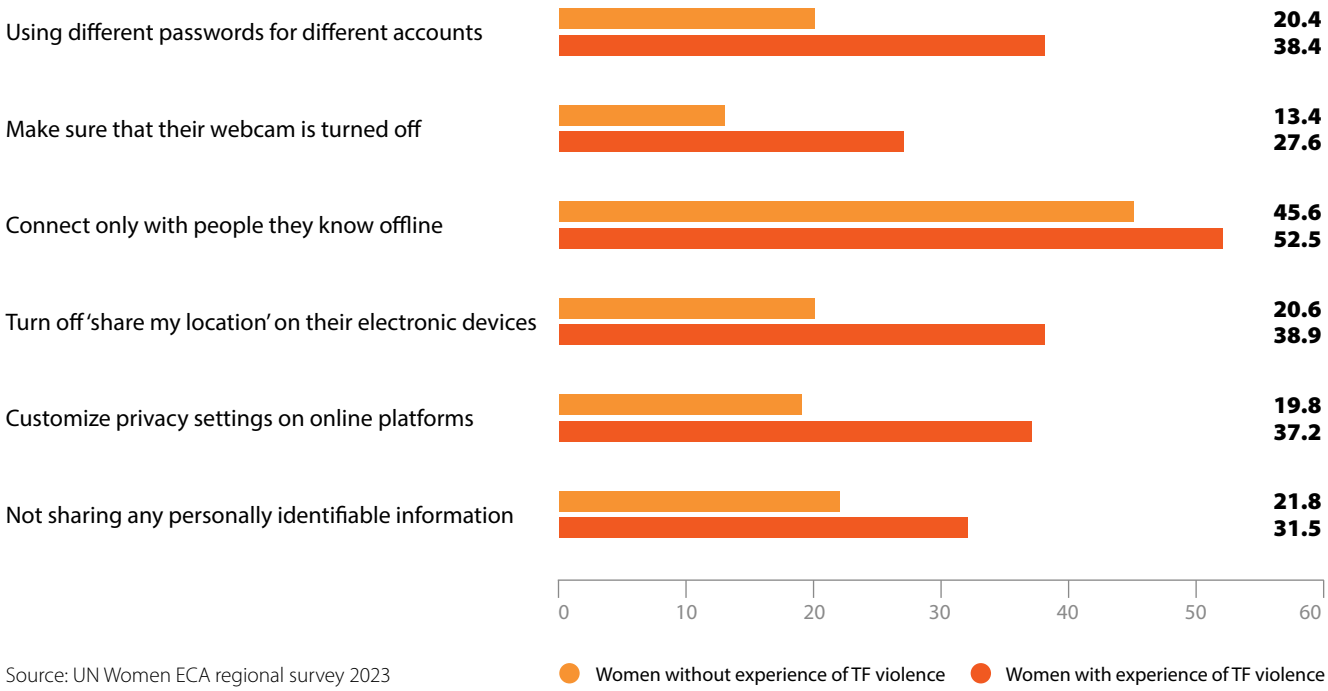
A higher proportion of women with higher education feel unsafe online than women with lower levels of education, which might be related to their higher exposure to violence, as well as greater awareness of risks. While among women with postgraduate degrees, 42.4% feel unsafe online, among women with only primary school education, 30.8% feel unsafe. Women with diverse gender identities and sexual orientations also feel unsafe in higher proportion. While among heterosexual women, 34.5% feel unsafe online, 49.3% of asexual women and 47.1% of lesbian or gay women feel unsafe.

Although longer hours on the internet increase risks of violence, a lower proportion of women who spend more time online feel unsafe on the internet. For example, among women who spend more than 8 hours every day on the internet on social media, online messaging, browsing or online gaming, 73% feel safe online, while among women who spend less than 20 minutes daily in such activities, 60.6% feel safe online. Also, a greater proportion of women who have public profiles on internet platforms feel safe online than women who do not have public profile (70.3% vs. 55.6%).

Women who have faced TF violence are more likely to apply different safety measures when going online, such as using different passwords for different accounts, turning off web cams, connecting online only with people they know offline, turning off the 'share my location' feature on their electronic devices, customizing privacy settings on online platforms or avoiding sharing any personally identifiable information (Figure 20). Although it is not possible to infer causality, it may be the case that safety measures were more frequently taken by women who experienced TF VAW exactly because of that experience.

Orange The World 2016 – Kyrgyzstan.
Photo: © UN Women Kyrgyzstan/Munira Noruzbaeva

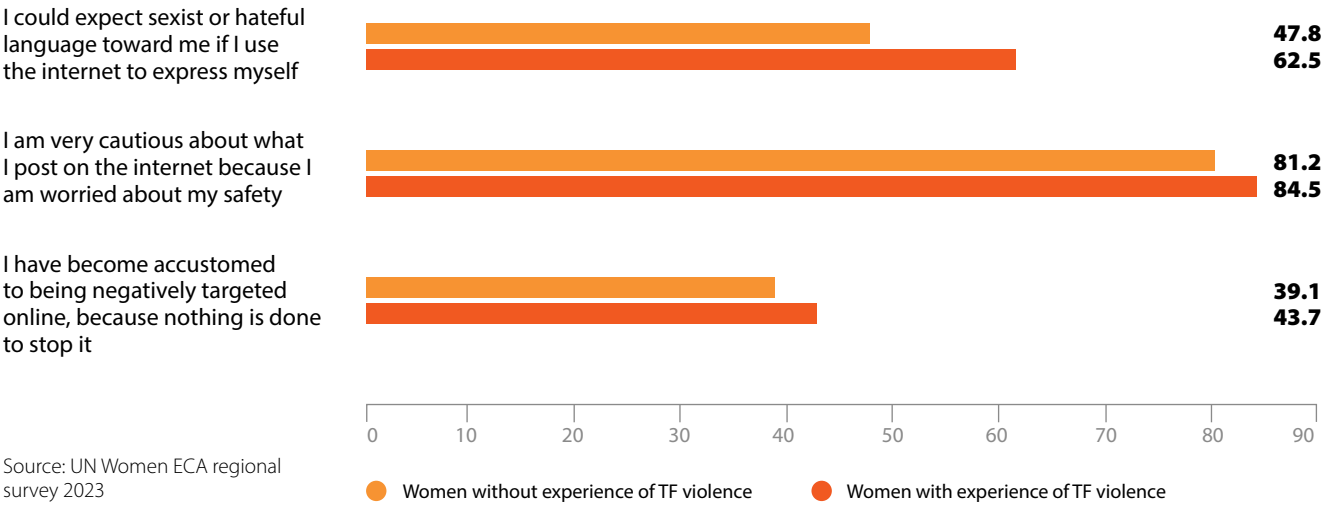
Figure 20: Women's use of precautionary measures online by experience of technology-facilitated VAW (%) (N = 12526)



Source: UN Women ECA regional survey 2023

Women who have experienced TF VAW are more likely to expect sexist or hateful language if they express themselves on the internet, which might inhibit their expression and encourage withdrawal from online communication or communities. While most women show awareness of the need to be cautious about what they post on the internet, those with experience of TF VAW report slightly greater awareness. It is concerning that a significant proportion of women, particularly those who were exposed to TF VAW, have become accustomed to such violence, which contributes to more tolerance and a less proactive attitude to combating gender-based violence in digital media (Figure 20).

Figure 21: Women's attitudes towards technology-facilitated VAW, by experience of technology-facilitated VAW (% of agree and strongly agree answers) (N = 12526)



Source: UN Women ECA regional survey 2023

4.7 REPORTING AND COMBATING TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN

KEY QUESTIONS:

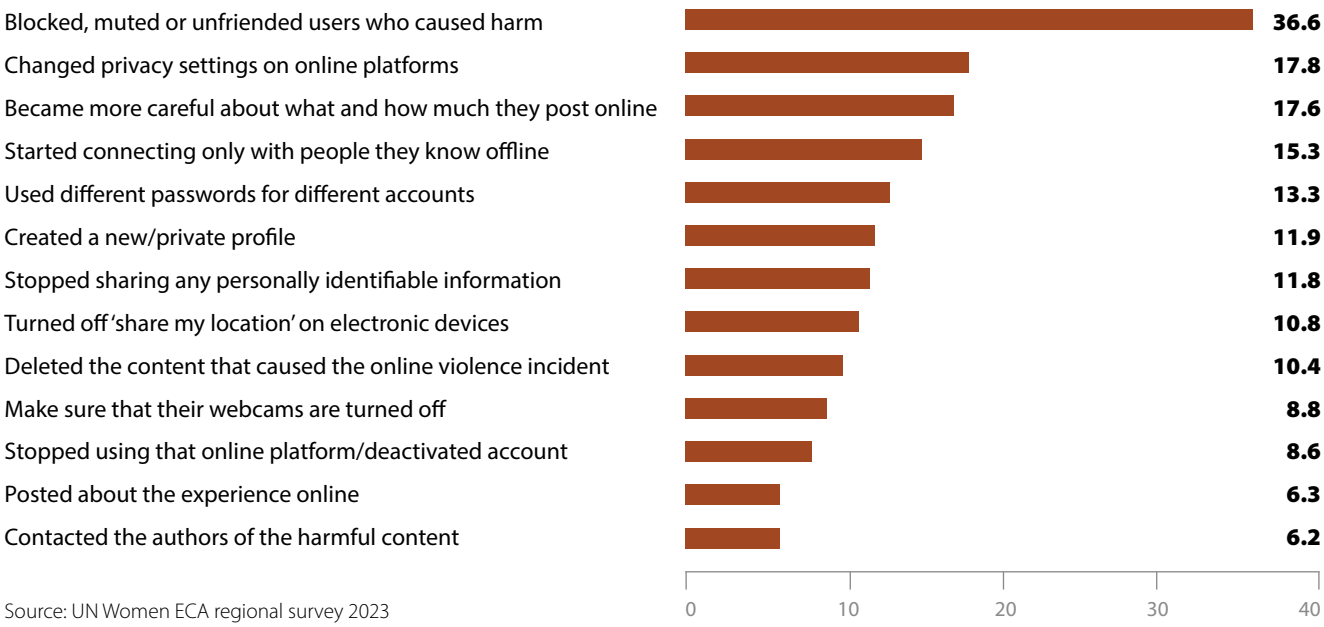
- How did women react to technology-facilitated (TF) violence?
- What are their coping strategies after experiencing TF VAW? Are women proactive in terms of reporting, publishing, sharing experiences, or are they more defensive – withdrawing, keeping to themselves?
- How many women approach the institutional system to report and seek help and how many approach their personal safety networks?
- What are the outcomes of support seeking actions?

KEY FINDINGS:

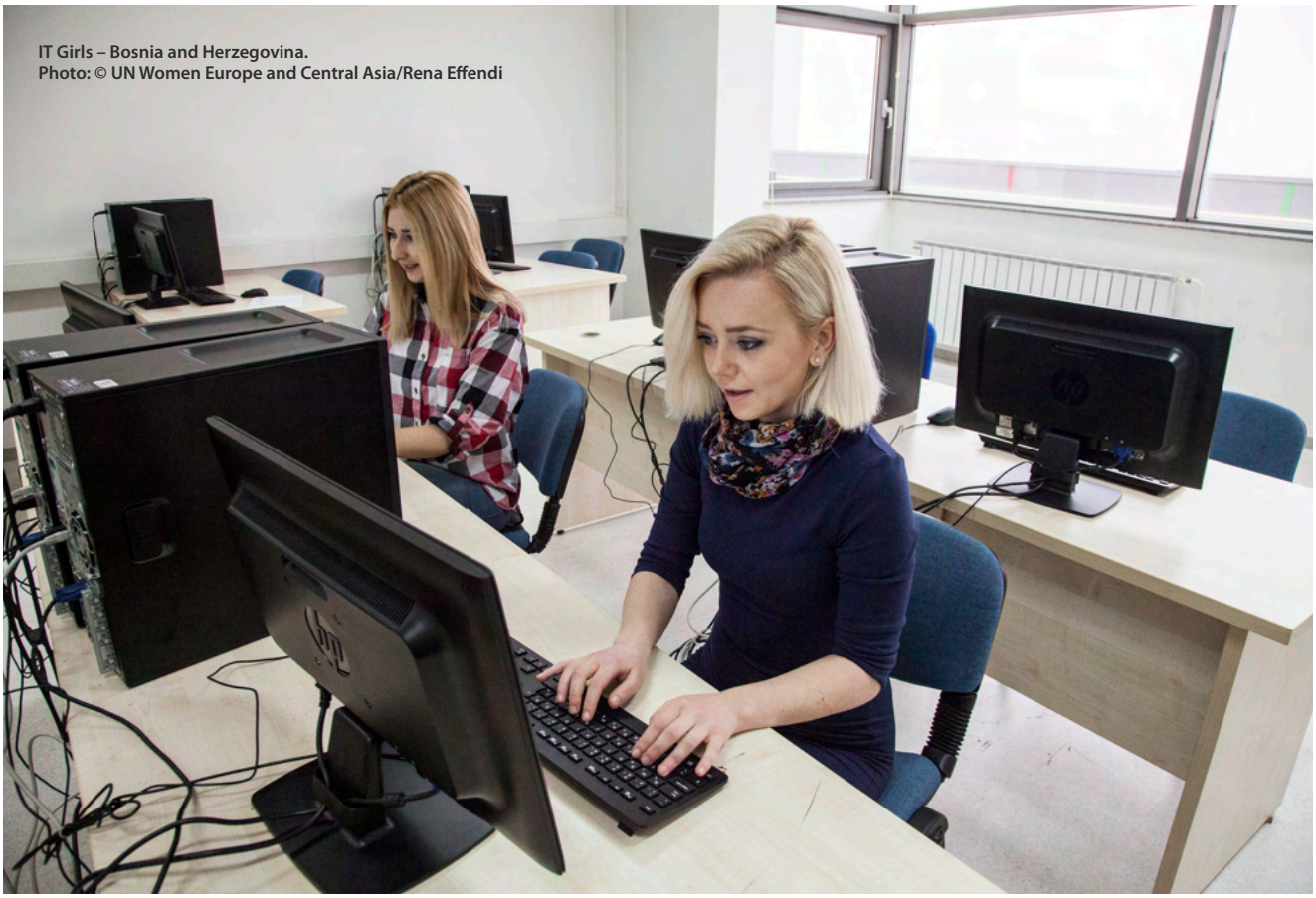
- After experiencing TF VAW, the majority of women took some steps to increase their safety on the internet, such as to block, mute or unfriend the person who caused harm.
- Women rarely report cases of violence to the police or other institutions, and even less so to non-governmental organizations; less than half of women reported their experience to friends or family.
- The reasons for not reporting are the belief that nothing will be done, lack of trust in institutions, fear that confidentiality will not be respected and fear that they will be blamed for the experience.
- Women who asked for support from their partner, family or friends often received support.
- A high proportion of women would like stronger accountability and responsibility from companies that own internet platforms and apps, more effective protection from institutions, and more awareness raising in order to empower women to prevent, report or counter TF VAW.

