KOREA
Sharing Hope Sharing Future

Ministry of Foreign Affairs
Republic of Korea

UNDP

Assessment of Legal, Policy, Institutional, and Technological Frameworks on Technology-Facilitated Gender-Based Violence (TF GBV) in the Western Balkans

KOREA
Sharing Hope Sharing Future

Ministry of Foreign Affairs
Republic of Korea

UNDP

Assessment of Legal, Policy, Institutional, and Technological Frameworks on Technology-Facilitated Gender-Based Violence (TF GBV) in the Western Balkans

UNDP 2025

CONTENT

1. INTRODUCTION **8**
- **1.1.** Framing the Issue: Understanding Technology-Facilitated Gender-Based Violence 8
- **1.2.** Key Forms of Technology-Facilitated Gender-Based Violence 9
- **1.3.** Online Sexual Violence Targeting Children 10
- **1.4.** Interconnectedness of TF GBV Forms 10

2. ASSESSMENT OF LEGAL RESPONSES TO TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE IN THE WESTERN BALKAN **14**
- **2.1.** International policy framework 15
- **2.2.** Country-specific legal frameworks 16
  - Albania 16
  - Bosnia and Herzegovina 17
  - Kosovo* 20
  - Montenegro 22
  - North Macedonia 23
  - Serbia 24
- **2.3.** Advances and Gaps in Legal Frameworks Addressing TF GBV in the Western Balkans 25
- **2.4.** Conclusion 27

3. MAPPING CHALLENGES: INSTITUTIONAL AND CIVIL SOCIETY STAKEHOLDERS ADDRESSING TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE (TF GBV) **30**
- **3.1.** Widespread nature of TF GBV across the Western Balkans 30
- **3.2.** Stakeholder Landscape in Addressing TF GBV Across the Western Balkans 35
- **3.3.** Institutional Gaps and Challenges in Addressing TF GBV 38

4. RECOMMENDATIONS FOR ADDRESSING TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE IN THE WESTERN BALKANS **50**

01 Introduction

1. Introduction

Technology-Facilitated Gender-Based Violence (TF GBV) is a growing global issue with far-reaching ramifications for human rights, gender equality, and online safety in digital environments. In the Western Balkans – where digitalisation is progressing alongside enduring structural inequalities – TF GBV exacerbates existing vulnerabilities and reveals critical gaps in protection mechanisms. Technology-facilitated violence against women is alarmingly widespread in the region; over half of all women aged 18 and older active online report experiencing some form of digital abuse in their lifetime. Unwanted sexual content or advances on social media (30%), receiving rude or threatening messages (39.7%), and having their personal accounts or websites hacked (25.4%) are the most prevalent types of harassment. While 40% of affected women reported experiencing this type of violence once, one in four endures it on a daily or weekly basis. The impact is profound: nearly two-thirds of survivors reported feeling emotionally distressed, unsafe, or humiliated. For some, the harm extends beyond the screen - one in ten women said the abuse had damaged their relationships and social connections. These figures demonstrate the extent of the issue as well as the severe psychological and societal harm it causes.[1]

This analysis seeks to provide a comprehensive assessment of the legal, policy, institutional, and technological frameworks and capacities related to TF GBV across the Western Balkans. By identifying key strengths, gaps, and emerging trends, it aims to inform the development of actionable recommendations to bolster regional and national responses to TF GBV, strengthen prevention efforts, and improve victim support mechanisms.

The overarching goal is to contribute to a more harmonised, effective, and resilient regional approach to combating TF GBV across the region, while fostering the integration of innovative technological solutions in prevention and response strategies.

As a starting point in this process, the analysis conducts a thorough review of existing legal frameworks relevant to TF GBV in the Western Balkans.

1.1. Framing the Issue: Understanding Technology-Facilitated Gender-Based Violence

Digital technologies have transformed communication, participation, and economic and political engagement worldwide, but have also given rise to new and deeply harmful patterns of violence, particularly targeting women, girls, children and marginalised groups. Technology-Facilitated Gender-Based Violence (TF GBV) is now widely recognised as a serious and growing human rights violation, compounding existing inequalities and causing profound physical, psychological, economic, and societal harms – both online and offline.[2]

According to the United Nations Entity for Gender Equality and the Empowerment of Women (UN Women), TF GBV encompasses “any act committed or aggravated through the use of digital

1 UN Women (2023). The Dark Side of Digitalization: Technology-Facilitated Violence Against Women in Eastern Europe and Central Asia. Available at: https://eca.unwomen.org/sites/default/files/2024-01/research-tf-vaw_full-report_24-january2.pdf

2 UN Women. (2024, October). Repository of UN Women’s work on technology-facilitated gender-based violence. https://www.unwomen.org/sites/default/files/2024-10/repository-of-un-womens-work-on-technology-facilitated-gender-based-violence-en.pdf

tools or technologies that causes physical, sexual, psychological, social, political, or economic harm to women and girls because of their gender." TF GBV leverages the reach, speed, and anonymity of digital platforms to inflict abuse, often reinforcing the gendered power dynamics that persist offline.[3]

1.2. Key Forms of Technology-Facilitated Gender-Based Violence[4]

While Technology-Facilitated Gender-Based Violence (TF GBV) is continually evolving in both form and scope, this report identifies a core set of acts as a starting point for analysis - examined through a lens of both gender equality and legal framework, as well as current practices in the region. TF GBV encompasses a broad spectrum of abusive behaviours, not limited to:

- **Online Gender-Based Harassment:** Repeated, unwanted digital communication intended to cause distress or fear, often expressed through unsolicited images, threats, defamatory language, and insults rooted in misogynistic, homophobic, or sexist stereotypes.
- **Virtual Mobbing:** Coordinated online attacks by groups using digital platforms to spread hostile commentary targeting individuals, particularly women's rights defenders, activists, marginalised groups, and female journalists.
- **Gendered or Sexist Hate Speech:** Communications that incite discrimination, hatred, or violence based on sex, sexual orientation, or gender identity.[5]
- **Image-Based Sexual Abuse:** Non-consensual sharing, manipulation, or public dissemination of intimate images or videos, often intended to shame, extort, or silence victims. Women's rights organisations reject the term 'revenge porn', emphasising that it misplaces blame onto victims and sexualizes abuse.
- **Deepfake Pornography:** AI-generated manipulated content depicting individuals in sexually explicit scenarios without their consent, used for harassment, blackmail, or reputational damage.
- **Cyberstalking:** Persistent, technology-enabled monitoring, messaging, or harassment that installs fear, anxiety, and lasting emotional distress.
- **Doxxing (Targeted Exposure):** The collection and publication of a person's private information such as address, phone number, or family contacts, with the intent to humiliate, intimidate, or endanger them.
- **Slut-Shaming and Body-Shaming:** Online harassment targeting women based on perceived or real sexual behaviour or physical appearance, aimed at publicly shaming and diminishing their social standing.[6]
- **Exclusion:** Deliberate marginalisation or silencing of women and marginalised groups in online platforms and forums, undermining their participation and credibility.
- **Online Threats:** Threats of physical or sexual violence directed at women and marginalised individuals, often targeting public figures such as female journalists, politicians, and activists.