After experiencing some form of technology-facilitated (TF) violence, the majority of women (88.4%) took some steps related to online safety. The most common reaction was to block, mute or unfriend the person who caused harm (Figure 21). However, 11.6% of women did nothing in reaction to the violence experienced.

Figure 22: Responses to technology-facilitated violence by women who experienced such violence, by action (%) (N=6662)



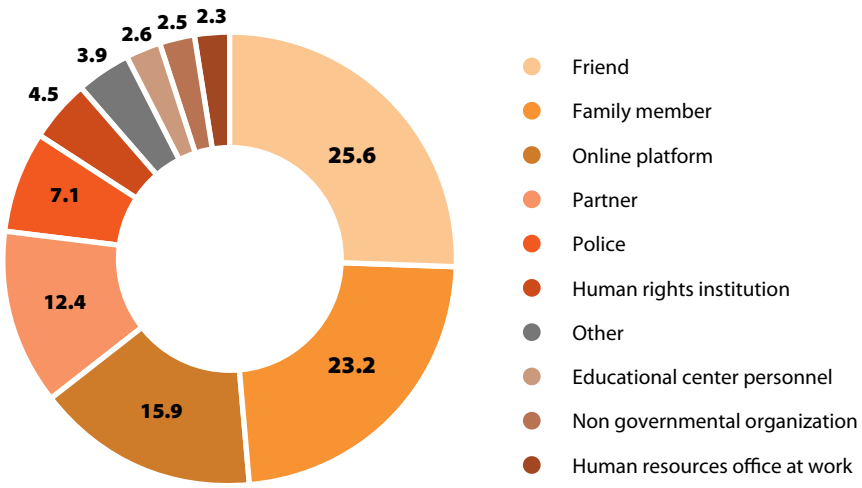
Source: UN Women ECA regional survey 2023



IT Girls – Bosnia and Herzegovina.
Photo: © UN Women Europe and Central Asia/Rena Effendi

Less than half of women who experienced TF VAW (43.8%) have shared that experience with someone or asked for support. They most often reported their experience to friends and family members, and a small proportion contacted the police, institutions or non-governmental organizations specialized in supporting victims of VAW. Answers also indicate a modest level of reporting directly to the online platforms on which violence happened (Figure 22).

Figure 23: Reports of technology-facilitated violence by women who experienced such violence, by persons and institutions (%) (N=2916)



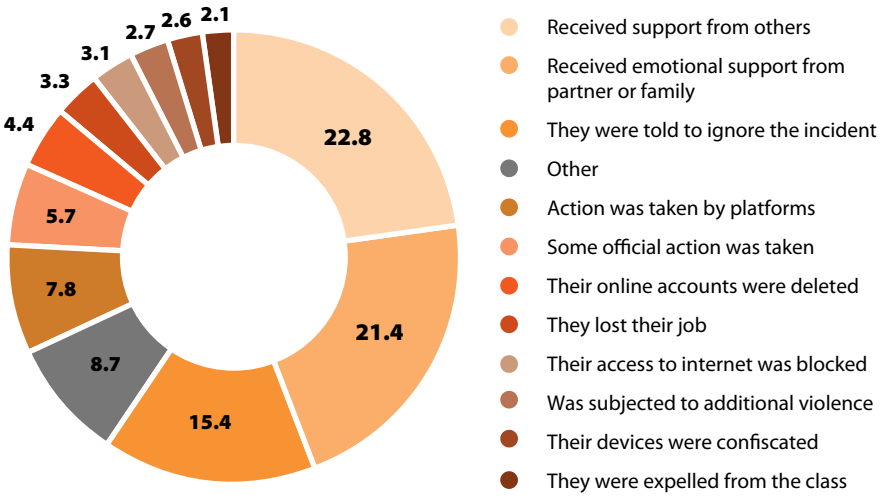
Source: UN Women ECA regional survey 2023

Among those who did not seek support or tell anyone, one-third (33.6%) did not report because they did not think it would make a difference, 14.7% did not recognize at that time that it was violence, 13.6% did not know who to report to, 9.8% did not trust other persons enough to report. 9.2% did not trust institutions, 7.8% were concerned that confidentiality would not be guaranteed, 6.3% blamed themselves and felt ashamed and therefore hid it, and 5.0% felt scared.

Among women who reported incidents of TF VAW (regardless of to whom they reported it), 44.2% got support from partners, friends or family, or other persons; 7.8% got some kind of support through an action taken by the platform on

which violence happened. Some type of official action was taken in only 5.7% cases, while 15% of women were told to ignore the case, and 18.2% of women were exposed to further violence and various negative outcomes (Figure 23).

Figure 24: Outcome of reporting of technology-facilitated violence by women who reported an act of such violence, by type of outcome (%) (N=2916)

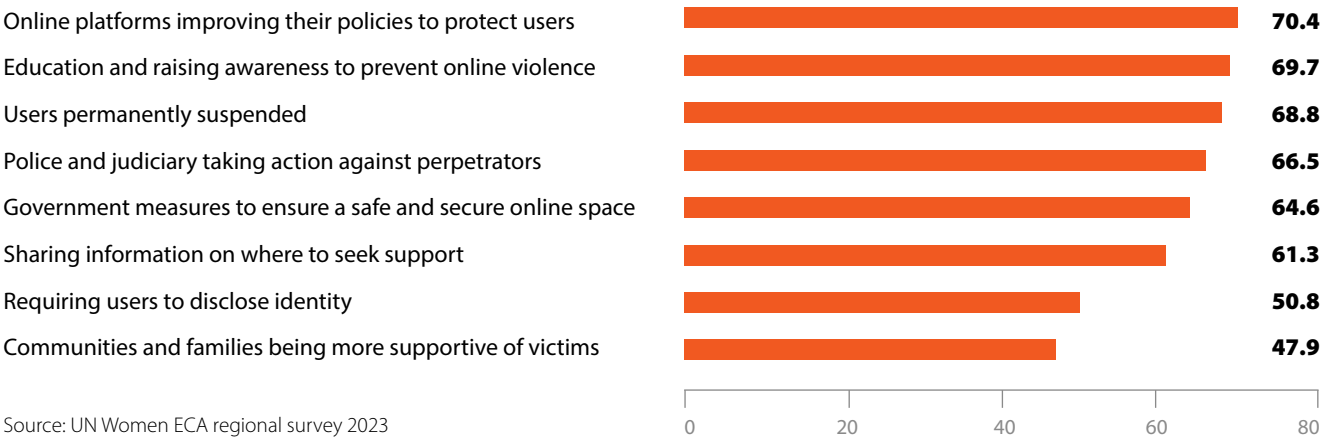


Source: UN Women ECA regional survey 2023

Among women who reported an incident of TF VAW to the online platform (465 women), action was taken by platforms in 23.7% of cases (110 women), other official action was taken in 3.5% of cases (24 women), but in 14% of cases (65 women), the representatives of the platform advised women to ignore the incident. Among those who reported the incident to police (206 women), 18% (37 women) were told to ignore the incident, while action was taken by authorities in 25% of cases (42 women).

Women were asked to propose the best ways to combat technology-facilitated VAW. Their answers emphasize first and foremost the responsibilities of online platforms, companies who own the communication platforms and their policies that protect users (Figure 24). The second most frequent proposal is related to prevention through raising awareness and education to prevent TF VAW. A high proportion of women proposed firmer measures against perpetrators, such as permanent suspension of their accounts. Two thirds of women proposed more effective reactions from police and judiciary who should take measures against perpetrators. Almost the same proportion of women proposed an improved legal framework and more adequate government measures to provide a more secure online space. They also proposed better informing women where they can ask for support in cases of TF VAW. Slightly more than half of women proposed new online policies that would require the real identities of users when opening online accounts. Almost half of women also proposed to create a more supportive environment for victims, not to be blamed and punished for experienced violence, which requires awareness raising among families and within communities (Figure 24).

Figure 25: Women's preferred ways to combat technology-facilitated VAW (multiple responses, percent of all answers) (%) (N=12526)



Source: UN Women ECA regional survey 2023

Youth Forum: "Feminist and intergenerational digital futures: Innovation and technology for gender equality".
Photo: © UN Women/Catianne Tijerina

5 · STAKEHOLDER ENGAGEMENT AND NEEDS FOR BETTER RESPONSE

There is a consensus among interviewed stakeholders of all types that technology-facilitated (TF) violence against women has increased since the outbreak of the COVID-19 pandemic and has become more pervasive and intense. This chapter reflects the views, experiences, and roles of various stakeholders engaged in the response to TF VAW; their assessment of their own capacities to effectively tackle TF VAW; and their ideas of what is needed for a better response.

5.1 THE PERSPECTIVE OF GOVERNMENTAL STAKEHOLDERS

5.1.1 National gender equality mechanisms

Gender equality mechanisms take different forms across the region. In some countries, the main gender equality mechanisms are attached to the executive power, while in others, mechanisms are attached to legislative power. In some countries, there are multiple mechanisms at national/central/state level, while in others there is a single mechanism. There are also differences in terms of the existence and effectiveness of regional and local gender equality mechanisms.

One of the key roles of gender equality mechanisms in the area of EVAW includes monitoring and leading initiatives for revising legislation, particularly in regard to alignment with Istanbul Convention within countries that are signatories.

Their role is to lead the processes of designing and implementing national gender equality and EVAW policies, organizing or supporting various awareness campaigns, coordinating gender equality policies and mechanisms horizontally (across ministries) and vertically (between local and central governance levels), and collaborating with other stakeholders, such as human rights institutions, ministries, parliaments, civil society in designing and implementing policies and various initiatives. Interviewed representatives of gender equality mechanisms provided information about various processes regarding the advancement of legal frameworks and policies for combating VAW.

Many achievements were reported during interviews. It is clear that alignment with the Istanbul Convention (which was not only found among signatories but also among others, such as Kosovo) is one of the main processes: legislation was changed to align with the Convention, multisectoral response was initiated or improved, and a more comprehensive understanding of the diversity of forms of VAW was introduced (for example, more focus on psychological and economic violence, stalking, forced marriages, sexual harassment).

> ***'I don't think we have achieved little. We have advanced toward the elimination of VAW. We established the system for support, but there is always the issue of effective implementation of laws and regional distribution of services. There are big differences in the availability of services and multisectoral responses between local communities.'***

(Representative of gender equality mechanism, Western Balkan country)

At the same time, they reported a need to further improve legislation, policies and institutional capacities to more effectively address TF VAW. Even when EVAW is high on the policy agenda, technology-facilitated dimensions are not sufficiently included. Interviewed representatives of national gender equality mechanisms reported lacking sufficient knowledge about TF VAW, which is very much needed to ensure its appropriate place in national policies.

> ***'We don't place enough focus on technology-facilitated violence against women. This is one of the huge risks for women's safety in the era of digitalization. We did not attach sufficient importance to this issue…We do not recognize it as specific among other forms of violence. When I think about it, with my experience of 20 years working in the area of EVAW, I am not sure what could be done in the situation of such violence. If I would experience such violence online, I would not know whom to ask for support or what the gaps are in legislation. I know there are many problems in regard to the evidence, but all I know is just partial.'***

(Representative of gender equality mechanism, Western Balkan country)

'We need more efforts to adjust the legal framework and policies to technology-facilitated violence against women. We know this is very brutal, especially for women in politics or in public roles. We need to adjust legislation and action plans. At this moment, technology-facilitated violence is not effectively addressed. Digital space is quite new for law enforcement structures. Cyber-attacks, harassment, and all other types are not well covered by the law.'

(Representative of gender equality mechanism, Eastern Europe country)

'It is quite a new phenomenon, and it is not easy for institutions to know how to deal with it. We need more instruments, more knowledge, strong profiles of people that are specialized in violence against women… We need a more holistic approach.'

(Representative of gender equality mechanism, Western Balkan country)

Regional and international cooperation is highly appreciated by stakeholders. As indicated by representatives of gender equality mechanisms, in the sub-region of the Western Balkans, the Regional Board for gender equality was established in 2015 with the support of European Institute for Gender Equality (EIGE). Initially it focused on the implementation of UN Resolution 1325 on women, peace and security, but with time it expanded its work on other topics, such as economic empowerment of women, status of women, etc. In interviews, some representatives of gender equality mechanisms suggested to raise the issue of TF VAW in future gatherings.

5.1.2 Public institutions in response to technology-facilitated violence against women

Multisectoral response mechanisms

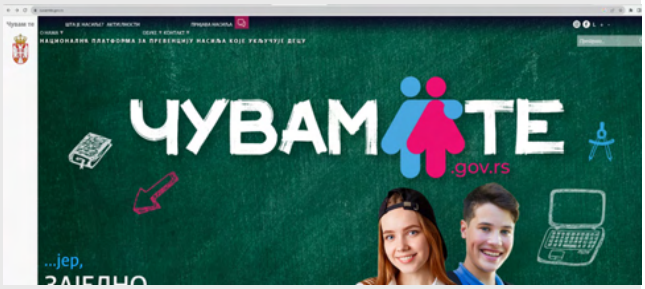
Services in support of TF VAW, when available, are integrated into services in support to survivors of VAW in the public/state service sector. Information collected through interviews with stakeholders indicates several weaknesses in the existing capacities of the system for addressing VAW to adequately respond to TF VAW:

- TF VAW, particularly violence committed by unknown perpetrators, or generalized violence against women on the internet in the form of hate speech and misogyny are most often out of the scope of available services in support to victims of VAW;
- TF VAW is mainly recognized by public service providers as the use of digital tools or channels within cases of intimate partner and domestic violence;
- Existing specialized public services to support to victims of TF violence are dedicated to children rather than women. These are usually web platforms through which children can report technology-facilitated violence and get information about forms of violence, measures of protection, available services and similar.

Stakeholders representing institutions engaged in response to VAW and domestic violence have reported significant improvement of multisectoral cooperation for addressing violence against women over the last several years. This can be attributed to a great extent to the reforms grounded in

Serbia: I protect you (Čuvam te)

The web platform 'I protect you' was established by the Republic of Serbia under the cabinet of Prime minister. Children can report violence via the platform, which also offers awareness raising content for children, parents, and teachers in regard to online violence and peer to peer violence.



the Istanbul Convention. Multisectoral teams composed of representatives of the police, social protection, judicial institutions and other stakeholders (depending on the country-specific modalities or specific local communities) are established at local level to varying degrees in all 13 countries. However, these mechanisms are not designed specifically for TF VAW, and information obtained through qualitative research about their effectiveness indicates remarkable variability among countries as well as among regions. In some communities, these local EVAW mechanisms are more effective, while in others, they mainly exist only formally. Generally, all interviewed stakeholders are aware that multisectoral response mechanisms are not sufficiently equipped with resources to address TF VAW. They lack knowledge, means and other capacities to effectively engage with cases of TF VAW.

Cybercrime police

One of the institutions that represents an important pillar of protection for TF VAW and which is rarely included in EVAW multisectoral mechanisms is **cybercrime police**. As described by some of the representatives of this police branch, their role is, among other things, to continuously monitor social networks and other online spaces to support investigations of other police departments as necessary to identify criminal offences in cyber space and to refer to prosecution when crimes are evidenced.

In some countries, challenges that police face in performing their responsibilities in the area of TF VAW are related to overlapping responsibilities. If a current or former partner commits violence against a woman by publishing her intimate photos on the internet, this falls under the jurisdiction of the domestic violence unit, and if the same is done by an unknown perpetrator, the case will be assigned to the cybercrime unit. Cooperation between domestic violence and cybercrime units is not always clearly regulated. Sometimes the domestic violence unit would collect evidence related to digital technologies, for example taking data from mobile operators, while in other cases they would ask for support from the cybercrime unit. This is decided on a case-by-case basis.

As explained by representatives of the cybercrime police, it is often much more difficult to tackle TF VAW than 'offline' VAW as it can be very complicated to identify perpetrators. Depending on the media used to perpetrate violence, there are different technological possibilities to identify perpetrators. For cases where violence happens online, the identification of the perpetrator goes through the identification of IP address. It was explained that it is often difficult for perpetrators to effectively manipulate IP addresses, so eventually they can be caught. For that, cooperation with online communication platforms is crucial. As indicated by several representatives of cybercrime police units, cooperation with Facebook and Instagram is positive in cases of child pornography. They are cooperative and assist the police in identifying perpetrator and provide data on accounts (based on a court warrant), but this occurs only in cases of child pornography, terrorism, drug-related crime, and human trafficking. This kind of cooperation does not include VAW. TikTok and Snapchat were labelled as much less cooperative. Police requests were not answered for months, which prevents the identification of perpetrators and the collection of evidence.

It is particularly difficult to identify perpetrators who use peer-to-peer programmes, which is often the case for the dissemination of pornographic materials. These programmes require advanced technology to tackle. However, available resources in terms of knowledge, technology and personnel are often not optimal for such complex tasks.

It was emphasized that **international cooperation between police forces** is very important for effective action against TF VAW. Representatives of the police from Western Balkan countries indicated very good cooperation with Interpol and Europol. That cooperation includes not only joint work on criminal cases, but also capacity building activities through training sessions organized by Interpol and Europol.

Many stakeholders representing different institutions in the system for response to VAW indicated that protective measures are nowadays much more effectively introduced and implemented. In some countries, these measures by default also prohibit the perpetrator from contacting the victim through information and communication technology.

Justice system

The justice system faces many obstacles in regard to TF VAW when it is international. It is difficult to get statements and to translate statements or other documents. Cross-border cases are time-consuming and raise questions of jurisdiction when it comes to applying sanctions. Generally, the criminal offense should be processed in the country where the perpetrator is located, but it is difficult for victims to access justice systems in foreign countries.

In some countries, **free legal aid** to victims of violence is available in the judiciary system, while in others it is only available if provided by NGOs. There are also examples of specialized services for perpetrators within the justice systems. The following example from Georgia demonstrates the efforts to prevent recidivism among perpetrators of violence against women by introducing voluntary therapeutical programs in prisons for sentenced offenders. While a promising initiative, the service shows limitations, as it is not adequately integrated within the broader system for prevention and protection, lacking proper links with survivors and programmes in their support.

Georgia: Special Penitentiary Service

This institution is established under the Ministry of Justice and its function is the rehabilitation of prisoners. It is a decentralized agency present in all 13 prisons in the form of therapy programmes for convicted perpetrators. Personnel include social workers and psychologists. During their prison term, perpetrators are allowed to communicate with victims and are even allowed to have 24-hours visits from victims. The heads of the service are aware of the risks related to communication and visits, but current rules prevent them from developing a more appropriate approach. Gaps in the service are related to the fact that service personnel do not have contact with victims, so they cannot get insights into the behaviours of perpetrators and thus lack information to conduct proper risk assessments.

They only get information from perpetrators themselves, which is often biased. Contact with victims is allowed only with the consent of the perpetrator, which is often not the case. There is no collaboration with the prosecutor office, and these gaps prevent the service from providing a more holistic risk assessment that would be in favour of the victim.

During the research, interviews with two beneficiaries of the service were conducted.

#orangetheworld – Albania.
Photo: © Women in Development Korçe NGO

Availability of data and administrative records

Lack of data on TF VAW is one of the main gaps in the system for prevention and protection. Until recently, data on the prevalence of partner and non-partner violence against women were limited in the sub-region. Only a few studies, based on representative samples across the region (e.g., in Albania, Bosnia and Herzegovina, Georgia and Serbia), were available prior to the OSCE-led survey on the safety and well-being of women, but they were not comparable. For the first time, this 2018 survey provided comparable and systematic data on prevalence, characteristics, consequences of violence against women, reporting and access to services for 8 countries (6 Western Balkan countries and Moldova and Ukraine). After the OSCE-led survey, countries in the Western Balkans continued to work on producing statistics on VAW. Thus far, North Macedonia and Serbia have introduced VAW surveys aligned with EU Fundamental Rights Agency (FRA) methodology. However, these surveys do not adequately include TF VAW, so the official survey-based statistics still do not provide adequate data.

Türkiye: Research on violence against women in politics

In some countries in the region, research initiatives aim to investigate technology-facilitated violence against specific groups of women who may be more exposed to such violence. One such example is research conducted in Türkiye on violence against women in politics.

According to this new research,[84] women in politics in Türkiye face different forms of violence throughout all phases of their political lives, including technology-facilitated violence. As women politicians' visibility increase in traditional and social media around election cycles, they are subjected to online gender-based discrimination and violence, often focused on their appearance. The research also reveals that women politicians are often targeted with violent and sexually explicit smear and harassment campaigns on social media, as well as other acts of violence in communication with constituents after they have been elected. The report, produced by UN Women Türkiye with the technical support of Terra Development Cooperative, was published in October 2023.

When it comes to administrative records provided by various institutions engaged in the response to VAW, the main trend across the region is incomplete data records. There are several gaps in administrative data. The most common case is that each institution has its own records and databases, which are not synchronized nor linked between police, judiciary, prosecution, and social protection sectors. In rare cases where a unified database is established, it is limited to domestic violence and does not include other forms of VAW. Again, there is no focus on TF VAW, and it is not possible to identify cases which included different forms of TF VAW. There are also other shortcomings within such databases. For example, in some countries, cases are recorded only if they are taken to prosecution and judiciary.[83]

Information obtained through qualitative research indicates that professionals in all sectors in many countries were subjected to trainings and awareness-raising in regard to gender equality, EVAW, and changing stereotypes. However, participants in the interviews and focus groups pointed to existing prejudices and lack of knowledge and competences to work in prevention and protection from VAW, particularly in regard to technology-facilitated dimensions.

83 Similar challenges were also identified also in the EU, as reported by EIGE. (EIGE, Police and justice sector data on intimate partner violence against women in the European Union, https://eige.europa.eu/publications-resources/publications/police-and-justice-sector-data-intimate-partner-violence-against-women-european-union)

84 UN Women, Terra Development Cooperative (2023). Violence against Women in Politics in Türkiye. A Qualitative Study

5.2 THE PERSPECTIVE OF INDEPENDENT HUMAN RIGHTS OVERSIGHT INSTITUTIONS

Countries in the region mainly have generalized independent but governmental human rights institutions, such as Ombudspersons, but few have specialized human right institutions dedicated to the protection of equality or protection from discrimination, including based on gender. In the case of generalized Ombuds offices, there are often separate divisions for gender equality. Information collected through qualitative research indicates the active engagement of these institutions in the protection of gender equality and women's rights, but little to no engagement in the area of technology-facilitated VAW.

These institutions mainly supervise the implementation of laws and policies from a human right perspective, screening the work of institutions for discriminatory practices. As indicated by several representatives of human right oversight institutions, a large proportion of cases related to gender-based discrimination that are referred to them occur in the field of employment. In the area of VAW, these institutions mainly monitor whether the work of institutions is non-discriminatory, particularly regarding women from vulnerable groups (minorities, rural women, women with disabilities, etc.). Several institutions in the region are highly committed to monitoring femicide, recognizing the severity of the situation in the country and the consequences of femicide on women's overall wellbeing in the country.

High on the agenda of interviewed human rights institutions is hate speech, including hate speech against women, misogyny and sexism. In this line of oversight work, the institutions monitor the work of media, including internet portals and social media, and in some countries cooperate with audiovisual media authorities to sanction and educate media. This is particularly important in countries in which social media and internet news platforms are not regulated by media laws. While a media company can be subject to the law in their printed or electronic media, they can be out of reach of the law on their web news platforms, as they are not registered as media and not subject to the law.

The oversight institutions reported that cooperation with civil society organizations, particularly women's organizations combatting gender-based discrimination and violence against women, is crucial. The institutions rely on information from and competencies of women's CSOs. Representatives of oversight institutions emphasized that with this cooperation they are better able to issue opinions, declare remedies for discriminatory acts and advance the elimination of discriminatory practices within the work of public institutions. However, their effectiveness is often limited.

> ***'There is a lot of discriminatory, stereotypical, sexist language which is frequently used toward women in general but also individually. When a woman is a public person, politician or head of public institution, they are not attacked for their actions, but on basis of their sex. We issued some decisions which addressed sexist hate speech against women. Parliament is not eager to take measures for inappropriate language… We see that society remains in some ways very patriarchal, so daily work is required from different institutions to continuously address this. Especially during electoral campaigns – sexist language is frequently used during campaigns.'***

Representative of human rights oversight institution, Western Balkans

> ***'Cases of sexual harassment are not frequent. Women are not keen to expose experiences of sexual harassment. We had one case where we issued a decision on sexual harassment based on the grounds of gender. This was the first decision since the law was amended to include sexual harassment as form of discrimination. It was initiated by a CSO. Unfortunately, we have seen that the authorities ignored the decision. After some years they promoted the perpetrator to a higher position. Media reported on that, and CSOs reacted. That was a bad message to society. We must work more on public authorities, especially on awareness of gender-based violence, to react more effectively.'***

Representative of human rights oversight institution, Western Balkans

5.3 THE EXPERIENCES AND NEEDS OF WOMEN'S CIVIL SOCIETY ORGANIZATIONS

5.3.1 Perception of trends

In general, the research found that information and communication technology has profoundly changed the landscape of VAW and placed new requirements for prevention and protection that CSOs engaged in EVAW initiatives or direct service provision cannot currently meet adequately. Similar to governmental stakeholders, civil society organizations – whether they are direct service providers, advocacy-oriented activists in the area of women's rights, or gender equality experts – are much more engaged in the 'traditional' area of gender-based violence and VAW, and only a few are particularly focused on technology-facilitated (TF) VAW. During focus group discussions and interviews, they often emphasized that TF VAW is increasingly present in their work.

In their experience, TF VAW, unlike violence that is exclusively perpetrated offline and without using digital technologies and which stops when you separate the victim from the perpetrator, can occur 24 hours a day. The anonymity provided on the internet often enables perpetrators to be more aggressive. Content that is uploaded to the internet can remain there forever, leading to years of victimization. Part of the problem is a low 'safety culture' and lack of awareness among women. Some publish private photos and photos of their children, not understanding the risks that this may bear.

Organizations working in the area of human trafficking report that the internet and digital technologies are used more than ever for the recruitment of victims, particularly minors.

> ***'Digital violence has changed the whole context of violence against women. It gave new means to perpetrators – not one but a hundred hands. It has changed the way we treat victims, how we design services. For example, when you place a woman in the shelter, you also have to control her communication. Particularly for women that have court processes. Even when you remove a woman from the situation of violence, you did not protect her, as the perpetrator now has powerful tools to continue to harm the woman remotely.'***

(Representative of CSO, Western Balkans)

> ***'Violence continues even when a woman leaves a violent relationship. We see this in our safe house. Partners have all the passwords from women's accounts. They were forced to share accounts with them. It is very complex from the aspect of proving harm. A perpetrator may not send threatening messages. He can send love messages, he can spread these messages 'full of love' throughout joint internet accounts, but this is very disturbing for the victim. However, institutions do not see that as disturbing or threatening. It is much easier when there is a direct threat.'***

(Representative of CSO, Western Balkans)

At the same time, information and communication technologies gave new opportunities to partners or non-partners to control and abuse women. The old solutions do not work as before. It is not enough to place a woman in a shelter to protect her.

Controlling forms of partner violence have changed. Previously, forms of control were more overt: a husband would forbid a woman from visiting family or friends or would check her purse. But now, women are often unaware they are being controlled. Partners control women through shared location on mobile phones and hidden mobile apps that monitor their communication. Sometimes, though the control is more overt, women accept to share Facebook or Instagram or other internet accounts, or they give their passwords to partners so he can monitor their online communication. New digital technologies are used to record explicit videos and use them to extort money or sexual services or as revenge porn to humiliate women who did not comply with men's will. The power of this form is fierce, as women's lives are destroyed because technology enables these videos to go viral, to be spread to everyone they know, and even to go global. Content uploaded to the internet can remain there forever, repeating victimization over and over.

In addition to the universal trends and characteristics of TF VAW, there are certain specific circumstances that make it distinctive for countries in the region. One of the specific situations is related to the withdrawal of Türkiye from the Istanbul Convention. According to interviewed stakeholders, the situation regarding VAW, including technology-facilitated

Clockwise from left: Jonada Shukarasi in her room; her mobile phone showing the application; Jonada is passionate about human rights and poetry. Photo: © UN Women/Eduard Pagria

VAW, has escalated since the withdrawal. The Istanbul Convention was very important in protecting women's rights in the area of safety and protection from violence. NGOs continue to work and provide protection but in a much worse situation. Public institutions are not open, particularly not for some specific groups, such as the LGBTQI population.

Another aggravating situation is related to the consequences of the devastating earthquake in Türkiye in spring 2023. The earthquake strongly impacted the capacities of CSOs to deliver services, as funds were reallocated to earthquake survivor assistance. The price of renting space has significantly increased in affected regions and some organizations have lost the capacity to provide space for work. Consequently, their capacities to provide adequate support to survivors of VAW and to expand these services to address cases of technology-facilitated VAW are lower than before.

The war in Ukraine brought new suffering for women – increased risk of rape, sexual assault and other forms of violence which increase during conflict situations and situations of forced migration among refugees and IDPs. Similar to Türkiye, these crises make it even more challenging for CSOs to adapt and expand their services to address TF VAW.

5.3.2 Women under particular risk of technology facilitated violence

Representatives of CSOs identified diverse categories of women at greater risk of technology-facilitated VAW, according to the experience they gathered through their work with survivors or in the broader system for prevention and protection.

Women in divorce proceedings are at particularly high risk of TF VAW. They are often already victimized prior to their decision to divorce, but the process of divorce triggers the husband to be much more aggressive and 'creative' in using digital technologies to increase pressure on women to stop the divorce or to be 'less demanding' in requests related to guardianship over children, division of property, etc., or simply as revenge for her intention to divorce since divorce means a loss of control over her.