3 Ibid.

4 UNFPA. Technology-Facilitated Gender-Based Violence: A Growing Threat. https://www.unfpa.org/TFGBV; UN Women. (2024, October). Repository of UN Women's work on technology-facilitated gender-based violence. https://www.unwomen.org/sites/default/files/2024-10/repository-of-un-womens-work-on-technology-facilitated-gender-based-violence-en.pdf

5 Council of Europe, Gender Equality Unit. (2016, February 1). Background note on sexist hate speech. Council of Europe. https://rm.coe.int/background-note-on-sexist-hate-speech/16805917cb

6 Goblet, M., & Glowacz, F. (2021). Slut shaming in adolescence: A violence against girls and its impact on their health. *International Journal of Environmental Research and Public Health, 18*(12), 6657. https://doi.org/10.3390/ijerph18126657

TF GBV also intersects with broader and more traditional forms of violence:

- **Domestic Violence:** Technology increasingly serves as a tool for coercive control, surveillance, psychological abuse, and financial manipulation within intimate relationships.
- **Sexual Harassment:** Digital spaces create new arenas for sexual harassment, particularly in professional, educational, and political settings.
- **Human Trafficking:** Technology is exploited to recruit, groom, and control victims for sexual exploitation and labour, often targeting vulnerable groups including minors.
- **Child Sexual Abuse Material (CSAM):** Production, distribution, and possession of sexually exploitative images and videos involving children is a persistent and growing digital threat worldwide.

1.3. Online Sexual Violence Targeting Children

Children and adolescents across the Western Balkans, as elsewhere, are increasingly vulnerable to forms of online sexual exploitation:

- **Online Grooming:** Adults use social media, gaming platforms, or messaging apps to manipulate minors for sexual purposes, often posing as peers. Greater internet access among the Balkans youth has heightened grooming risks, with law enforcement across the region noting a rise in incidents, particularly in the COVID-19 pandemic.[7]
- **Child Sexual Abuse Material (CSAM) Sharing:** Production and dissemination of CSAM is facilitated by encrypted apps and anonymous networks. In 2021 alone, 85 million images and videos of child sexual abuse were reported globally. While the full extent of the problem in the Western Balkans remains underreported, regional police and Europol/Interpol operations have uncovered trafficking and sharing networks involving CSAM.[8]
- **Sextortion of Minors:** Perpetrators coerce children into producing explicit material and then blackmail them with threats of exposure. Sextortion cases involving teenagers have been widely reported across the region, with serious consequences, including self-harm.
- **Live-Streaming Abuse:** Although few high-profile cases have been publicly disclosed in the Western Balkans, authorities remain vigilant against the growing threat of offenders directing real-time sexual abuse of children via livestreams, a particularly difficult crime to detect.

1.4. Interconnectedness of TF GBV Forms

These forms of violence often overlap and reinforce one another, with TF GBV rarely occurring as a single event but rather unfolding as a cascade of interconnected harms. For instance, a woman's private sexual content may be hacked and publicly distributed (image-based sexual abuse); her identity exposed through doxxing; and she may subsequently face cyberstalking and sexual harassment by strangers.

7 INTERPOL. (2020, September). Threats and trends: Child sexual exploitation and abuse – COVID-19 impact. https://www.interpol.int/content/download/15611/file/COVID19%20-%20Child%20Sexual%20Exploitation%20and%20Abuse%20threats%20and%20trends.pdf

8 Europol. (2023, November 8). *39 suspects identified in major online child sexual abuse swoop in Western Balkan region*. https://www.europol.europa.eu/media-press/newsroom/news/39-suspects-identified-in-major-online-child-sexual-abuse-swoop-in-western-balkan-region

What binds these acts together is the digital setting in which these actions take place, the technology tools used to facilitate abuse, and the underlying gendered power dynamics, typically involving men perpetrating violence against women.

TF GBV is frequently an extension or continuation of offline domestic violence, used to exert control, intimidate, monitor, or punish (former) intimate partners. Gender-based violence in the digital realm manifests not only as sexual violence (e.g., image-based abuse, harassment) but also as psychological violence (e.g., stalking, doxxing) and economic violence (e.g., damaging a woman's employment prospects through public shaming).

The impacts of TF GBV extend beyond personal trauma to include professional, educational, and social exclusion. Victims often experience job loss, withdrawal from education, forced relocation, or community ostracism.

Importantly, perpetrators go beyond their former intimate partners; private content may be obtained without a victim's knowledge through secret recordings, sexual assault, digital hacking, or AI manipulation (deepfakes). Whether based on authentic or fabricated material, non-consensual distribution of such content serves to shame, humiliate, blackmail, or coerce victims, leading to devastating psychological, social, and economic consequences.

With the growing awareness of TF GBV, it becomes increasingly critical to evaluate how national legal systems conceptualise, recognise, and respond to these evolving harms.

The following sections of this chapter present an in-depth analysis of criminal legislation in Serbia, Bosnia and Herzegovina, Montenegro, Albania, North Macedonia, and Kosovo. Through structured tables summarising the key provisions by type of violence and critical reflections on both progress and gaps, the chapter assesses regional progress and identifies the enduring challenges in ensuring comprehensive protection against TF GBV.

02 Assessment of Legal Responses to Technology-Facilitated Gender-Based Violence in the Western Balkans

2. Assessment of Legal Responses to Technology-Facilitated Gender-Based Violence in the Western Balkan

For the purpose of this assessment, criminal codes of six Western Balkan jurisdictions were systematically reviewed to identify legal provisions that may be applicable to technology-facilitated gender-based violence (TF GBV). The analysis focused on substantive criminal law, examining whether offences such as stalking, harassment, threats, non-consensual distribution of intimate content, online sexual exploitation, and identity-related abuses are criminalised in ways to include crimes committed via digital technologies. Special attention was given to provisions on child protection, articles related to domestic violence, and offences related to personal data misuse or cyber intrusion. This legal mapping aimed to highlight both explicit and implicit coverage of TF GBV within existing legislation, while also identifying inconsistencies, legal gaps, or areas requiring harmonisation across jurisdictions.

Before presenting the country-specific legal analysis, this paper provides a brief overview of international conventions and legal instruments relevant to advancing the understanding and prosecution of technology-facilitated gender-based violence (TF GBV). Although countries in the Western Balkans are at different stages of the EU accession and alignment with Council of Europe standards, international conventions and the EU directives offer essential legal and policy benchmarks for addressing emerging forms of violence, including technology-facilitated gender-based violence (TF GBV). These instruments help define obligations around criminalisation, prevention, protection, prosecution, and cross-border cooperation, and they increasingly reflect the need to adapt legal systems to the digital dimension of GBV. Their implementation—either through binding ratification or policy alignment—can guide legislative reform, institutional training, and victim protection in the region.

2.1. International policy framework

Instrument	Scope	Relevance to TF GBV
CEDAW (1979)	Convention on the Elimination of All Forms of Discrimination against Women	General Recommendation No. 35 (2017) recognises that violence occurs in all spheres of human interaction, thus stating that *"contemporary forms of violence occur online and in other digital environments"*
Istanbul Convention (2011)	Violence against women and domestic violence	Article 3a provides a broad definition of violence, while Articles 33, 34, and 40 can be interpreted to encompass forms of cyberviolence. This interpretation was clarified by GREVIO in its 2021 General Recommendation No. 1, requiring States Parties to establish legal and policy frameworks that explicitly address cyberviolence against women.
Budapest Convention (2001)	Cybercrime and digital evidence	Provides tools for investigation, evidence collection, and international cooperation in cyber-enabled violence cases.
Lanzarote Convention (2007)	Child sexual abuse and exploitation	Criminalises online grooming, CSAM, and abuse via ICTs. Relevant to TF GBV targeting children.
European Commission Directive on combating violence against women and domestic violence	Introducing common standards across EU Member States for preventing and combating violence against women and domestic violence, while ensuring victims' protection and access to justice.	The EU Directive uses the term *cyber violence* without offering a single definition, instead outlining specific forms such as cyberstalking, cyber harassment, non-consensual sharing of intimate images, and cyber incitement to violence or hatred. It also proposes robust victim protection measures, including the ability to report such crimes online or via secure digital channels.
Victims' Rights Directive (2012/29/EU)	Rights and protection of crime victims	Ensures that TF GBV victims are informed, protected, and supported in judicial processes.
Equal Treatment Directive (2006/54/EC)	Gender equality in employment	Covers sexual harassment, potentially including workplace-related cyber harassment.
General Data Protection Regulation (GDPR) (2016/679)	Data protection	Applies in cases of non-consensual sharing of personal/intimate content (e.g. doxxing, image-based abuse).
E-Commerce Directive (2000/31/EC)	Online service provider liability	Requires platforms to remove or block illegal content, including TF GBV material.
Directive on Combating Sexual Abuse of Children (2011/93/EU)	Sexual exploitation of minors	Applies to online abuse, requiring Member States to block/remove CSAM and protect children online.
Audiovisual Media Services Directive (2010/13/EU)	Content regulation across media	Requires platforms to address content inciting hate or violence based on sex or gender; relevant to TF GBV in video content.
Anti-Trafficking Directive (2011/36/EU)	Human trafficking	Relevant where trafficking involves online grooming, recruitment, or exploitation of women and girls; does not yet fully address digital dimensions.

While the phenomenon of Technology-Facilitated Gender-Based Violence (TF GBV) is increasingly recognised as a serious threat to human rights and gender equality, legislative frameworks across the Western Balkans show considerable differences in both the conceptualisation and institutional responses to these forms of violence. This Chapter offers a comprehensive overview of criminal legislation relevant to TF GBV in Serbia, Bosnia and Herzegovina, Montenegro, Albania, North Macedonia, and Kosovo. Through a systematic examination of the most relevant offences and legal instruments, it critically assesses the extent to which different jurisdictions address online and technology-facilitated forms of violence, identifying areas of progress as well as persistent gaps. The tables presented below categorise the relevant legal provisions by type of violence and serve as an analytical foundation for exploring regional legislative trends, normative advancements, and the enduring challenges in ensuring comprehensive protection against TF GBV.

2.2. Country-specific legal frameworks

Albania

Type of Violence	Relevant Legal Provisions (Criminal Code of the Republic of Albania) Law No. 7895/1995, 8733/2001, 9086/2003, 9275/2004, 9686/2007, 9859/2008, 10023/2008, 23/2012, 144/2013, 36/2017 and 89/2017)
(Cyber) Stalking	- Article 121/a: Stalking
Doxxing	- Article 117: Pornography – Child Pornography - Article 123: Obstruction or Violation of the Privacy of Correspondence
(Cyber) Sexual Harassment	- Article 107/a: Sexual Violence - Article 108/a: Sexual Harassment
Sharing of intimate images	- Article 109/b: Coercion by Blackmail or Violence to Surrender Property - Article 130/a: Domestic Violence

The Criminal Code of the Republic of Albania does not explicitly address technology-facilitated violence against women as a separate legal category. However, several existing provisions can be applied to acts of online abuse. For instance, Article 121/a criminalises stalking, which can include cyberstalking behaviours. Article 123 on the violation of the privacy of correspondence could also be relevant in cases of doxxing, while Article 108/a specifically criminalises sexual harassment, covering actions that create a threatening, hostile, humiliating, or offensive environment—potentially including online harassment.

Importantly, under Article 50 (item j) of the Criminal Code, gender-based crimes are treated as aggravating circumstances, thereby recognising the heightened gravity of gender-based violence, whether committed online or offline. In addition to the Criminal Code, Albania's *Law on Protection from Discrimination* includes sexual harassment as a form of discrimination, defining it as unwanted sexual behaviour that undermines a person's dignity and creates a hostile or humiliating environment.

While these provisions provide some legal grounds for addressing TF GBV, the absence of specific offences directly targeting online forms of abuse leaves gaps in the protection of

women and children in digital spaces. Current protections rely heavily on interpreting general offences (such as stalking, harassment, or privacy violations) in the online context, which can create challenges in prosecution and victim protection.

In strengthening its response to TF GBV, Albania could benefit from more explicit recognition of technology-facilitated offences within its criminal legislation and continued efforts to sensitise law enforcement and judiciary on the specific nature and harms of online gender-based violence. Alignment with the Istanbul Convention commitments, ratified by Albania, suggests a need for ongoing legislative development to fully address emerging forms of digital violence.

Bosnia and Herzegovina

Type of Violence	Federation of BiH (FBiH)	Republika Srpska (RS)	Brčko District (BD)
(Cyber) Stalking	- Article 186: Violation of Secrecy of Letters or Other Consignments - Article 189: Unauthorised Optical Recording - Article 193: Unauthorised Use of Personal Data - Article 183: Endangering Safety	- Article 144: Stalking - Article 150: Endangering Safety - Article 156: Unauthorised Photography - Article 156a: Unauthorised Publication and Display of Another's Writing, Image, or Recording - Article 157: Unauthorised Use of Personal Data	- Article 186: Violation of Secrecy of Letters or Other Consignments - Article 189: Unauthorised Optical Recording - Article 193: Unauthorised Use of Personal Data - Article 183: Endangering Safety

Type of Violence	Federation of BiH (FBiH)	Republika Srpska (RS)	Brčko District (BD)
Doxxing	- Article 183: Endangering Safety - Article 211: Exploitation of a Child or Minor for Pornography - Article 186: Violation of Secrecy of Letters or Other Consignments - Article 193: Unauthorised Use of Personal Data	- Article 150: Endangering Safety - Article 153: Violation of Secrecy of Letters or Other Consignments - Article 156: Unauthorised Photography - Article 156a: Unauthorised Publication and Display of Another's Writing, Image, or Recording - Article 157: Unauthorised Use of Personal Data - Article 208a: Defamation - Article 208b: Disclosure of Personal and Family Circumstances - Article 208v: Public Ridicule Based on Race, Religion, or Nationality - Article 175: Exploitation of Children for Pornography - Article 176: Exploitation of Children for Pornographic Performances - Article 178: Use of Computer Networks or Other Means for Commission of Sexual Abuse or Exploitation of a Child - Article 359: Public Incitement and Provocation of Violence and Hatred	- Article 183: Endangering Safety - Article 211: Exploitation of a Child or Minor for Pornography - Article 186: Violation of Secrecy of Letters or Other Consignments - Article 193: Unauthorised Use of Personal Data
(Cyber) Sexual Harassment	- Article 296: Blackmail	- Article 170: Sexual Harassment - Article 170a: Misuse of Photographs and Videos of Sexually Explicit Content - Article 178: Use of Computer Networks or Other Means for Commission of Sexual Abuse or Exploitation of a Child	- Article 296: Blackmail

Type of Violence	Federation of BiH (FBiH)	Republika Srpska (RS)	Brčko District (BD)
Sharing of intimate images	- Article 222: Domestic Violence - Article 296: Blackmail	- Article 166: Sexual Blackmail - Article 233: Blackmail - Article 156: Unauthorised Photography - Article 156a: Unauthorised Publication and Display of Another's Writing, Image, or Recording - Article 157: Unauthorised Use of Personal Data - Article 175: Exploitation of Children for Pornography - Article 176: Exploitation of Children for Pornographic Performances - Article 178: Use of Computer Networks or Other Means for Commission of Sexual Abuse or Exploitation of a Child - Article 190: Domestic Violence	- Article 222: Domestic Violence - Article 296: Blackmail

In order to guarantee a legal, institutional, and organisational framework for the prevention of violence against women, the protection of victims, and the prosecution of offenders, Bosnia and Herzegovina, as a signatory to the Istanbul Convention, has committed to implementing legislative and other measures.