Women in public positions, particularly politicians, journalists, activists. Women political candidates are particularly under attack during election periods.

> ***'We witness online hate speech against women in politics, regardless of ethnicity. You can become a victim of hate speech on any platform. Women become easier targets than men. Women are left alone to deal with online hate speech violence. There is no reaction even from their political parties to respond and protect them.'***

(Representative of CSO, Western Balkans)

> ***'Violence against women in public positions is most visible during electoral campaigns, when women are more visible in the media. It is intended to discourage women through humiliation and degrading content. It is assumed that women accept that violence as part of the public career. As soon as they leave children at home, they should be ready to be exposed to violence. There was the case of a woman MP dancing behind birthday cake. The media published that, commenting that she could do pole dancing. We submitted a complaint to the Council for press [media supervisory body] but they replied that there are no grounds for gender-based violence, as she should accept those kinds of comments since she is a public person. Their decision was that the law on gender equality was not violated.'***

(Representative of CSO, Eastern Europe)

'During the 2019 electoral campaign, a woman running for councilor in one municipality was attacked in the most terrible way. She was the subject of a fake photo and fake profile on a porn site. She was labelled as a prostitute and people commented that she should not run for politics. That photo is still on the internet. The person who posted this is a blogger located outside of [the country]. She asked for help from some organizations, and all organizations submitted complaints to the police, but in the end, she did not submit a complaint to the police and she withdrew from the campaign.'

(Representative of CSO, Eastern Europe)

Women from ethnic minorities are at higher risk, particularly if they are in public roles or activists. Some of them have been exposed to violence for decades, and although they are still very active in women's movements as women's rights defenders, their sentiment is one of disappointment that the state did not protect them after they invested so much effort in the improvement of the system for protection and that the social context continues to be aggressive, burdened with intersecting discourse based in misogyny and nationalism.

'A large number of older women activists were silent in the face of Naziism, fascism, and hate speech, terrorizing women from ethnic minorities. They did not react. They see me as a Muslim woman that must be silent. But I need to speak out. This is my need and my way of life…Online violence has escalated. It hurts me because there is no support. I am not a victim, I am a fighter. This is how I live. I was wondering how must be for women who do not have courage, who cannot react. They constantly hacked my Facebook account.'

(Woman activist, Western Balkans)

Young women like to connect, and some even use social media and platforms as tools to earn income. They find themselves at high risk of gender-based violence in forms of blackmail, extortion, threats, humiliation, hate speech, and harassment. According to some activists' experiences, teenage girls, particularly those living in more traditional areas, are at higher risk as they are afraid to be blamed for violence and left at home without the right to education.

Women with disabilities, particularly those using software for visual or audio impairments. They use specialized software, and for them the use of phones or other digital equipment is very important. When there is an attack via phone, it is much more intense and dramatic than for women without disabilities.

Women earthquake survivors. As emphasized by the organizations supporting refugees and earthquake survivors, in the aftermath the earthquake in Türkiye, women found themselves at increased risk of TF VAW. As they lost their phones in the earthquake, they were forced to use others' phones, which increased the risk of abuse of personal data.

LGBTQI women are at higher risk, particularly in conservative communities, where they can be subjected to blackmail and extortion.

Women with HIV. If their health status becomes public, they can find themselves under attack. They are stigmatized, and according to laws in some countries, they are not allowed to have children.

'You can make a woman do anything you want if you blackmail her with her HIV status. She will live life in fear. Women with HIV cannot adopt children, which is a form of discrimination. They are also discriminated against in hospitals by medical staff. In some institutions, if they learn about their status, they will not deliver services to them. If they learn a woman is pregnant, they might force her to abort, they will humiliate them.'

(Representative of CSO)

Furthermore, representatives of CSOs participating in the research pointed to w**omen IDPs and refugees, sex workers, and trans women.**

5.3.3 Role of civil society and challenges faced

There are emerging services provided by CSOs that directly target TF VAW, but they are not many. Some organizations who dedicate their work primarily to TF VAW have established online platforms where citizens can report violence, and which represent valuable sources of information and knowledge on TF VAW.

Examples include gender.monitor.md in Moldova and the Albanian national hotline for internet safety iSIGURT.al.

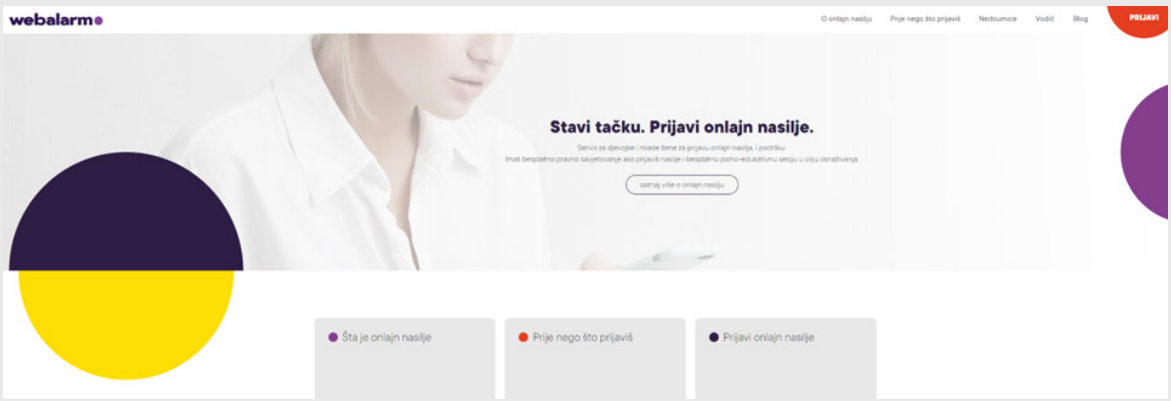
Moldova: gender.monitor.md

Gender.monitor.md was created by the Platform for Gender Equality and administered by the Promo-LEX Association, a member organization of the Platform for Gender Equality. This online platform was created to map cases of sexism in the public sphere and cases of violence against women in and between elections. The Platform for Gender Equality (PGE) is a voluntary union of 42 NGOs and civic activists that act as an active and united voice for the promotion of gender equality in all spheres of life. The Platform is a tool through which citizens and CSOs can signal in public and address cases of gender discrimination, sexism in the public sphere, including online spaces, and messages inciting discrimination.

Montenegro: WebAlarm – Put a period on violence

'Technology is galloping at such a pace that even when we manage to capture something and detect it as violence, it takes on a more terrible form five minutes later. I've turned into a terrified person because of the booming manosphere and patriarchy on the internet. We managed to modernize the patriarchy, to equip it with modern technologies. It is much more persistent, more dangerous than this traditional patriarchy, because it carries the additional challenge of a large gap in women's professional management of technologies. In the context of online violence, women have so many problems. We have created several campaigns about online violence, we are here as pioneers in the fight against online violence. As a result, we have a platform that, at the time when we built it two years ago, was the first in the Balkans.'

(WebAlarm founder)



WebAlarm is a platform where women and girls can report online violence and get support. They can access free legal aid and psycho-educative support with aim to be empowered.

Albania: iSIGURT.al

iSIGURT.al is a National Platform for Safe Internet in Albania, whose purpose is to provide support to children and young people from online violence and hate speech. This is national service provided by CRCA/ ECPAT Albania, non-profit organizations which are part of the International ECPAT Foundation. The Platform deals with all issues of online violence, especially online sexual abuse, extreme bullying and hate speech. Citizens can report violence to the platform which will evaluate and share the report with responsible authorities. The platform monitors and refers but does not provide direct psychosocial or similar support. The platform conducts awareness classes in schools, universities, community centers and various institutions to inform them about online violence and where they can report such issues. Page www.iSIGURT.al is visited by 20,000 - 30,000 people annually of different ages, who can also find information and guides on how to be safe online. The information is also tailored to the needs of professionals, such as police, teachers, social workers, NGOs, etc.

The platform is a partner of major global platforms. The main achievements include the high percentage rate of pages and accounts closed in response to reports, the establishment of strong partnerships at global level with all major social networking companies, and the openness of the media. When it comes to challenges, funding is always an issue, especially in countries like Albania and the Western Balkans, where the level of awareness on online life, protection and respect is very low. Challenges are also weak laws and policies in institutions, from law enforcement to regulatory bodies..

Challenges identified by CSOs

Representatives of CSO service providers and women's rights activists listed numerous challenges faced by civil society in attempting to provide adequate prevention and protection services related to TF VAW. They noted obstacles in providing 'traditional' support services that are mainly focused on offline domestic and partner violence and very little engagement with technology-facilitated violence, except in the context of domestic or partner violence. It is worth noting that challenges present in their work with offline violence are also present in their work with technology-facilitated forms and dimensions of TF VAW, with additional challenges related to specific nature of TF VAW.

Inadequacy of legal framework and ineffective implementation. There is consensus among interviewed representatives of CSOs that legal frameworks in all countries are not adequate to properly address TF VAW. It was noted that there are some legal provisions that can be applied for cases of TF VAW, but due to ineffective implementation of laws, existing legal provisions are often not used for processing TF VAW cases. Moreover, due to trends toward backlash against gender equality, in some countries, legal provisions are used to punish victims.

Lack of awareness and underreporting. Women are still not aware that harmful experiences to which they are exposed to online or with other use of digital technologies are forms of violence. But this is not the only reason for not reporting TF VAW. Fear of retribution, shame, embarrassment, or lack of trust in institutions are also mentioned as important reasons for underreporting.

The existing multisectoral mechanisms for protection from VAW do not include technology-facilitated dimensions and cannot provide adequate response in these cases. Respondents indicated that multisectoral cooperation mechanisms are mainly established but they lack capacities in terms of knowledge, skills, protocols that would enable them to provide adequate protection in cases of TF VAW. Some respondents indicated that in their current capacities, it is unlikely that multisectoral mechanisms would be able to expand their services to include technology-facilitated dimensions of VAW beyond cases of intimate partner and domestic violence, as they are not even sufficiently effective in addressing the cases of offline partner and domestic violence for which they are established and trained. Their experience with public service providers indicates that professionals from institutions responsible for protection from VAW still often show stereotypes, prejudices, and in-

UN Women and Google partner for VR films about women human rights defenders. Photo: © UN Women/Ryan Brown

adequate treatment of victims. They still blame victims for violence and encourage women to 'forgive,' 'forget,' and pardon the perpetrators. They often react only in severe cases of physical violence but disregard other forms of violence, such as psychological, economic, stalking, and sexual harassment.

Participants shared experiences of successful cases in which they managed to stop technology-facilitated violence against women. They reported that police do not take seriously such cases, or that girls and women do not want to go to the police as they find CSOs more discrete.

'A man from [Central Asian country] repeatedly blackmailed a 13-year-old girl with her intimate photos. He threatened to distribute these photos through social media if she did not send new erotic photos. The organization asked the police for help, but they did not react. The director of the organization then wrote to the perpetrator warning him that legal measures will be taken if he does not stop, presenting the articles of law by which he can be sentenced to 17 years in jail. The violence has stopped.'

(Woman activist, Central Asia)

In other cases, police simply do not react to cases of TF VAW due to a lack of training, unconscious bias or other reasons, as reported by activists.

'The normalization of violence is very dangerous and it happens when institutions do not react. With the young blogger example [blogger who committed sexual harassment against women], police only reacted when a deputy from Parliament said that it should be punished. Only after that, after pressure from political circles, the police reacted. We see double standards.'

(Woman activist, Eastern Europe)

There is no cooperation between cybercrime police and other police departments as well as other institutions in the multisectoral mechanism or with CSOs. Also, procedures implemented by cybercrime units are not in line with human right standards in protection of women from violence. Women's technology is often confiscated for investigation.

'Women report they feel punished when their phones are taken [as part of an investigation]. They need to purchase a new phone, a new SIM card, and they lose contacts, sometimes support groups. Women often perceive this as an intrusion into their private space. When their phone is taken for forensic investigation, women do not have control over the content that will be seen by investigators. This is an issue of protection of personal data.'

(Woman activist, Western Balkans)

Weak prevention and screening in the education sector. This is considered as one of the key sectors in the prevention of VAW. Educational institutions are places where young persons adopt norms and shape their attitudes. However, in schools across the region, human rights, women's rights, non-violent communication, and prevention of gender-based violence are not adequately addressed. Insufficient attention is paid to digital literacy and safety on the internet. Teachers are not sufficiently educated about technology facilitated violence, yet these forms of violence are very much present and could be extremely harmful for young people. University education does not systematically include topics related to women's rights. Cases of cooperation between CSOs and academia are more often the exception than the rule.

Dina's testimony* (age 26): Stalking

The stalking started in 2019. The stalker was a colleague from a study group. It started with light socializing, together with other colleagues from the group, but from the very beginning I noticed some warning signs. He started to repeatedly contact me, to contact my friends, to monitor my accounts. I was blocking his accounts, but he would use fake accounts. The turning point was when he saw on my Facebook profile that I would attend some literary event. He came there and saw my friends, but fortunately, I was not there. I stopped publishing any information on my accounts, but he would discover where I would be from accounts of my friends. At that point I realized that I don't want to be defensive, to close accounts and withdraw, but I wanted to report him. So I reported him to the police.

At that time, I started to become interested in VAW and started to learn about that. I learned that stalkers can switch to new victims. And I discovered that he had another victim before me, also a student from the faculty. With me his threats were more subtle. He would write to me 'I will be whatever you want, but I will not be without you.' Women who are aware of VAW can recognize the threat in this. The other victim was not so informed, so he was more direct with her. He threatened to rape her and to kill her brother.

After a one-year break, he returned to the faculty but changed the study group. He also changed his approach to me. I was so afraid, and when he saw that I was afraid, he became more aggressive. He would approach me, threaten me, yelling throughout the faculty halls. I reported this to the faculty authorities, but they did not show understanding. At the same time, my case was under investigation by cybercrime police and a criminal case was processed by the court, but the faculty authorities did not recognize that as violence. They claimed that this is dating and not violence. The police were relatively OK. They were not completely sensitized, but they behaved with empathy, like I am a beautiful young girl so they want to help me. But this lasted for a long time. I reported the violence in September 2019, and they issued a restraining order in March 2021. The stalker confessed and this was taken for granted so they did not even inform me. The restraining order would have been issued much faster if we had lived together, because then it would be grounded in the Law on prevention of domestic violence. But in my situation, it was based on the criminal code and went much more slowly. His other victim gave up and left the studies. She realized that he was stalking among faculty peers.

So the first phase finished in court in 2021 with a restraining order which included prohibition of communication, including online, and three years of mandatory therapy. The second phase started in August 2022.

At that time, I got a call from the cybercrime unit. A woman inspector asked me to come to the police station urgently. There I found out that he messaged the President of Serbia from his fake account to say that he would kill me with a gun because I ruined his life and the life of his family. Because it had all gone too far. The police arrested him and found not only a gun but a whole arsenal of weapons, including bombs.