Within its complex constitutional setup, Bosnia and Herzegovina has four separate criminal codes in place:

- Criminal Code of Bosnia and Herzegovina (CC BiH),
- Criminal Code of Republika Srpska (CC RS),
- Criminal Code of the Federation of Bosnia and Herzegovina (CC FBiH),
- Criminal Code of Brčko District of Bosnia and Herzegovina (CC BDBiH).

As the substantive part of the CC BiH primarily addresses conflict-related gender-based violence (GBV), this Code was not the subject of analysis for TF GBV in non-conflict settings.

For all types of violence considered, including cyberstalking, doxxing, cyber sexual harassment, and the non-consensual sharing of intimate images, there are relevant criminal offences with provisions applicable to acts of technology-facilitated gender-based violence. However, a closer look at legislative frameworks shows that Republika Srpska has introduced greater precision in

defining offences that more directly correspond to acts of TF GBV, particularly through explicit provisions on stalking, sexual harassment, and the misuse of digital content. In May 2025, similar provisions were integrated into the amended Criminal Code of the Federation of Bosnia and Herzegovina, aligning it with the Istanbul Convention. The House of Representatives of the Federation Parliament unanimously adopted the Draft Law on Amendments to the Criminal Code. For the law to enter into force, it must also be adopted by the House of Peoples of the Federation Parliament.

Protection for minors and children is rather well-established in all three criminal codes, particularly through provisions criminalising the exploitation of children for pornography and the use of digital networks to commit sexual offences against minors.

Despite these positive developments, significant challenges remain. Fragmentation of criminal codes across the two Entities and the Brčko District leads to inconsistencies in victim protection and enforcement. While various offences may apply to technology-facilitated violence and all criminal codes show progress in this area, there is still no uniform or clearly articulated legal definition of TF GBV behaviours.

In order to fully meet the standards outlined by the Istanbul Convention, further legislative harmonisation and the introduction of specialised TF GBV offences would strengthen the legal framework, ensure more consistent protection across the country, and enhance access to justice for victims of digital forms of gender-based violence.

Kosovo*

Type of Violence	Relevant Legal Provisions (Criminal Code No. 06/L-074 of the Republic of Kosovo, Official Gazette No. 2, 14 January 2019, Priština)
(Cyber) Stalking	- Article 182: Harassment - Article 202: Unauthorised Photographing and Other Forms of Recording - Article 232: Child Pornography Exploitation
Doxxing	- Article 232: Child Pornography Exploitation - Article 231: Offering Pornographic Material to Persons Under Sixteen - Article 202: Unauthorised Photographing and Other Forms of Recording - Article 199: Violation of Secrecy of Letters and Computer Databases - Article 181: Threat - Article 141: Incitement to Discord and Intolerance
(Cyber) Sexual Harassment	- Article 183: Sexual Harassment - Article 199: Violation of Secrecy of Letters and Computer Databases - Article 231: Offering Pornographic Material to Persons Under Sixteen - Article 232: Child Pornography Exploitation - Article 327: Unauthorised Access to Computer Systems - Article 329: Blackmail
Non-consensual sharing of intimate images	- Article 336: Identity Theft and Unauthorised Use of Access Devices - Article 329: Blackmail - Article 327: Unauthorised Access to Computer Systems - Article 248: Domestic Violence - Article 232: Child Pornography Exploitation - Article 202: Unauthorised Photographing and Other Forms of Recording - Article 192: Coercion

* This designation is without prejudice to positions on status, and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.

Kosovo's Criminal Code offers important tools to address various forms of Technology-Facilitated Gender-Based Violence (TF GBV), even though TF GBV is not explicitly recognised as a separate criminal category. A range of offences are applicable to different manifestations of online and technology-mediated violence, including harassment, cyberstalking, online threats, unauthorised access to personal data, and exploitation of minors. The legal system in Kosovo is very robust when it comes to safeguarding children from being sexually exploited online. Articles 232 and 231 criminalise the exploitation of children in pornography and the offering of pornographic material to minors under the age of sixteen, addressing some of the most severe forms of TF GBV against children.

Although Kosovo's Criminal Code does not define non-consensual sharing of intimate images[9] as a separate criminal offence, it provides protection through several related provisions. Acts typically associated with non-consensual sharing of intimate images may be prosecuted under:

- Article 336 (Identity Theft and Unauthorised Use of Access Devices),
- Article 329 (Blackmail),
- Article 327 (Unauthorised Access to Computer Systems),
- Article 248 (Domestic Violence),
- Article 202 (Unauthorised Photographing and Other Forms of Recording),
- Article 192 (Coercion).

Where victims are minors, additional safeguards are triggered under Articles 232 and 231, ensuring stricter penalties for the abuse and exploitation of children in online contexts.

One particularly noteworthy development in Kosovo's system is the regulation of domestic violence. Article 248 defines domestic violence broadly to include physical, psychological, sexual, and economic violence. Importantly, the Code treats any criminal offence committed in a family setting as an aggravating circumstance, signalling the state's recognition of the gravity of violence perpetrated against intimate partners or family members, including technology-facilitated forms of abuse such as digital surveillance, threats, and harassment.

Another distinctive feature is found in Article 62 (Prohibition from Holding Office in Public Administration or Public Service). According to paragraph 4, courts must impose a ban of one to five years on officials convicted of domestic violence, prohibiting them from holding office in public administration or public service. This provision strengthens the accountability of public officials and represents a progressive step in linking criminal sanctions with impacts on one's career.

Despite these positive developments, Kosovo's framework remains somewhat fragmented in addressing TF GBV:

- There is no explicit definition of TF GBV or systematic recognition of technology-facilitated acts as a distinct form of violence.
- Prosecution of non-consensual sharing of intimate images and other digital abuses relies on adapting general provisions not originally designed for the digital age, which may create inconsistencies in interpretation and application.

9 Non-consensual sharing of intimate images is often referred to as *revenge pornography*, though the term is avoided here as misleading. Instead, it resorts to a more accurate term *image-based sexual abuse*, which centers the violation of consent rather than presumed motives

- Specialised training for law enforcement and judiciary is needed to ensure that digital abuses are properly identified, prosecuted, and sanctioned.
- Kosovo's Criminal Code reflects significant progress in adapting traditional criminal law concepts to emerging forms of technology-facilitated violence. Most prominent strongpoints are its safeguards against child exploitation, its recognition of domestic violence dynamics, and the integration of professional sanctions for public officials convicted of abuse. Future steps should aim to explicitly define and categorise TF GBV, harmonise the treatment of image-based abuse, and strengthen victim-cantered approaches to better protect women, children, and marginalised groups in the evolving digital environment.

Montenegro

Type of Violence	Relevant Legal Provisions (Criminal Code of Montenegro) Official Gazette, No. 70/2003, 13/2004, 47/2006 and Official Gazette, No. 40/2008, 25/2010, 32/2011, 64/2011 – other laws, 40/2013, 56/2013, 14/2015, 42/2015, 58/2015 – other laws, 44/2017, 49/2018, 3/2020, 26/2021 - correction, 144/2021 and 145/2021 and 110/2023
(Cyber) Stalking	- Article 168a: Stalking - Article 168: Endangering Safety - Article 174: Unauthorised Photography - Article 175: Unauthorised Publication and Display of Another's Writing, Image, or Recording - Article 176: Unauthorised Collection and Use of Personal Data
Doxxing	- Article 168: Endangering Safety - Article 172: Violation of Secrecy of Letters and Other Consignments - Article 174: Unauthorised Photography - Article 175: Unauthorised Publication and Display of Another's Writing, Image, or Recording - Article 176: Unauthorised Collection and Use of Personal Data - Article 211: Exploitation of Children for Pornography - Article 443: Racial and Other Discrimination
(Cyber) Sexual Harassment	- Article 211c: Sexual Harassment - Article 211: Exploitation of Children for Pornography
Non-consensual sharing of intimate images	- Article 174: Unauthorised Photography - Article 175: Unauthorised Publication and Display of Another's Writing, Image, or Recording - Article 175a: Misuse of Another's Recording, Photograph, Image, Audio Recording, or Writing with Sexually Explicit Content - Article 176: Unauthorised Collection and Use of Personal Data - Article 211b: Luring a Child Under Fourteen Years of Age for the Purpose of Committing Criminal Offences Against Sexual Freedom - Article 220: Domestic Violence or Violence in the Family Setting - Article 251: Blackmail

Various provisions of the Criminal Code in Montenegro offer protection for women in the online arena across different types of technology-facilitated violence. However, Montenegro stands out for introducing a separate criminal offence, *Misuse of Another's Recording, Photograph, Image, Audio Recording, or Writing with Sexually Explicit Content* (Article 175a), thus addressing online abuse more comprehensively.

This provision criminalises both the unauthorised dissemination and the manipulation of sexually explicit materials without the consent of the depicted person, prescribing a prison sentence of up to two years for basic offences, up to three years when distributed to a larger audience, and from one to eight years if committed against a child. Threats to commit the offence are also punishable.

The adoption of Article 175a represents a notable advancement in Montenegro's legal response to TF GBV. By explicitly addressing both the sharing of real images and the fabrication of manipulated content (such as deepfakes), the law reflects a forward-looking approach aligned with emerging digital threats. It also brings Montenegro closer to fulfilling its obligations under the Istanbul Convention. Continued efforts in awareness-raising, training, and enforcement will be essential to fully operationalise these protections and ensure meaningful access to justice for victims.

North Macedonia

Type of Violence	Relevant Legal Provisions (Criminal Code of the Republic of North Macedonia) (Official Gazette Republic of Macedonia, No. 37/96, 80/1999, 4/2002, 43/2003, 19/2004, 81/2005, 60/2006, 73/2006, 7/2008, 139/2008, 114/2009, 51/2011, 135/2011, 185/2011, 142/2012, 166/2012, 55/2013, 82/2013, 14/2014, 27/2014, 28/2014, 41/2014, 115/2014, 132/2014, 160/2014, 199/2014, 196/2015, 226/2015, 97/2017, 248/2018 and 36/2023.
(Cyber) Stalking	- Article 202: Endangering Safety - Article 203: Stalking - Article 206: Violation of Secrecy of Letters or Other Consignments - Article 207: Unauthorised Disclosure of Personal Records - Article 208: Misuse of Personal Data - Article 210: Unauthorised Eavesdropping and Audio Recording - Article 211: Unauthorised Visual Recording
Doxxing	- Article 202: Endangering Safety - Article 210: Unauthorised Eavesdropping and Audio Recording - Article 211: Unauthorised Visual Recording - Article 253: Display of Pornographic Material to a Child - Article 254: Production and Distribution of Materials Depicting Sexual Abuse of Children
(Cyber) Sexual Harassment	- Article 210: Unauthorised Eavesdropping and Audio Recording - Article 251: Sexual Harassment
Non-consensual sharing of intimate images	- Article 255: Unauthorised Distribution of Photographs, Films, and Video Recordings of Sexual Nature - Article 348: Blackmail

North Macedonia has developed a relatively structured legal framework applicable to various forms of Technology-Facilitated Gender-Based Violence (TF GBV), even though TF GBV is not yet explicitly recognised as a standalone category. The Criminal Code contains several provisions addressing cyberstalking, doxxing, cyber sexual harassment, and revenge pornography. Notably, Article 255 criminalises the unauthorised distribution of photographs, films, and video recordings of sexual nature, directly targeting one of the most harmful manifestations of online abuse and aligning national legislation with international standards, including the Istanbul Convention.

A significant development occurred in February 2023, when North Macedonia amended its Criminal Code to explicitly criminalise stalking and harassment in both physical and digital forms. These amendments also address the misuse of personal data as a means of harassment. Sanctions for these offences range from fines to prison sentences of up to three years, with harsher penalties when the crime is committed by an intimate partner or against a child. These reforms aim to provide comprehensive protection against multiple forms of violence, including digital violence, and represent an important step toward the full implementation of the Istanbul Convention, ratified by North Macedonia in 2017.

The Criminal Code also includes important provisions on stalking (Article 203) and sexual harassment (Article 251), and multiple protections related to the unauthorised recording and dissemination of private information (Articles 210–211), further strengthening safeguards against TF GBV.

However, while the amendments benefit legal clarity, TF GBV is still addressed through the interpretation of general offences, which can lead to challenges in uniform application and victim protection. To consolidate progress, North Macedonia could further benefit from introducing a specific legal definition of TF GBV and ensuring that law enforcement and judiciary receive specialised training to recognise and effectively prosecute digital forms of gender-based violence.

Overall, North Macedonia has made significant and commendable strides in adapting its legal system to the realities of online abuse. Continued efforts to implement the new provisions consistently and to strengthen institutional capacities will be crucial to ensuring effective protection and access to justice for victims.

Serbia

Type of Violence	Applicable Legal Provisions (Criminal Code of the Republic of Serbia, (Official Gazette RS, No. 85/2005, 88/2005 - correction, 107/2005 - correction, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016, 35/2019 and 94/2024).)
(Cyber) Stalking	- Stalking (Article 138a) - Endangering Safety (Article 138) - Unauthorised Photography (Article 144) - Unauthorised Publication and Display of Someone Else's Writing, Image, or Recording (Article 145) - Unauthorised Collection of Someone Else's Data (Article 146)
Doxxing	- Endangering Safety (Article 138) - Violation of Secrecy of Letters and Other Consignments (Article 142) - Unauthorised Photography (Article 144) - Unauthorised Publication and Display of Someone Else's Writing, Image, or Recording (Article 145) - Unauthorised Collection of Someone Else's Data (Article 146) - Insult (Article 170) - Disclosure of Personal and Family Circumstances (Article 172) - Violation of Honour Due to Racial, Religious, National, or Other Affiliation (Article 174) - Use of Computer Networks or Other Communication Technologies to Commit Crimes Against Sexual Freedom Involving a Minor (Article 185b) - Racial and Other Discrimination (Article 387)

(Cyber) Sexual Harassment	- Sexual Harassment (Article 182a) - Use of Computer Networks or Other Communication Technologies to Commit Crimes Against Sexual Freedom Involving a Minor (Article 185b)
Non-consensual sharing of intimate images	- Unauthorised Photography (Article 144) - Unauthorised Publication and Display of Someone Else's Writing, Image, or Recording (Article 145) - Unauthorised Collection of Someone Else's Data (Article 146) - Display, Acquisition, and Possession of Pornographic Material and Exploitation of a Minor for Pornography (Article 185) - Domestic Violence (Article 195) - Blackmail (Article 215)

The table shows that Serbia has established a range of legal provisions applicable to various forms of Technology-Facilitated Gender-Based Violence (TF GBV). Although the Criminal Code of Serbia does not explicitly recognise non-consensual sharing of intimate images as a distinct criminal offence, it offers protection through related offences such as Stalking (Article 138a), Unauthorised Photography (Article 144), Unauthorised Publication and Display of Someone Else's Writing, Image, or Recording (Article 145), Sexual Harassment (Article 182a), Domestic Violence (Article 194), and Blackmail (Article 215). In cases involving minors, additional safeguards are provided through Display, Acquisition, and Possession of Pornographic Material and Exploitation of a Minor for Pornography (Article 185), and the Use of Computer Networks or Other Communication Technologies to Commit Crimes Against Sexual Freedom Involving a Minor (Article 185b).