They realized that he wrote from the same account to the USA embassy, but they did not react. They realized that he wrote to me as well, but since he was blocked, the messages went to a special folder so I did not see his messages, which were really nasty. This was a violation of the restraining measure and a new criminal act – endangering the security of a person. This time, the reaction of the police was terrible. They tried to persuade me that this could not be counted as violence because he is sick. Eventually they arrested him and took a statement from me, but their behaviour was really bad. Their behaviour was additional violence. They did not want to inform me about the process. When the stalker was released, they sent information to the faculty and not to me personally. They ignored my requests for information. They were completely closed.

So what could I do? I went to the media, and the case went viral, many journalists were writing about case. They contacted the prosecution and the public prosecutor in charge of the case was replaced. But at the end, this had little effect. The investigation is still ongoing. A psychiatric assessment was done with the conclusion that he is not accountable, and the sentence was again mandatory therapy without a prison sentence. The restraining order is still effective.

I don't have energy to go from institution to institution. All of that is secondary victimization. It is not fair that I have to live with this every day. I have a feeling that I was in prison much more than him. The fact that they proclaim he is not accountable will not stop him. At this moment, there is no final court decision so he is not in therapy. Last time his mother was complaining that he does not want to take medication, and she cannot force him.

I divide my life into the periods before and after the stalking. It impacted whole my life. Making the case public was also traumatizing. Those misogynist spokesmen comment on you or people put you in the role of victim. I am now doing my PhD in the area of VAW, and I was activist in a women's right organization specialized in EVAW because like this I am not in the role of victim. I cannot stand to be a victim. But still, I have two parallel narratives in my head. On one hand, I know that it would be foolish not to be 150% cautious. On the other hand, I know if I am always 150% cautious, I will go mad. Therapy helps me, but feminism helps me as well.

Evidence from qualitative research
*Not her real name

Lack of recognition and support from state. Since organizations mainly provide support to survivors in regard to TF VAW as part of partner or domestic violence experience, the licensing of such services is an important issue. Many respondents talked about the difficulty in licensing services**.** In countries where licensing of services is mandatory, the criteria are too demanding, while at the same time, there is no stable financial support for service delivery. Moreover, many respondents complained that governments do not recognize nor value important services these organizations provide and the funds from public budgets have been shrinking. Participants in focus group discussions indicated that state actors do not recognize the quality of services provided by NGOs and instead of supporting NGOs with high competencies and longstanding experience in service provision, they open public services without adequate staff and protocols.

'Three years ago, one shelter was opened in [capital city], but they do not work according to standards, the approach is not sufficiently women centered. Sometimes they even receive men, sometimes homeless women, so it is not very adequate. Nor is their approach to beneficiaries adequate, they do not know how to talk to women, which questions to ask, to use psychologists. Women complain that it is not appropriate. Much better situation is in shelters run by NGOs, with a more professional approach and women centered.'

(Representative of CSO, Central Asia)

The capacities of organizations to provide support in cases of TF VAW is affected by their general ability to ensure sustainability and to expand their work to more diverse dimensions of TF VAW. In some countries hostile attitude towards CSOs are on the rise and organizations are struggling to ensure sustainability. For some activists, lack of commitments demonstrated by governments are very disappointing after decades of invested efforts in the improved protection of women from VAW.

> ***'For three decades we talk about zero tolerance to violence. I am ashamed to talk about that anymore because what we have is an increase of violence. We have cases when victims are sentenced to jail because they defended themselves from sexual violence. We can throw our licences [for support services] into the river. They are useless. If organizations are licenced, then you have to finance them. There is no political will, women's rights are not even mentioned anymore. We have the case where one man who was a perpetrator was assigned by political will to be manager of a shelter for victims of human trafficking. There were initiatives to close these women's organizations, but anyways they are closing us silently as they do not provide any funds for these services.'***

(Representative of CSO, Western Balkans)

Their low capacity to provide continuous support to survivors and to adjust their work to more diverse forms of TF VAW are also impacted by insufficient funds from donor sources and donor-driven, project-based funds which prevent service providers from tailoring their services beyond donors' needs and requests. Besides, project-based funding is short term and undermines the sustainability of services.

> ***'Donors give little funding for the protection of women's rights, only for projects. There is a need to fund organizations to provide continuous support. It is difficult to protect someone for 10 years without stable funds. Very ineffective judiciary.'***

(Representative of CSO, Central Asia)

The CSOs' capacities to provide support to survivors in relation to their experiences of technology-facilitated violence are influenced by their cooperation with government and state institutions. This cooperation is described in different ways by organizations. It is not easy to capture main trends, but experiences can be grouped into a few categories. In one category are organizations who report deteriorating trends of cooperation with government, police, and judiciary. Sometimes this does not apply to an entire country, but specific local communities. However, in general, organizations from Serbia, Montenegro, and North Macedonia reported more often these negative trends of declining cooperation. In Bosnia and Herzegovina, there is much stronger support to CSOs service providers by the state, but experiences are different between entities and also between cantons in the Federation of BiH. Participants form Albania and Kosovo indicated improved cooperation, but participants from Northern Kosovo indicated big institutional gaps due to the conflicts. Representatives of CSOs from Eastern Europe and Central Asia report more positive trends in cooperation with state institutions.

Cross-border violence is big challenge for organizations as they lack the means to access justice systems in other countries. One case that involved a perpetrator and victim from two neighbouring Western Balkan countries is illustrative. The organization was approached by a girl who was briefly in a relationship with a young man from a neighbouring country. When he returned to his country, he started to blackmail her and threaten to publish her intimate photos. He was extorting money, and the extortion lasted for two years because the young girl was afraid to tell anyone and living in very patriarchal community. She finally approached the organization for the help, but the organization was not able to assist as they were told that the girl should report the case to the police in the perpetrator's country. This was not possible, so the organization took a different approach to work with her to pick one family member who could be trusted and helpful. In the end, the case was solved with the assistance of her uncle who contacted the perpetrator.

CSOs service providers lack knowledge and capacities to address issues of technology-facilitated violence against women. The majority of service providers participating in the research provide 'traditional' specialized or general services to victims of VAW: shelters, psychosocial support, SOS lines, legal aid. They are very experienced with the provision of these services, but new trends related to TF VAW often pose new challenges. During a focus group discussion, one debate among service providers developed on how to protect victims from TF VAW when women are placed in safe houses. Mobile phones, especially smart phones, access to internet and social media, open a channel for perpetrators to continue with violence even when women are sheltered in safe houses. Current protocols require from shelter staff to take phones from women in order to prevent continued violence. But service providers are ambivalent toward this procedure.

'[Confiscating their phones] is like punishing women. I am against that. They need to have dignity, we cannot take control over their lives. In our safe house, we do not take their phones. All networks are available to them, but we teach them how to cope with the perpetrator's attempts to contact them, how to react and how to protect themselves. If they receive threats through SMS, we invite the police, they record messages and use that in designing protection measures and in investigation.'

(Representative of CSO, Western Balkans)

Representatives of CSO service providers are aware of their insufficient capacities to counter or adequately protect from very powerful technology facilitated dimensions of violence. They are aware that new knowledge, skills, means and tools are needed, but they are not equipped with these resources. Some organizations hired international experts and organized trainings of their staff in order to increase capacities for work with TF VAW. Some activists emphasized the need to significantly shift their approaches and methods of work when they work with TF VAW. According to these opinions, it is necessary to create new alliances with IT organizations and use the same tools and digital technologies to combat digital violence.

'We can only combat this violence [TF VAW] using digital tools. We cannot combat it with tools designed for offline violence. Protocols we developed for years for referral, for police, judiciary – they are not adequate. In digital spaces, tools are developed much faster and they can be used. We need to empower women to use these tools to counter violence. The answer must be in the digital space. Prevention campaigns also have to be in the digital space and all must be digital. We do not have enough knowledge and skills for that. We need new alliances with digital communities. We need them to teach us, to advise us.'

(Representative of CSO service provider, Western Balkans)

Qualitative research uncovered other innovative practices used by organizations for the prevention and combating of offline VAW using digital tools, although these practices did not focus on technology-facilitated VAW. One example was the mobile phone game 'Spring in Bishkek' aiming at raising awareness on the harmful practice of forced marriages, known as 'kidnaping bride'. The game was installed by 150,000 users and was awarded as the best public game at the Festival 'Games for Change'. This and similar practices could inform efforts to combat TF VAW.

Türkiye: 1 million fireflies against gender-based cyber violence

As part of the 16 Days of Activism against Gender-based Violence campaign, in 2020, UN Women Türkiye organized solidarity action against gender-based cyber-violence. The aim was to collect one million fireflies to light up the dark, while raising awareness on the issue through an interactive quiz.

UN Women Türkiye launched a challenge on Instagram that directed social media users to the campaign website www.fireflies.digital, where visitors could test their knowledge on cyber-violence by completing an interactive quiz and downloading a short guide on this subject. At the end of the quiz, visitors were instructed to challenge their friends on social media and invite them to join the solidarity action. The data from the quiz fed into UN Women's programming on cyber-violence and identifying next steps in partnership with different institutions.

Orange the World 2018 – Kosovo.
Photo: © UNMIK Kosovo

6 · CONCLUSIONS AND RECOMMENDATIONS

6.1 CONCLUSIONS

In the context of significant structural gender inequalities, highly prevalent VAW, and greater backlash to gender equality, the advancement of information and communication technologies and the expansion of social space to include digital space through the internet has profoundly changed the risks and forms of VAW and posed new challenges for stakeholders engaged in preventing and responding to VAW. International, regional, and national actors are still in the early stages of addressing technology-facilitated (TF) VAW, and the countries included in this research are no exception.

As with most countries worldwide, countries in the ECA region do not have an adequate legal and policy framework to address TF VAW. Only in a few cases do key laws directly address TF VAW, at least to some extent. Legal provisions and strategic objectives either insufficiently recognize the important role of digital technologies in the perpetration of VAW or lack an understanding of the specific nature of gender-based VAW and the closely interlinked relationship between offline and TF VAW. In addition, as the implementation of laws and policies in the region is often unsatisfactory, existing legal and policy frameworks offer poor protection from TF VAW. Policies and laws often lack a gender sensitive approach towards victims, which is crucial for adequately tackling any form of VAWG, be it offline or technology-facilitated.

Global and regional efforts to address TF VAW

Global processes have intensified during the last five years, driven by concurrent processes undertaken by the UN General Assembly, Secretary-General, UNSRVAW, Commission on the Status of Women, and UN Statistical Commission to advance global norms and standards on TF VAW. Gender mainstreaming of the Cybercrime Convention adds to the number of ongoing processes related to developing legal instruments to prevent and combat TF VAW. This progress will enable further progress in the development global guidance for legal frameworks, data collection, research, statistics, and other initiatives to enhance national responses to TF VAW.

In the European region, processes are marked by various initiatives of the Council of Europe and EU. One of the crucial milestones is the effort to reaffirm the Istanbul Convention and its relevance for TF VAW in GREVIO recommendation No. 1

Prevalence and forms of TF VAW

The web-based survey conducted with over 12,000 women across the region revealed that TF VAW was experienced by more than half of adult women. The most prevalent forms of technology-facilitated violence include receiving unwanted or offensive content or messages, receiving inappropriate sexual advances or content on social networking and hacking women's account and web pages. One woman in four experienced multiple forms of violence.

A major proportion of women experienced the technology-facilitated violence only once (40.4%), but one in four women lives with such violence daily or weekly.

Virtual places of TF VAW

Facebook and Instagram are two 'virtual places' with the highest prevalence of violence against women, as every third woman who experienced TF VAW had that experience on one of these two platforms. Tik Tok and e-mail or messaging applications such as Skype, Snapchat, messenger, Viber or similar are the channels through which one on ten women with experience of TF violence was violated.

There are certain country-specific patterns in the role of specific channels: women from the Western Balkans link their experiences of violence to Facebook in higher proportions than women in other countries; women from Albania and Türkiye point more to Instagram; and women from Central Asia point more often to WhatsApp and Telegram than women from other regions.

Some virtual places are particularly toxic due to the type of communication or perhaps the sub-culture of the virtual community, as seen in communication through messaging on platforms like Snapchat, Facebook, or Instagram and in gaming communities.

Perpetrators of TF VAW

The majority of technology facilitated violence is perpetrated by unknown persons (50.3%) or persons only known on internet (17.5%). However, almost one third (32.1%) of technology facilitated violence is an extension of offline violence women experience from persons in their social proximity, such as partners, family members, friends, acquaintances, colleagues, bosses or co-students.

While unknown perpetrators and those known to women only on the internet are more inclined to commit violence in the form of hacking women's accounts or sharing offensive or other unwanted content, partners are more frequently linked to cases of threats or controlling acts. Meanwhile, family members combine controlling behavior with sexual harassment, and bosses are predominantly linked to forms of sexual harassment.

Risks and consequences of TF VAW

Risks of TF VAW are not evenly distributed among women with different socio-demographic backgrounds. Younger women are at a higher risk of TF VAW than older women. Women with education beyond primary level are at higher risk than women with primary school education, and the risk is highest for women with secondary technical training. LGBTQI women, women from larger cities, and divorced women also face higher risks of TF VAW.

Women who spend more time on the internet are at higher risk of being exposed to violence. Possession of a public profile on internet platforms, particularly more than one, and a larger number of friends and followers also increase the risk of violence.

Technology-facilitated violence against women has noticeable consequences for women's psychological wellbeing. Two-thirds of women with some experience of TF VAW reported emotional symptoms, feelings of unsafety, or embarrassment due to their exposure to the violence. One in ten women reported that the violence damaged their personal social relations with others. The consequences are more prevalent among women who were exposed to repeated violence compared to those with a one-off experience of TF VAW, except for embarrassment, which is more present among women with a single violent incident. Women who were targeted by partners suffered more from psychological consequences; women targeted by bosses felt unsafe in higher proportions, while those targeted by individuals known only on the internet felt more embarrassed.

Women who experienced any TF VAW feel more unsafe online than women without such experience. They are also more cautious in digital communication and, in higher proportions, apply various precautionary measures, such as turning off webcams, not sharing locations, using different passwords for different accounts, customizing privacy settings on platforms, and communicating only with persons they know offline. Experienced violence leads to the discouragement of women expressing themselves on the internet, and a significant proportion becomes accustomed to violent attacks. This potentially leads to increased tolerance to violence and a less proactive approach to combat it.

Survivor response to TF VAW

Women rarely report cases of violence to the police or other institutions, and even less often to non-governmental organizations. Less than half of the women report their experiences to friends or family. The reasons for this include beliefs that nothing will be done, a lack of trust in institutions, fear that confidentiality will not be respected, and fear that they will be blamed for such experiences.

Women, in large proportion, demand stronger accountability and responsibility from companies that own internet platforms and apps, more effective protection from institutions, and widespread awareness-raising to empower women to prevent, report, or counter TF VAW.