An important limitation, however, lies in the procedural aspects of prosecution: while offences such as child pornography, stalking, blackmail, and sexual harassment are prosecuted ex officio (by state authorities without the need for a private complaint), cases involving the unauthorised publication or sharing of another person's intimate images — which frequently occurs in instances of revenge pornography — require the victim to initiate a civil lawsuit. This can create additional barriers for victims seeking justice, particularly considering the emotional and social pressures involved.

2.3. Advances and Gaps in Legal Frameworks Addressing TF GBV in the Western Balkans

Over the past decade, countries of the Western Balkans have made important strides in adapting their criminal legislation to better respond to emerging forms of Technology-Facilitated Gender-Based Violence (TF GBV). However, despite notable progress, legal responses across the region remain fragmented, incomplete, and often reactive rather than proactive. The analysis of criminal law frameworks in Serbia, Bosnia and Herzegovina, Montenegro, Albania, North Macedonia, and Kosovo reveals both encouraging developments as well as critical areas for improvement.

Advances:

- **Growing political will to review and constructively amend legislation, driven in part by international and regional obligations.**

  While not yet fully consolidated, this external pressure—particularly through EU accession processes and Council of Europe commitments—has begun to yield results, with

several countries initiating legal reforms aligned with global standards on technology-facilitated gender-based violence (TF GBV).

- **Recognition of Key Forms of TF GBV:**

  Across the region, criminal codes now cover a wide array of behaviours relevant to TF GBV. Core offences such as cyberstalking, online harassment, threats, unauthorised surveillance, and the non-consensual distribution of intimate images ('revenge pornography') are criminalised in various forms. Serbia, Montenegro, and North Macedonia, in particular, have introduced specific offences such as stalking, sexual harassment, and the unauthorised dissemination of sexually explicit material, providing a stronger foundation for prosecution.

- **Addressing Image-Based and Child Sexual Abuse:**

  Most countries have incorporated robust provisions criminalising sexual exploitation of children online, including production, possession, and distribution of child sexual abuse materials (e.g., Kosovo's Articles 277/I and 231; Bosnia and Herzegovina's Entity laws). This alignment with international standards, such as the Lanzarote and Budapest Conventions, reflects growing regional commitment to protecting minors in digital spaces.

- **Recent Legislative Reforms:**

  Some jurisdictions have taken meaningful steps to modernise their frameworks. North Macedonia's 2023 amendments explicitly criminalised stalking and harassment in both physical and digital spaces, a significant development aligned with Istanbul Convention obligations. Montenegro's introduction of Article 175a, specifically addressing the misuse of sexually explicit recordings (including deepfakes), represents an advanced legal response that few countries in the region currently match.

- **Integration of Gender-Based Violence Perspectives:**

  Several criminal codes recognise gender as an aggravating circumstance (e.g., Albania's Criminal Code, Article 50(j)), which enhances the gravity of offences committed with a gender-based motive. Kosovo's Article 248/A criminalising violence against women in public life—though not explicitly digital—can be interpreted to apply to online political harassment, signalling an awareness of the gendered dimensions of TF GBV.

Gaps and Challenges:

- **Absence of Explicit TF GBV Definitions:**

  None of the reviewed countries explicitly define 'technology-facilitated gender-based violence' as a standalone legal category. Instead, offences applicable to TF GBV are scattered across multiple general provisions. This fragmentation can result in uneven enforcement, inconsistent victim protection, and challenges in data collection, case identification, and specialised prosecution.

- **Limited Specificity for Digital Contexts:**

  Although general offences (e.g., harassment, threats) are adaptable to online environments, many criminal codes still lack provisions that directly reference digital or online behaviours. Only Montenegro (through Article 175a) and, more recently, North

Macedonia (through its amendments) have moved toward directly regulating online-specific abusive practices such as non-consensual sharing of manipulated content or cyberstalking.

- **Overreliance on Interpretation by Law Enforcement and Judiciary:**

  The reliance on broad, non-digital-specific legal provisions places a significant burden on police, prosecutors, and judges to interpret and apply the law to new forms of violence. Without specialised guidelines, training, and awareness, there is a risk of underreporting, misclassification of crimes, or failure to recognise the severity of technology-facilitated abuse.

- **Private Prosecution Requirements for Certain Offences:**

  In some jurisdictions, victims must initiate private legal action (e.g., Serbia for certain types of unauthorised image sharing), creating additional obstacles for survivors who may already face emotional, financial, and societal barriers to seeking justice.

- **Limited referral mechanisms, inadequate access to legal aid, and the absence of a consistent victim-centred approach** undermine effective multi-sectoral cooperation. These gaps are further compounded by weak regulatory frameworks for addressing the role and responsibility of online platforms in cases of TF GBV.

- **Limited Protection for Adult Victims of Image-Based Abuse:**

  While child sexual exploitation is relatively well covered, legal protections for adult victims of non-consensual intimate image distribution are weaker. Few laws explicitly criminalise the sharing of intimate images of adults without consent, unless they are prosecuted through more general privacy or data protection offences.

- **Insufficient Linkages Between Domestic Violence and TF GBV:**

  Although domestic violence laws exist across the region, only a few—such as Kosovo's Article 248—explicitly recognise that psychological and economic abuse can be perpetrated through technology. Notably, the Law on Protection from Domestic Violence in the Federation of BiH includes in its definition of violence the "misuse of photographs and recordings of a family member with the aim of discrediting or demeaning their personality." This provision is highly relevant to forms of Technology-Facilitated Gender-Based Violence (TF GBV), particularly image-based abuse, digital shaming, and the non-consensual sharing of intimate content within intimate or family relationships. However, many legal frameworks still lack specific recognition of digital coercive control, online surveillance, or financial abuse committed via digital means in domestic violence contexts.

2.4. Conclusion

In summary, while legislative advances are evident, especially in recent years, the legal frameworks addressing TF GBV across the Western Balkans remain incomplete. Countries have largely incorporated TF GBV-relevant offences through traditional criminal law instruments, without systematically codifying or conceptualising TF GBV as a specific phenomenon.

Across the Western Balkans, the legal landscape continues to fall short in effectively addressing online gender-based violence. While all countries in the region have adopted legal provisions that criminalise general forms of violence and harassment—primarily through criminal codes and domestic violence laws—TF GBV remains largely undefined and unrecognised as a distinct form of abuse. This lack of legal specificity contributes to widespread underreporting, limited prosecution, and institutional inaction.

The existing legal framework is often fragmented and outdated, forcing TF GBV cases to be processed under broad or ill-fitting legal categories such as defamation, unlawful data processing, coercion, or hate speech—though the latter is rarely applied in cases involving gender-based abuse. In Bosnia and Herzegovina, for example, none of the criminal codes at the Entity or Brčko District level explicitly address technology-facilitated violence. As a result, many cases are treated as misdemeanours or pursued through civil lawsuits, placing a disproportionate burden on survivors to navigate complicated legal procedures with minimal institutional support.

Even where legal provisions could potentially apply, implementation is often inconsistent. Law enforcement, prosecutors, and judges frequently lack the training, gender awareness, and digital competencies needed to recognise and respond to TF GBV effectively. Survivors commonly experience secondary victimisation, disbelief, or dismissal of the severity of online abuse.[10] Institutional responses remain largely reactive, with few proactive mechanisms in place for digital evidence collection, early intervention, or coordination with technology platforms.

Furthermore, survivors face significant barriers when seeking protection. Tools such as restraining orders, emergency measures, or content removal requests are difficult to obtain or enforce in online contexts. Laws designed to protect against domestic violence rarely apply when abuse occurs exclusively online or outside of intimate partner relationships, leaving victims of digital harassment, stalking, or non-consensual content sharing with little recourse. To achieve full alignment with international human rights standards, regional efforts should prioritise:

- Defining TF GBV explicitly in criminal codes,
- Strengthening protections for adult victims of online sexual violence,
- Expanding legal recognition of digital forms of coercive control and harassment,
- Training law enforcement and judiciary on recognising and effectively prosecuting TF GBV cases,
- Facilitating victim-centred, accessible reporting and prosecution mechanisms.

Harmonisation of laws and the development of specialised TF GBV provisions are essential steps toward providing comprehensive protection for victims in an increasingly digital world.

10 Halilović M.(2024) Riječi koje bole: Posljedice govora mržnje u Bosni i Hercegovini. Sarajevo: Atlantic Initiative. Council of Europe. Available at: https://atlantskainicijativa.org/rijeci-koje-bole-posljedice-govora-mrznje-u-bosni-i-hercegovini/

03 Mapping Challenges: Institutional and Civil Society Stakeholders Addressing Technology-Facilitated Gender-Based Violence (TF GBV)

3. Mapping Challenges: Institutional and Civil Society Stakeholders Addressing Technology-Facilitated Gender-Based Violence (TF GBV)

Technology-facilitated gender-based violence (TF GBV) is an increasingly pervasive form of abuse that intersects with deeply rooted gender inequalities and the rapid evolution of digital technologies. While legal and policy frameworks across the Western Balkans have begun to acknowledge aspects of this violence, significant gaps remain in institutional recognition, coordination, and response. Building on the legal and policy analysis presented in the previous Chapter, the following section shifts focus to the realities on the ground—mapping the actors, structures, and systemic challenges that shape the prevention, identification, and prosecution of TF GBV in the region.

The methodology for this Chapter combines desk research with semi-structured interviews to develop a comprehensive understanding of how TF GBV is addressed—or overlooked—within existing state and non-state systems. In light of the limited number of recorded prosecutions, particular attention was paid to examining how this form of violence is recognised in law enforcement and judicial practice, and whether institutional responses reflect the urgency and severity of the harm inflicted.

Country-specific reports, legal analyses, and assessments of victim services were reviewed to identify institutional roles, inter-agency coordination mechanisms, and the extent to which TF GBV is integrated into broader GBV response systems. A systematic stakeholder mapping was also conducted to identify key actors involved in addressing TF GBV, including government institutions (such as police, judiciary, prosecution, and gender equality mechanisms), regulatory and oversight bodies (including data protection agencies and media regulators), civil society and international organisations active in the field.

Insights from interviews with institutional representatives, civil society actors, and regional experts were essential to contextualizing the reality of TF GBV. These testimonies illuminated not only the structural and technical obstacles to effective response but also revealed the institutional blind spots, lack of accountability, and normalisation of digital violence that continue to undermine access to justice and protection for victims. Together, these findings provide a grounded, cross-sectoral analysis of the challenges that must be addressed to develop a more coordinated, victim-centred, and accountable regional response to TF GBV.

3.1. Widespread nature of TF GBV across the Western Balkans

This mapping reveals that technology-facilitated gender-based violence (TF GBV) is widespread and growing in scope and complexity across the Western Balkans. Its presence is consistently confirmed through available research,[11] reports, and expert testimonies from the region. Interviewees and research reports across the region consistently report a lack of disaggregated

11 UN Women (2023). The Dark Side of Digitalization: Technology-Facilitated Violence Against Women in Eastern Europe and Central Asia. UN Women.

data on technology-facilitated gender-based violence (TF GBV). As a result, it is not possible to monitor trends, track increases in reports or prosecutions, or understand the characteristics of affected victims. This data gap is further compounded by the absence of an intersectional approach in current reporting systems, limiting efforts to develop targeted and evidence-based responses.

A recent survey from North Macedonia found that the most commonly reported forms of TF GBV include online harassment (61%), sexist and gender-based hate speech (37.3%), online stalking (33%), and the spreading of altered or false information (23.24%). Facebook was identified as the most common platform where abuse occurred (75.7%), followed by Instagram (37.3%). The majority of perpetrators were unknown men (40.94%), although a significant number of cases involved known male individuals (31.5%).[12]

Albania has also experienced a general rise in digital crimes. A 2021 study by the Albanian Women Empowerment Network (AWEN) found that nearly one in ten respondents reported having been blackmailed with sexually explicit photos, videos, or other material at least once. The prevalence was significantly higher among women, with 12% of young women and almost 5% of young men reporting such experiences. Instagram was identified as the most frequently used platform by perpetrators (44%), followed by Facebook/Messenger (26%), while phone calls and messages were also commonly used tools. Contact was most often made via fake accounts (41%), though in 39% of cases, the blackmailer was someone known to the victim. In 69% of reported cases, the perpetrator was male. The most commonly misused intimate content included images (59%) and sexually explicit conversations (33%). Notably, in 39% of cases, the blackmail was linked to the perpetrator's intent to maintain or re-establish sexual relations, often following a breakup.[13]

Similarly, in Serbia, research shows that one in ten high school girls had private photos or videos—originally shared in confidence—published without their consent, illustrating the extent to which TF GBV is affecting young people.[14] Experts across the region consistently underline that this form of violence is not only prevalent but increasingly normalised, particularly in the absence of strong institutional responses. Together, these findings reflect a regional trend of persistent digital violence that is inadequately addressed by the legal, institutional, and educational systems in place.[15]

A participant from Albania shared that awareness of TF GBV significantly increased during the COVID-19 crisis, when online abuse escalated drastically. In Albania, shelters for GBV victims in some cases address TF GBV as part of the broader continuum of violence. They have identified cases involving teenage girls and adolescents who were either at risk of or directly subjected to online violence. The majority of these cases involved trafficking or exploitation, with perpetrators often use online platforms to initiate contact and groom victims. Increase of online violence in Albania was also discussed in Albania's GREVIO report.[16]

12 Chalovska Dimovska, N. (2024). Analysis of technology-facilitated gender-based violence. UNDP. Skopje

13 Dhëmbo, E. and Duci, V. (2021). *Intimate partner violence and sexual violence among young people in Albania*. AWEN. Available at: www.awenetwork.org/media/6488746058da0.pdf

14 Sanja Pavlovic, "Awareness, experiences and strategies of high school girls and boys for naming the problem of digital sexual and gender-based violence - report for Serbia", Autonomous Women's Centre

15 Milivojević, A. (2024). *Gender-based digital violence in Serbia: A review of trends.* SHARE Foundation.

16 GREVIO (2024). *Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) Baseline Evaluation Report: Albania.* Council of Europe.

Technology-facilitated gender-based violence (TF GBV) is found across the region in various forms, including online harassment, virtual mobbing, gender-based hate speech, image-based sexual abuse, deepfake pornography, cyberstalking, doxxing, slut-shaming, body-shaming, exclusion from online spaces, and online threats. These acts are often rooted in misogynistic, homophobic, or sexist beliefs and disproportionately target women, activists, journalists, and marginalised groups. In addition to these manifestations, TF GBV also occurs in the context of domestic violence and child sexual exploitation, where digital tools are used to control, intimidate, or further harm victims.[17]

While both men and women can be victims of technology-facilitated gender-based violence (TF GBV), women and girls are disproportionately affected. Such violence against them occurs far more frequently, reinforcing a broader environment in which discrimination, harassment, and abuse are normalised and sustained. The anonymity and lack of direct contact in TF GBV contribute to a false sense of impunity among perpetrators, who may not perceive their actions as genuine violence with real consequences. Victims, meanwhile, face risks of repeated abuse and privacy violations, as harmful content can be widely shared and amplified by others. This form of violence transcends physical boundaries, occurring at any time and in any space.[18]

The digital environment enables and amplifies gender-based violence through multiple interconnected factors. The anonymity and perceived impunity of online spaces often encourage perpetrators, while inadequate legal protections leave victims vulnerable. Digital platforms' algorithms can reinforce gender stereotypes and foster toxic subcultures rather than curb them. With minimal effort, perpetrators can target individuals across borders, extending harm beyond physical boundaries. As a result, deeply ingrained misogyny and discrimination are replicated and sustained in the digital sphere, reinforcing existing gender inequalities and patriarchal norms.[19] TF GBV has especially escalated during the COVID-19 crisis, as increased reliance on digital communication and prolonged periods of isolation created new opportunities for abuse.[20]

Technology-facilitated abuse is widely recognised by both research participants and regional studies[21] as a powerful tool used to silence individuals and suppress dissenting voices, posing a direct threat to freedom of expression and human rights advocacy. Women in public and political roles are disproportionately targeted by cyber violence and gendered disinformation campaigns aimed at discrediting, humiliating, intimidating, and ultimately silencing them across all spheres of public life. This targeted abuse undermines women's participation in democratic processes and erodes the integrity of governance structures.