State actor perceptions and response

Qualitative research found a consensus among interviewed stakeholders that TF VAW has particularly increased after the outbreak of the COVID-19 pandemic and has become more pervasive and intense. At the same time, stakeholders are aware of their limited capacities to provide an adequate response to these new trends, and they have proposed ways to further improve legislation, policies, measures, instruments, and practices in response to TF VAW. Many of these proposals are presented in the chapter with recommendations.

Representatives of gender equality mechanisms and public institutions – such as the police, judiciary, social protection, and public service providers – are only partly informed about the diverse dimensions of TF VAW. They lack comprehensive information and statistical data on these dimensions of violence, their prevalence, characteristics, and other aspects crucial for revising laws and designing future policies. Multisectoral mechanisms are established, but they are often ineffective even for offline dimensions of VAW, for which they are mainly responsible. Meanwhile, TF VAW is mostly under the responsibility of cybercrime police. However, according to testimonies, the cybercrime police are not sufficiently equipped to effectively address the growing issue of TF VAW, and they are not integrated into the multisectoral cooperation mechanisms.

Cooperation with internet platforms where violence occurs and between stakeholders in the region or in broader international community is crucial, as TF VAW has no borders. However, the information obtained by the qualitative research reveals that cooperation is limited and there are still obstacles in identifying perpetrators and processing cases in cross-border situations.

Civil society perceptions and response

Similar to governmental stakeholders, civil society organizations, whether they are direct service providers, advocacy-oriented activists in the area of women's rights, or gender equality experts, are much more engaged in the 'traditional' areas of gender-based violence and VAW. Only a few are particularly focused on technology-facilitated violence. During focus group discussions and interviews, they often emphasized that technology-facilitated dimensions of violence are increasingly present in their work. They also described various forms of technology-facilitated violence they face in their work and highlighted categories of women who are at higher risks of being exposed to such violence. This includes women in divorce procedures, women in public positions (e.g., politicians, journalists, activists), women from ethnic minorities, young women, rural women, women living with disabilities, LGBTQI women, women with HIV, and women affected by earthquakes or war (such as refugees, IDPs, and victims of conflict-related sexual violence).

Research found very innovative approaches among CSOs that specialize in addressing TF VAW. Unfortunately, there aren't many such organizations. The majority of organizations lack knowledge and skills to engage with TF VAW, even when it comes to TF dimensions present in cases of domestic and partner violence that are the main focus of their work. As the main challenges in providing prevention or support in cases that include TF VAW, organizations reported an inadequate legal framework, lack of awareness and underreporting, problems in referrals and cooperation with public service providers, a weak role of the education sector in preventing and screening TF violence among children and young people, difficulties related to cross-border cases, and a lack of knowledge, skills, and tools to properly address TF violence in their work. As one of the conclusions, participants emphasized the need to create new alliances with IT organizations in order to develop new capacities and approaches in preventing and combating TF VAW. Some innovative solutions were discovered during the research, and these can be used as good practices that can be further replicated or inspire other organizations to transform their practices.

6.2 RECOMMENDATIONS

Based on the research findings and proposals of governmental and non-governmental stakeholders participating in the qualitative survey, as well as the suggestions and recommendations provided by UN Women offices and members of the Technical Advisory Board, sets of recommendations are proposed along six streams of action for relevant stakeholders.

IMPROVING LEGAL AND POLICY INSTRUMENTS

In consultation with relevant stakeholders, including victims of TF VAW and women's organizations, **state actors** can take a number of steps to improve legal and policy instruments, also guided by the agreed conclusions of the 67th session of the Commission on the Status of Women and processes to harmonize national legislation with the EU legal framework on TF VAW, particularly by developing, amending and/or expanding EVAW legislation and policies as per global and regional standards to cover the digital dimensions of VAW and strengthen their implementation including through victim-informed responses and fast-track processes to prevent, eliminate and respond to all forms and dimensions of TF VAWG. Strategies for preventing and combating TF VAW should be gender and age responsive, including to specifically address sexual exploitation and abuse of girls in digital contexts. Laws and policies should also ensure the responsibility of perpetrators, including in the case of transborder acts of violence, and accountability of the technology sector, including through a firmer control over digital and communication technologies and online media to prevent and address TF VAW, hate speech, gender stereotypes, and sexual abuse.

International and regional organizations also play an important role in accelerating the improvement of legal and policy instruments, particularly in advancing and promoting international and regional frameworks on TF VAW, producing guidance on states' alignment with such frameworks, and ensuring that relevant frameworks under preparation, such as the UNODC-led International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, are gender-sensitive and sufficiently address TF VAW. Furthermore, EU institutions should leverage EU accession processes to encourage and support EU candidates and potential candidate countries to align national legislation with the EU legal framework related to TF VAW.

The technology sector, including social media, online gaming and IT companies, should closely monitor the development of the international and national legal frameworks for protection from TF VAW and align their 'community guidelines' to international norms.

IMPROVING MULTISTAKEHOLDER COORDINATION ON TF VAW

At national level, all stakeholders, including state and civil society actors as well as technology companies, must strengthen their cooperation and coordination in order to achieve a robust multisectoral approach to prevent and respond to TF VAW.

At international level, all stakeholders, with an emphasis on **state actors**, should enact, support and advocate for the following:

- There is a need to ensure more effective cooperation among national police forces. This collaboration should allow victims to report violence to the police in their own countries rather than in perpetrators' countries.
- Exchanges of knowledge are essential, learning from countries with more advanced systems for addressing TF VAW.
- Regional exchange between gender equality mechanisms can contribute to more coordinated efforts to improve cross border cooperation in cases of TF VAW that include perpetrators and victims from different countries.

International coalitions and networks such as the multistakeholder Generation Equality Action Coalitions on Technology and Innovation for Gender Equality and on Gender-Based Violence which share TF VAW as a common priority and the Global Partnership for Action on Gender-Based Online Harassment and Abuse can leverage their commitments and goals to accelerate progress towards ending TF VAW and engaging more State and non-State partners to participate in these global efforts.

CONDUCTING WHOLE OF-SOCIETY PREVENTION STRATEGIES

All stakeholders, state and non-state, should:

- Raise awareness among all professionals, including the police, prosecution, judiciary, social protection, and education sectors about the magnitude, manifestations, consequences of TF VAW, so they can understand that TF VAW requires equal attention as other dimensions and forms of VAW;
- Encourage a more proactive role of the education system in raising awareness among students and teachers about TF VAW. Utilize existing or create new school-level mechanisms to address technology facilitated violence among students;
- Prioritize digital literacy and knowledge on the nature and forms of TF VAW and how to protect personal security while using digital and communication technologies, also reflected in national gender equality policies and programmes;
- Educate men and boys on the forms, dimensions, severity and consequences of TF VAW, with a particular focus on the forms and dimensions that may already be normalized or are at risk of being normalized, as well as more generally on equitable masculinities and non-violent communication.

The **technology sector** has an important role to play, by its outreach, to contribute to prevention efforts to change social norms and attitudes and should develop educational resources to raise awareness on TF VAW and the importance of nonviolent and safe communication and use of technologies.

Media outlets also play a role in shaping public opinion and perception of TF VAW:

- Journalists and members of the media should improve their awareness and understanding of TF VAW, and journalistic standards and codes should be revised to include ethical considerations related to TF VAW;
- The media should raise awareness about TF VAW and accurately report on cases of TF VAW rather than minimizing or romanticizing the actions and their impact on victims.

IMPROVING MULTISECTORAL RESPONSE TO TF VAW

State actors should consider several recommendations to strengthen the multisectoral response to TF VAW:

- Specialized and generalized services should address TF VAW. This necessitates the revision of protocols for multisectoral cooperation and the development of capacities for professionals from all sectors involved in EVAW;
- In countries where cybercrime police are mandated with investigating TF VAW, they should be more systematically integrated into multisectoral mechanisms, and their roles in responding to TF VAW should be defined more clearly in bylaws or protocols;
- Response services and interventions focused on protection of women and girls from gender-based violence should include women and girls in their design, apply a victim centered approach and be accompanied by guidelines for data protection, with a focus on meeting the needs of particularly vulnerable women, such as women living in rural and remote areas, women with disabilities, women affected by conflict, refugee and displaced women, women from minority groups;
- Specific protection mechanisms should be developed to protect women in the public eye, including women

activists and civil society actors engaged in support services to VAW survivors as they are more often exposed to TF VAW. Their protection is crucial for creating a safe and enabling environment in which they can provide support to women and contribute to their empowerment.

Civil society organizations should expand their services to cover dimensions and forms of TF VAW as well as strengthen cooperation and coordination among CSOs to more effectively and cohesively counter TF VAW.

The technology sector should proactively, promptly and effectively monitor and remove hate speech, sexist and misogynistic content and incidents of TF VAW, including by improving response to platform-based reporting mechanisms, as this has far-reaching consequences that victimize the broader community in addition to the direct victims. They should also enhance their cooperation with law enforcement to improve response time to cases of TF VAW and more rapidly lock or remove offenders' accounts.

EMPOWERING CSOS AND WOMEN'S RIGHTS ORGANIZATIONS

State actors, as well as **international and regional organizations**, should empower CSOs and women's rights organizations to effectively address TF VAW:

- Support CSOs to strengthen their capacities to fully understand and provide services related to TF VAW;
- Include CSOs as key partners in the development of programmes, policies and legislation related to TF VAW;
- Ensure sustainable funding for CSOs service providers, outside of project-based funding.

IMPROVING DATA AND EVIDENCE

International and regional organizations are well positioned to lead the way on improving data collection on TF VAW:

- Global standards and guidance are needed on the collection of data on TF VAW. The work of the UN Statistical Commission, supported by UN Women and its sister agencies, and in consultation with National Statistics Offices and other relevant stakeholders, should in the coming years offer tools to do so, that are responsive to regional and sub-regional specificities;
- Statistical surveys on VAW should encompass technology-facilitated dimensions. In the European region, learnings from methodologies to collect survey and administrative data on TF VAW developed by Eurostat, EIGE and FRA should feed and inform further regional and global methodological developments in this area;

State actors should also expand their practices:

- Administrative data systems on VAW should be strengthened, better coordinated and include dimensions related to TF VAW. Administrative data reports should be regularly shared and should clearly present (anonymized) findings;
- Fund and produce research on TF VAW that not only covers interpersonal violence but also sexist, misogynistic hate speech on social media, providing an evidence base for designing campaigns that counter such behaviour;
- Monitor the proportion of funds from public budgets or international aid allocated to prevention and combating VAW, specifically TF forms and dimensions.

Finally, **civil society organizations** that provide services to victims of VAW should develop and improve their internal collection of administrative service data to screen for and document incidents of TF VAW.

REFERENCES

Adriane van der Wilk (2021) *Protecting Women and Girls from Violence in the Digital Age. The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women*, Council of Europe

CEDAW (2017) *General recommendation No. 36 on the right of girls and women to education*

Council of Europe, *The Budapest Convention and its Protocols*

EIGE (2022*) Combating Cyber Violence against Women and Girls*

GREVIO *General Recommendation No. 1 on digital dimension of violence against women*, Council of Europe

Massey, D. (1994) *Space, place, and gender*. Minneapolis: University of Minnesota Press.

OSCE (2019) *OSCE-led survey on violence against women. Wellbeing and safety of women. Main report.*

Sandberg, L (2011). Fear of violence and gendered power relations. Responses to threats in public space in Sweden. Umea: Gerum.

UN Economic and Social Council, Commission on the Status of Women, Sixty-seventh session (2023) *Innovation and technological change, and education in the digital age for achieving gender equality*

UN General Assembly (2020-2021*) The right to privacy in the digital age: resolution / adopted by the General Assembly*

UN General Assembly (2020-2021*) Intensification of efforts to prevent and eliminate all forms of violence against women and girls: resolution / adopted by the General Assembly*

UN General Assembly (2013-2014*) Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms: protecting women human rights defenders : resolution / adopted by the General Assembly*

UN Human Rights Council (2021) *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*

UN Human Rights Council (2018) *Report of the Special Rapporteur on the right to privacy*

UN Human Rights Council (2018) *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective.* Thirty-eight session

UN Women (2022) Technology-facilitated Violence against Women: Towards a common definition. Report of the meeting of the Expert Group 15-16 November 2022, New York, USA

UN Women, WHO (2022) Foundational Expert Group Meeting (EGM) on Online and technology-facilitated violence against women and girls: Towards a common definition. Background Note. New York, USA, 15-16 November 2022.

Zarizana Abdul Aziz (2023) Due Diligence and Accountability for Online Violence against Women.

ANNEX 1: RESEARCH METHODOLOGY

Mapping of normative and policy frameworks and processes

At the global level, focus was placed on UN Women-initiated processes as well key conventions such as CEDAW and the Cybercrime Convention currently in development.

At the regional level, the mapping included the Istanbul Convention and other relevant strategies and normative documents of the Council of Europe, as well as relevant documents of the European Union as they may impact future developments in the ECA region through EU Enlargement and EU Neighborhood policy.

At the national level, the mapping included an overview of:

- Criminal codes
- Specific laws addressing gender equality, GBV, VAW and/or domestic violence
- National strategies/action plans for gender equality
- National strategies/action plans specifically addressing GBV, VAW and/or domestic violence
- Laws and strategies specifically focused on cybercrime (if and where they exist)

Table 2: List of reviewed documents

Global level	
1.	CEDAW, General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19.
2.	UN Economic and Social Council, Commission on the Status of Women, Sixty-seventh session (2023) *Innovation and technological change, and education in the digital age for achieving gender equality*
3.	UN General Assembly (2020-2021*) Intensification of efforts to prevent and eliminate all forms of violence against women and girls: resolution / adopted by the General Assembly*
4.	UN General Assembly (2013-2014*) Promotion of the Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms: protecting women human rights defenders : resolution / adopted by the General Assembly*
5.	UN Human Rights Council (2021) *Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression*
6.	UN Human Rights Council (2018) *Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective.* Thirty-eight session
7.	UN Human Rights Council (2018) *Report of the Special Rapporteur on the right to privacy*
8.	UN Women, *Accelerating efforts to tackle online and technology facilitated violence against women and girls (VAWG). Summary*
9.	UN Women (2022) *Safe consultations with survivors of violence against women and girls*
10.	UN Women, Violence against women in the online space. Insights from a multi-country study in the Arab States. Summary report.
11.	UN Women, WHO (2023) *Technology-facilitated violence against women: taking stock of evidence and data collection*
12.	UN Women (2022) Stepping Up Action to Prevent and Respond to Online and ICT-Facilitated Violence against Women and Girls. Observer paper prepared by UN Women.
13.	Un Women, WHO, The state of evidence and data collection on technology-facilitated violence against women (2023), https://www.unwomen.org/en/digital-library/publications/2023/04/brief-the-state-of-evidence-and-data-collection-on-technology-facilitated-violence-against-women
14.	WHO (2016) *ethical and safety recommendations for intervention research on violence against women*
Regional level	
15.	Council of Europe (2021) *Protecting women and girls from violence in the digital age. The relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in addressing online and technology-facilitated violence against women*
16.	EIGE, Combating Cyber Violence against Women and Girls, 2022. https://eige.europa.eu/publications-resources/publications/combating-cyber-violence-against-women-and-girls?language_content_entity=en
17.	GREVIO General Recommendation No. 1 on digital dimension of violence against women. Adopted on 20 October 2021.

National level	
Albania	
18.	Kodi Penal Republikës së Shqipërisë
19.	Law on Measures Against Violence in Family Relations
20.	National Strategy on Gender Equality 2021-2030
Bosnia and Herzegovina	
21.	Criminal Code of BiH
22.	Gender Equality Law in BiH
23.	Criminal Code of Federation of BiH
24.	Law on protection from domestic violence
25.	Criminal Code of Republika Srpska
26.	Law on protection from domestic violence in Republika Srpska
Georgia	
27.	Criminal Code of Georgia
28.	Law of Georgia on Combating Violence against Women/Domestic Violence and Protection of Victims of Violence
29.	State Gender Equality Concept
30.	National Action Plan on Combating Violence against Women and Domestic Violence and Measures to be Implemented for the Protection of Victims (Survivors) for 2022-2024
Kazakhstan	
31.	Criminal Code of the Republic of Kazakhstan
32.	Law on State Guarantees of Equal Rights and Equal Opportunities for Men and Women
33.	Law on prevention of domestic violence
Kosovo	
34.	Criminal Code of the Republic of Kosovo
35.	Law for protection from domestic violence
36.	The Kosovo Programme for Gender Equality 2020-2024
37.	National Strategy for protection from domestic violence and violence against women 2022-2026
Kyrgyzstan	
38.	The Kyrgyz Republic Criminal Code
39.	Law on State Guarantees of Equal Rights and Equal Opportunities for Men and Women
40.	Law on the Safeguarding and Protection from Domestic Violence
Moldova	
41.	Criminal Code of the Republic Moldova
42.	Law on prevention and combating domestic violence
43.	New national program for accelerating gender equality in Republic of Moldova for the years 2023-2027
44.	National Gender Equality Strategy 2030
Montenegro	
45.	Criminal Code of Montenegro
46.	Law on protection from domestic violence
47.	National strategy for gender equality 2021-2025 with Action Plan 2021-2022

North Macedonia	
48.	Criminal Code of the Republic of North Macedonia
49.	Law on prevention of violence against women and domestic violence
50.	Gender Equality Strategy 2022-2027
Serbia	
51.	Criminal Code of the Republic of Serbia
52.	Law on prevention of domestic violence
53.	Gender Equality Strategy 2021-2030
54.	Action plan for 2022-2023
55.	Strategy for prevention and combating gender based violence against women and domestic violence 2021-2025
56.	Law on organization and responsibilities in combating cyber crime
Tajikistan	
57.	Criminal Code of the Republic of Tajikistan
58.	Law on prevention of domestic violence
59.	National Strategy for enhancing the role of women in the Republic of Tajikistan for 2021-2030
60.	State Programme of Republic of Tajikistan on Prevention of violence in the family for 2014-2023 and its Action Plan
Türkiye	
61.	Criminal Code of Türkiye
62.	Law to Protect Family and Prevent Violence against Woman
63.	National Strategy and Action Plan on Women's Empowerment (2018-2023)
64.	National Action Plan on Combatting Violence against Women (2021-2025)
Ukraine	
65.	Criminal Code of the Republic of Ukraine
66.	Law on preventing and combating domestic violence

Web-based survey

The web survey was implemented by applying RIWI technology which allows for the rapid capture and assessment of large samples of broad, truly randomized opinion and perceptions data on an ongoing basis. Basically, methodology is based on reaching people who are surfing online through web-intercept recruitment**.** Survey participants are accessed on all Web-enabled devices. To access the content, they are not asked to sign up or download any apps or tools. Recruitment takes place directly on respondents' devices within the environments they spend most of their time.

Methodology operates using a rotating roster of thousands of survey entry points to ensure highly diverse set of respondents and prevent duplicate respondents. Web intercept can be employed in highly sensitive environments with high-security protocols to ensure the complete anonymity of respondents and clients. The procedure is to geo-target respondents automatically by country, region, state, and city, and present a language-appropriate survey. Survey data are delivered on an interactive Dashboard, through which variables of interest can be analyzed, together with hourly updated results in SPSS and Excel. No personally identifiable information is collected, stored, or transferred.

In addition to observations from the survey questionnaire, the agency which implemented survey also provided the following information generated automatically for all respondents: date of access, time in Pacific time (PT), time in UTC, type of device used to answer the survey, operational system, operational system version, city, region, region code, country, and number of answers. Respondents could exit the survey at any time. No information was collected from people who chose not to participate in the survey.

Respondent category	Survey is considered to be completed at…
Women who reported having experienced technology-facilitated violence	Respondent is considered to have completed the survey if they answered a module of 30 questions. 10 questions are specific to respondents who have experienced online violence.
Women who did not report having experienced technology-facilitated violence	Respondent is considered to have completed the survey if they answered a module of 20 questions.

NON-INCENTIVIZED RECRUITMENT

Dormant Domains

- As people are using the web, there is the chance of them coming across a dormant domain through incorrect URLs, web browser searches, redirection outside of apps to sites that no longer exist, etc.
- Instead of encountering a "page does not exist" notification or an ad, RIWI can render your content, survey, or redirect them to other content. Web users then decide whether they would like to anonymously participate in the research, and do so without incentivization.
- This method is non-incentivized, so many measures and strategies are introduced to engage and retain online participants when RIWI is hosting the survey, including optimizing the survey instrument for ease of participation on all device screens and bandwidths, as well as clear, concise language for immediate comprehension at a wide range of literacy or education levels.

INCENTIVIZED RECRUITMENT

Apps and Active Websites

- Web users can also be intercepted on active apps or websites by co-opting spaces where advertisements may have been, or by being an activity instead of payment for in-app purchases.
- Incentives differ, but will often be coupons, charity donations, discount codes, gift cards, paid application downloads, vouchers, in-app currency, or access to something that would otherwise cost money. Neither UN Women nor RIWI directly controls the incentivization process.
- An example would be a user trying to access a news article that typically requires payment, but randomly being given the opportunity to fill out a RIWI survey in exchange for getting past the newspaper's paywall. If they choose to opt-in and complete the survey, they are given free access to the article.

Rates of experience of online violence by recruitment mechanism

Column % Count	Non-incentivized	Incentivized
Women who reported having experienced online violence	34%	61%
	1,194	5,468
Women who did not report having experienced online violence	66%	39%
	2,324	3,540

STRENGTHS, LIMITATIONS AND USE CASES

Web-intercept methodology achieves a diverse sample of respondents and can be done so without capturing personally identifiable information. As such, it's well suited for studies looking at widespread sentiment topics. The anonymity of respondents makes it possible to ask extremely sensitive questions, garner honest responses, and maintain the respondent's safety. However, where no identifiable information is known about a respondent, it is not possible to follow up with a respondent later on. Due to the scale of internet users, and the ability to sample the entire internet-using population of a country, it is possible to achieve very large samples in a short amount of time and engage large samples of previously unengaged voices.

As an internet-based technology, it cannot reach someone who has no access to the internet which, depending on the internet penetration rate, can create sampling biases that need to be identified and analyzed. However, because we do not recruit respondents based on their participation in a gated group (e.g. an app or password-protected website), even if someone does not personally own a device, if they are surfing online (e.g. through a web cafe or library), they still have a chance of coming across one of our entry points.

Population of internet users for the 12 countries under study

Country	Latest Year	All Individuals	Gender		Urban			Rural		
			Male	Female	Total	Male	Female	Total	Male	Female
		%								
Albania	2021	79. 3	80.3	78.3	...	...	...	...	...	...
Bosnia and Herzegovina	2021	75.7	79.2	72.7	78.9	84.4	74.4	73.3	75.5	71.3
Georgia	2021	76.4	76.8	76.1	83.2	83.7	82.8	66.4	67.5	65.3
Kosovo	2018	89.4	89.9	89	...	...	...	...	...	...
Moldova	2021	61.29	...	...	...	...	...	...	...	...
North Macedonia	2021	83.02	...	...	...	...	...	...	...	...
Serbia	2021	81.2	83.6	78.8	84.5	87.6	81.6	77.2	78.8	75.6
Turkiye (Completed)	2021	81.4	86.5	76.4						
Kazakhstan	2021	90.9	91.9	90	92.3	93.3	91.4	89	90	87.9
Kyrgyzstan	2021	77.92	...	...	...	...	...	...	...	...
Ukraine	2021	79.2	82	76.8	83.4	86.2	81	70.9	73.8	68.3
Tajikistan	2016	21.96	...	...	...	...	...	...	...	...

Note: Internet usage information comes from ITU latest statistics. (https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx)

RISK MANAGEMENT AND DATA QUALITY CHECKS

There were several risk management and data quality measures throughout the project lifecycle, which include:

I. **Continuous bot-filtering and anomaly detection** (e.g., straight-lining detection) are used to ensure answers are authentic human responses.

II. **Points of entry rotate regularly**, ensuring that respondents are unique and have not previously completed the survey or message test.

III. **Potential users' legitimacy is verified prior to study participation** through suspicious traffic filtration. Fraudulent participants are also blocked and removed through digital fingerprinting (e.g., IP address checks), behaviour analysis, and deduplication.

IV. **RIWI has significant experience developing and launching anonymous digital polling to safely reach users globally**. All data captured, acquired, used, published, or disseminated by RIWI technology and systems, or data released by RIWI, are fully compliant with all applicable laws and privacy rules, including the General Data Protection Regulation (GDPR).

V. **RIWI employs strategic security measures at all levels of the survey design, respondent experience, and data storage.** Security measures are specific to the topic and region of deployment, as well as the recognized security risk, and can be adjusted as new information and geopolitical developments unfold.

VI. **No response is traceable to an individual.** RIWI has taken physical and digital measures to protect the identity of the respondent.

Specific security measures include:

- RIWI surveys are hosted on real, registered, non-trademarked domain sites that contain **no malware and respondents are not contacted in any way via hackable links or insecure email.** No response is traceable to an individual. Since survey links are not emailed, as is the case with most panel survey solution companies, it is not possible to hack into respondent emails.
- In the unlikely event RIWI Web servers are breached, RIWI has taken physical and digital measures to protect the identity of the respondent (i.e., survey visitor). By disabling cookies, access logs and optionally destroying Web servers after three days (or fewer) in the field, RIWI can eliminate evidence the respondent has visited our Web servers.
- RIWI's platform cannot be blocked, censored, monitored, or tracked. In the event of one of the entry-points that RIWI redirects users is shut down or blocked due to government monitoring and censorship, RIWI is able to circumvent these restrictions by rotating points of entry rotate regularly. **There is no one source to block or shut down.**

PROJECT SPECIFICATIONS

Data collection took place between January 30th, 2023 and June 24th, 2023. 12,527 **women** completed surveys were collected in total, throughout **Albania, Bosnia and Herzegovina, Georgia, Kazakhstan, Kyrgyzstan, Kosovo,**

Moldova, North Macedonia, Serbia, Tajikistan, Türkiye, and Ukraine, with at least 1,000 completed surveys collected in each country. The survey only included women aged at least 18 years old, and it was offered in various languages, according to each country: Albanian, Georgian, Kazakh, Kyrgyz, Macedonian, Romanian, Russian, Serbian, Ukrainian, Tajik, and Turkish.

The survey was made up of 22 questions for all respondents, and up to 34 questions depending on the skip logic and country. The survey modules are attached in Appendix B. Respondents were first asked about their online activity – if they have public profiles, the number of hours they usually spend online, and which platforms they use the most, among others. Then they were asked about their experience and perceptions of technology-facilitated VAW. Respondents that indicated they had experienced TF VAW were taken through a path that asked them about this experience and its ramifications on their life. They were asked about the type(s) of experience(s) they had, their impact, and their reporting behaviours, including whether they have sought support, from whom, and why some respondents decided not to. Lastly, all respondents were asked to express what they think should be the best approach to combat TF VAW and to complement their responses with some demographic information. At the end of the survey, respondents saw a language-appropriate message with support resources for women who reported having experienced TF VAW, including an email address and telephone number for contact.

RETENTION RATES

The survey had an average retention rate of 17.26%, with 77,567 respondents answering the first question about their age and gender, and 12,527 respondents completing the entire survey. Retention rates vary depending on the employment of incentivized recruitment as described in the Methodology section.

Country	AL	BA	GE	KG	KZ	MD	MK	RS	TJ	TR	UA	XK	TOTAL
Respondents	5982	19416	9042	4456	2928	3650	3885	4121	3436	1208	1114	13329	**72567**
Completed surveys	1000	1106	1002	1006	1011	1001	1006	1200	1008	1180	1000	1007	**12,527**
Retention rates	16.72%	5.70%	11.08%	22.58%	34.53%	27.42%	25.89%	29.12%	29.33%	97.68%	89.77%	7.55%	**17.26%**

Qualitative research

Table 3: List of participants in interviews and FGDs

	FGDs and interviews with CSOs	FGD and interviews with state institutions engaged in response to VAW	National GE mechanism	HR institution
Albania	9	4	1	1
BiH	6	3	1	1
Georgia	3	4	1	1
Kazakhstan	4	1	-	-
Kosovo	4	1	1	-
Kyrgyzstan	3	1	-	-
Moldova	8	2	-	1
Montenegro	4	-	-	-
North Macedonia	4	2	-	-
Serbia	4	-	1	1
Tajikistan	1	-	-	-
Türkiye	3	1	-	-
Ukraine	4	1	-	-
Total	**57**	**20**	**5**	**5**

ANNEX 2: STATISTICAL ANNEX

Table 4: Women who experienced any online and technology facilitated violence by type of violence and country (%) (N=6662)

Type of violence	Regional average	AL	BA	GE	KG	KZ	MD	MK	RS	TJ	TR	UA	XK
Received inappropriate sexual advances or content	30.0	27.7	39.6	28.9	17.5	18.9	34.2	38.6	42.6	12.0	24.1	35.7	20.0
Been pressured to share sexually explicit images or messages	9.3	9.7	10.7	10.7	5.2	6.2	8.5	3.8	9.6	6.1	17.9	8.5	8.7
Being threatened that personal information will be revealed without consent	11.3	7.8	10.7	11.5	9.2	11.0	9.6	10.0	10.6	9.1	18.9	10.5	11.7
Private information was revealed without consent	11.2	10.5	9.1	8.3	9.4	12.9	12.4	10.0	10.3	9.7	15.2	10.7	13.8
Received unwanted or offensive content or messages	39.7	34.3	57.2	31.4	22.9	29.4	45.0	45.9	57.4	19.1	41.8	38.8	26.1
Someone monitored phone calls, messages	11.8	9.0	7.6	13.2	13.4	13.8	11.0	12.8	7.2	19.7	15.6	11.8	8.3
Someone monitored location	9.4	9.7	7.8	10.9	9.2	8.7	10.2	7.4	8.2	9.1	13.2	7.0	10.3
Private accounts and web pages were hacked	25.4	25.5	24.9	30.8	19.6	29.4	30.7	28.2	22.9	11.3	16.2	35.5	22.7
Received threats	10.7	8.3	11.5	10.7	8.0	8.0	12.1	8.1	11.8	9.1	15.7	9.5	11.0
Photos manipulated, electronic defamation	11.3	15.3	12.8	10.5	6.6	9.2	9.9	8.7	11.5	9.1	15.8	8.2	16.3
Other	9.7	7.3	6.2	13.4	28.5	17.0	6.6	5.5	4.3	31.7	2.3	4.8	12.8

Table 5: Women who experienced any online and technology facilitated violence by communication channel through which violence occurred (in case of multiple acts of violence, the most recent one) (%) (N=6662)

Platform/tool	Regional average	AL	BA	GE	KG	KZ	MD	MK	RS	TJ	TR	UA	XK
E-mail or messaging applications (Skype, Snapchat, Messenger, Viber, etc.)	10.6	7.8	13.1	8.7	5.2	7.4	15.4	12.8	11.5	5.5	7.4	15.2	10.1
Facebook	36.3	30.5	62.3	51.0	11.1	7.6	37.3	68.6	55.8	12.3	24.1	26.8	23.2
Instagram	33.8	48.0	35.9	19.8	32.2	37.5	32.1	23.0	33.0	31.7	45.8	30.5	35.1
Knowledge sharing platforms	2.0	2.2	0.7	3.4	1.4	1.4	0.9	1.6	0.7	1.6	4.6	1.6	2.5
LinkedIn	2.0	2.2	0.4	3.2	0.7	0.7	0.9	1.3	1.5	1.6	5.6	1.3	2.5
Online dating platforms (Tinder, Bumble, OK Cupid, etc.)	4.9	1.7	2.8	5.5	4.0	2.5	5.4	4.1	4.2	2.6	7.7	6.5	7.1
Online gaming	6.5	3.4	2.7	6.5	7.3	8.3	4.6	2.5	2.8	4.5	13.5	9.8	8.5
Online news sources or blogs	3.4	2.2	1.4	5.1	4.5	3.2	2.4	2.4	2.1	1.6	5.4	4.6	4.1
Telegram	8.2	2.2	2.1	5.3	14.4	14.0	9.3	1.3	1.9	14.9	7.4	20.7	6.0
TikTok	10.9	15.9	4.8	10.5	13.2	16.3	8.3	4.9	5.1	8.1	18.1	10.0	18.6
Twitter	4.1	2.2	2.3	3.2	2.1	2.8	1.5	2.2	4.8	1.3	12.3	2.6	7.3
Virtual meeting tools (Skype, Zoom, Google Meet, Microsoft Teams, etc.)	3.2	1.7	1.4	4.2	4.3	3.0	2.9	1.9	1.8	1.9	5.2	4.2	4.8
WhatsApp	9.4	9.3	3.6	4.9	26.0	21.4	6.1	2.9	3.6	32.4	12.2	2.2	8.9
YouTube	7.4	4.6	3.7	8.1	7.8	7.8	4.1	3.5	4.2	12.9	17.6	4.2	10.3
BeReal	1.5	2.2	0.7	3.0	1.4	1.8	1.4	0.8	0.4	0.6	3.2	1.2	1.4
Other	7.3	4.4	4.6	9.1	19.4	13.3	11.3	4.1	3.6	12.3	1.4	7.6	4.8

Table 6: Perpetrators by type of violence (multiple options) (%) (N=6662) (marked categories with highest proportion for type of violence)

Type of violence	Partner (current or former)	Family member	Friends, co-students, neighbors	Supervisor, boss	Someone known only online	Unknown
Received inappropriate sexual advances or content	26.5	23.7	21.9	22.4	40.9	33.9
Been pressured to share sexually explicit images or messages	15.2	14.4	12.8	17.2	12.9	6.0
Being threatened that personal information will be revealed without consent	20.9	17.2	17.8	20.1	11.6	7.6
Private information was revealed without consent	18.4	17.2	15.7	22.4	10.9	8.7
Received unwanted or offensive content or messages	30.0	24.2	29.9	25.4	53.2	47.1
Someone monitored phone calls, messages	23.8	24.2	17.4	19.4	10.8	7.6
Someone monitored location	15.7	14.4	14.7	20.1	8.7	6.9
Private accounts and web pages were hacked	24.4	17.2	21.5	20.9	22.6	31.8
Received threats	15.3	13.0	14.4	11.2	14.6	8.3
Photos manipulated, electronic defamation	16.5	22.3	18.0	15.7	12.3	8.1

Table 7: Perpetrators by proportion of platform/application through which violence was committed (multiple options) (% of cases) (N=6662)

Platform/tool	Partner (current or former)	Family member	Friends, co-students, neighbors	Supervisor, boss	Someone known only online	Unknown
E-mail, messaging applications	12.7	9.9	8.1	14.6	12.0	11.1
Facebook	32.8	30.0	26.9	20.4	45.7	41.4
Instagram	34.5	28.7	33.1	25.5	35.1	37.7
Knowledge platforms	4.2	4.5	3.8	8.0	1.4	0.8
LinkedIn	3.8	2.7	4.9	10.2	0.6	1.0
Dating platforms	6.8	6.7	5.3	12.4	7.0	3.5
Online gaming	8.8	11.2	9.2	10.2	8.3	4.8
News sources or blogs	5.3	5.8	5.3	8.0	2.0	2.8
Telegram	11.1	13.0	13.3	13.9	8.9	6.1
TikTok	15.2	23.3	19.1	19.7	9.6	8.0
Twitter	7.0	5.4	5.0	7.3	4.6	3.2
Meeting tools	6.0	8.1	5.3	5.8	2.4	2.0
WhatsApp	15.9	20.6	15.0	16.1	7.6	6.8
YouTube	10.7	22.4	13.4	20.4	5.6	4.7
BeReal	2.8	4.0	5.0	5.1	0.5	0.5

Figure 26: Platforms on which women have experienced violence by type of perpetrators (%) (N=6662)

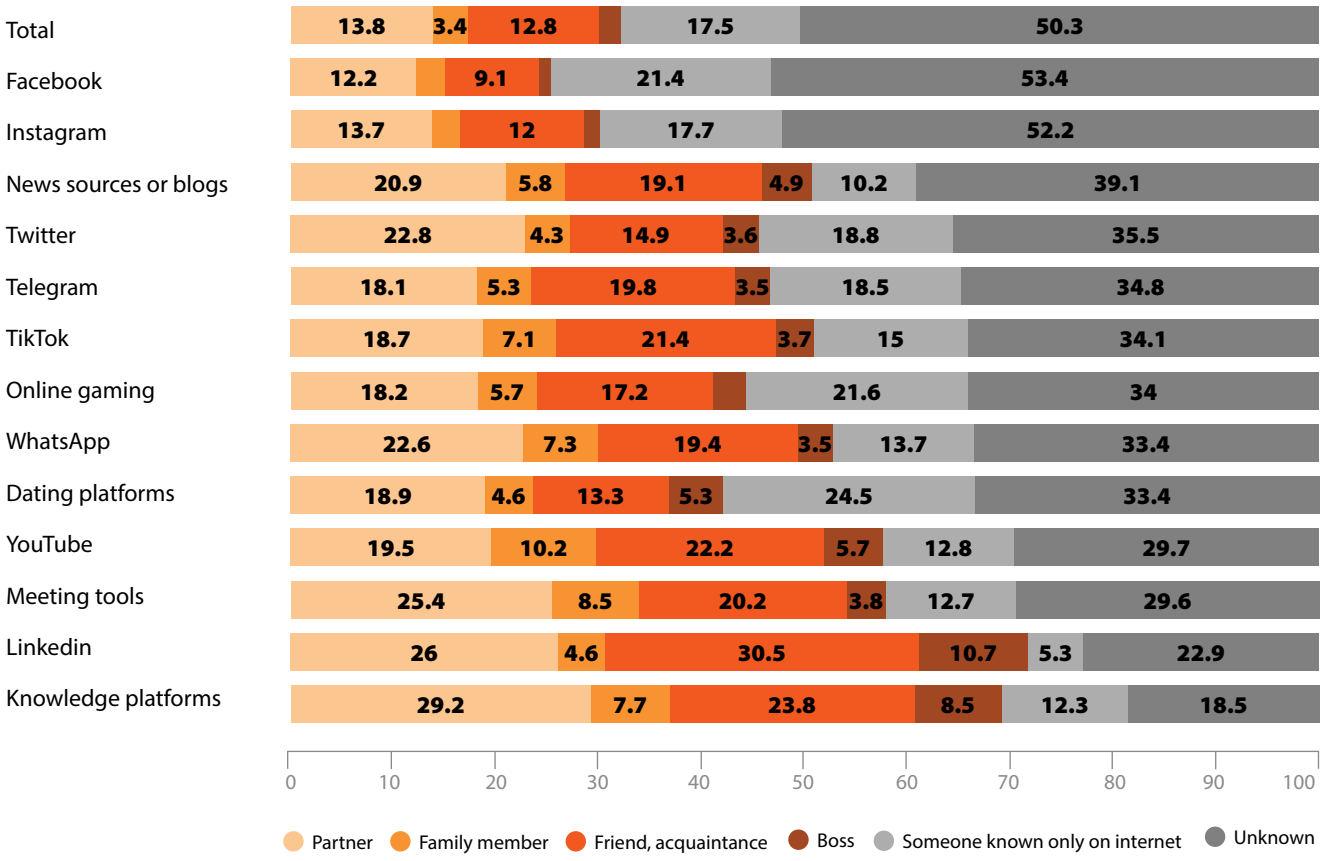


Table 8: Women who experienced violence by perpetrators and frequency of violent acts (%) (N=6662)

Frequency of violence	Spouse	Boyfriend, girlfriend, fiancé	Former partner	Family member	Friends, co-students, neighbors	Supervisor, boss	Someone known only online	Unknown
Daily	15.4	17.3	14.9	23.6	15.3	19.3	4.1	2.7
Weekly	7.7	9.3	9.7	10.0	10.0	11.4	8.0	3.8
Monthly	15.4	11.4	11.3	14.4	12.1	19.3	12.4	7.5
Every 6 months	12.6	12.5	11.5	10.0	9.5	16.4	15.0	11.5
Only once	29.1	28.7	28.5	24.9	34.7	20.7	42.0	47.1
Do not know	19.8	20.8	24.1	17.0	18.4	12.9	18.4	27.4
Total	100	100	100	100	100	100	100	100

Table 9: Women who experienced violence by consequences and country (%) (N=6662)

Consequences of violence	Regional average	AL	BA	GE	KG	KZ	MD	MK	RS	TJ	TR	UA	XK
Psychological consequences	19.2	23.4	20.8	14.4	15.6	18.6	14.2	24.1	15.2	11.4	27.2	19.7	18.8
Felt unsafe	19.3	27.1	18.8	15.6	12.3	15.4	14.4	24.2	21.2	11.0	22.0	23.2	17.9
Felt embarrassed	27.3	17.6	23.3	34.8	26.2	24.6	42.2	21.1	23.6	29.9	26.9	27.6	28.0
Caused harm to relationships	10.6	9.8	11.7	8.7	10.4	12.2	7.6	8.7	9.9	8.8	14.9	10.3	12.2
Other	23.6	22.2	25.4	26.5	35.5	29.2	21.6	21.9	30.0	39.0	9.0	19.3	23.2
Total	100	100	100	100	100	100	100	100	100	100	100	100	100

Table 10: Women who experienced violence by consequences and sub-region (%) (N=6662)

Type of Consequences	Regional average	Western Balkans	Türkiye	Eastern Partnership	Central Asia
Psychological consequences	19.2	23.4	20.8	14.4	15.6
Felt unsafe	19.3	27.1	18.8	15.6	12.3
Felt embarrassed	27.3	17.6	23.3	34.8	26.2
Caused harm to relationships	10.6	9.8	11.7	8.7	10.4
Other	23.6	22.1	25.4	26.5	35.5
Total	100	100	100	100	100

Binary logistic regression models

Model 1: Women's background characteristics as risk factors

Variables in the Equation[a]					
Dependent variable: TF VAW experience (0=no experience, 1= experience)					
	B	**Sig.**	**Exp(B)**	**95% C.I.for EXP(B)**	
				Lower	**Upper**
Civil_status (**refer. single**)		**.000**			
Civil status – married	-.077	.166	.926	.831	1.032
Civil status – divorced	.323	**.000**	1.381	1.171	1.628
Civil status – widowed	-.069	.577	.934	.734	1.188
Current employment status (**refer. employed for wages**)		.862			
Current employment status – **self employed**)	-.033	.645	.968	.842	1.112
Current employment status – **unemployed**	-.081	.195	.922	.816	1.042
Current employment status – **student**	-.058	.431	.944	.817	1.090
Current employment status – **retired**	-.063	.663	.939	.707	1.247
Current employment status – **not able to work**	-.041	.750	.960	.746	1.234
Education (**refer. primary**)		**.001**			
Education – **secondary school**	.346	**.001**	1.414	1.152	1.736
Education – **technical vocational training**	.508	**.000**	1.661	1.328	2.079
Education – **university college**	.331	**.001**	1.393	1.141	1.700
Education – **postgraduate**	.323	**.009**	1.381	1.084	1.759
Sexual orientation (**refer. heterosexual**)		**.000**			
Sexual orientation – **asexual**	.217	.122	1.242	.944	1.635
Sexual orientation – **bisexual**	.505	**.000**	1.657	1.333	2.061
Sexual orientation – **lesbian**	-.148	.277	.863	.661	1.126
Sexual orientation – **gay**	-.313	**.042**	.732	.541	.989
Sexual orientation – **pansexual**	.383	**.020**	1.466	1.061	2.025
Sexual orientation – **prefer not to answer**	-.694	**.000**	.499	.454	.549
Living place (refer. locality less 30k)		**.000**			
Living place – big city 500k	.204	**.001**	1.226	1.092	1.378
Living place – locality 100k – 500k	.227	**.001**	1.255	1.092	1.442
Living place – locality 30k – 100k	.379	**.000**	1.461	1.269	1.683
Age – refer 65+		**.000**			
Age_(- 24)	1.415	**.000**	4.115	3.187	5.315
Age (25-44)	1.215	**.000**	3.371	2.621	4.336
age_(45-64)	.800	**.000**	2.227	1.717	2.887
Constant	-1.066	**.000**	.344		
Cox & Snell R Square= 0,063; Nagelkerke R Square= 0,084[85]					

85 A set of independent variables explain explains between 6,3% and 8,4% of the variance.