They emphasised that TF GBV often **overlaps with, and reinforces, violence occurring in the physical world**. For instance, abusive partners may use digital tools to monitor, harass, or intimidate victims even after separation, while perpetrators of sexual harassment may extend their abuse through online stalking or the non-consensual sharing of images. These insights underline the **continuity between digital and** offline forms of abuse, and the urgent need for integrated approaches to prevention and protection.

17 Ibid.

18 Bukvić, A., Bukvić, A., & Vasić, M. (2023). Rodno zasnovano nasilje učinjeno upotrebom tehnologije. Alternativni centar za devojke.

19 Ibid.

20 UN Women, Facts and figures: Ending violence against women. Available online at: https://www.unwomen.org/en/what-we-do/ending-violence-against-women/facts-and-figures

21 DCAF. (2021). Cyber violence against women and girls in the Western Balkans: Selected case studies and a cybersecurity governance approach. The Geneva Centre for Security Sector Governance.

In recent years, the use of digital surveillance by intimate partners has emerged as a growing trend in Serbia and the broader Western Balkans region. Increasingly, partners secretly monitor phones and read private messages using commercially available spyware. According to media reports, software designed to access another person's phone can be purchased for as little as €85 per month, and thousands of individuals are reportedly using these tools. One such company, SpyTech, has sold over 3,500 new licenses and renewed more than 4,000 across Serbia, Montenegro, Bosnia and Herzegovina, and Croatia. These programmes allow users to listen to calls, read messages from chat applications, and even activate cameras remotely. The intentional use of such digital technologies to stalk, monitor, or control women causes significant psychological harm, including fear, anxiety, and emotional distress.[22]

Despite the clear violation of privacy and the significant harm inflicted, interviewed experts argued that institutional responses to technology-facilitated gender-based violence (TF GBV) remain inadequate across the region. This form of violence remains insufficiently recognised or addressed in either law or practice, leaving victims without meaningful avenues for protection or redress.

The mental health consequences of technology-facilitated violence, including gender-based violence (GBV), are severe and often long-lasting. Survivors frequently report anxiety, emotional distress, behavioural changes, as well as physical symptoms such as insomnia and somatic complaints. The psychological impact is further intensified by the public and persistent nature of digital abuse. Sexist hate speech, misogyny, and threats experienced by women activists, LGBT+ activists, and journalists have a ripple effect on entire communities. Examples from Bosnia and Herzegovina show that people often change their behaviour and daily routines, and avoid certain places due to the fear and intimidation caused by online GBV.[23]

Women in Public Life Targeted by Technology-Facilitated Gender-Based Violence

In the Western Balkans, female journalists, academics, and public figures who are vocal in criticising the ruling or opposition parties, religious institutions, or address sensitive topics such as war crimes, frequently face coordinated online harassment. This includes hate speech, misogynistic threats, doxxing, and smear campaigns, often amplified by media outlets aligned with political interests.[24] At the same time, shrinking civic space and the rise of anti-gender movements have led to increasingly frequent attacks on activists and human rights defenders across the region.[25] Experts from across the region shared examples of journalists and activists who were targeted for publicly speaking out on issues such as women's rights, LGBTQ+ rights, and corruption. These online attacks tend to intensify around events like PRIDE or other important public events, and most often take the form of threats, intimidation, or misogynistic abuse.

Violence against women in politics is a distinct form of gender-based violence that targets women because of their gender and seeks to deter or punish them for participating in public and political

22 Milivojević, A. (2024). Rodno zasnovano digitalno nasilje u Srbiji: Pregled trendova. SHARE Fondacija.

23 Halilović, M. (2024). *Riječi koje bole: Posljedice govora mržnje u Bosni i Hercegovini.* Vijeće Europe. Available at: https://www.mhrr.gov.ba/ljudska_prava/Rijeci%20koje%20bole%20-%20Posljedice%20govora%20mrznje%20u%20Bosni%20i%20Hercegovini.pdf

24 Sarikakis, K., Gudkova, O., Buvač, N., Marinković, A., & Ametova, G. (2025). *Giving up on the law? The disconnect of hate speech policy and female journalists' experiences.* Feminist Media Studies. https://doi.org/10.1080/14680777.2025.2505182

25 Kvinna till Kvinna Foundation (2023). *Women's Rights in Western Balkans: Women in Politics, Gender-Based Violence and Security for Women Human Rights Defenders in Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia and Serbia.* Kvinna till Kvinna Foundation.

life. While both men and women may experience hostility in politics, the violence directed at women is shaped by patriarchal norms and often takes gender-specific forms, including sexist threats, online harassment, sexual violence, and defamation. These acts are not only aimed at individual women but are also intended to discourage women's political engagement more broadly and to reinforce traditional gender roles. This issue is formally recognised in the Note by the Secretary-General on Violence against Women in Politics, submitted under Item 29 of the provisional agenda during the Seventy-third session of the UN General Assembly, which emphasises that such violence seriously hampers women's equal participation in political life and the exercise of their human rights.[26]

Findings from the OSCE in Serbia show that women in politics are frequently targeted with digital violence, including online harassment, stalking, and abuse via social media, internet portals, and politically aligned media. Tabloid outlets and platforms controlled by political actors often act as tools of psychological violence, shifting narratives depending on party leadership's stance toward particular women. Perpetrators include colleagues from their own party, superiors, political opponents, journalists, and in some cases entire parties or organised groups. While most perpetrators are men, women can also be involved. Citizens often join in through abusive comments online. Partisan protection is inconsistent and often conditional on loyalty. Even networks like the Women's Parliamentary Network face obstacles due to unclear procedures and competing pressures between partisan loyalty and gender solidarity. These patterns highlight how digital tools are misused to undermine women's political participation and reinforce structural inequality.[27]

In Montenegro, online violence against women in politics is increasingly recognised as a widespread issue, closely linked to the rise of digital media and social platforms. According to research by the Women's Political Network, one in four women politicians (26.6%) reported experiencing some form of online violence. This includes harassment or threatening emails, abusive text messages, derogatory blog posts, or the unauthorised distribution of images or video clips intended to humiliate or discredit them. The pervasive reach of the internet and the constant availability of mobile communication technologies have only amplified this form of gender-based violence, turning online spaces into key arenas for political intimidation and silencing of women.[28]

Interviews, supported by findings from other studies,[29] reveal that women activists, journalists, and public figures are frequent targets of sexist hate speech, threats, and misogyny—demonstrating how digital spaces are often weaponised to silence and intimidate those who challenge the status quo. Female journalists, in particular, are disproportionately subjected to cyber violence and digital attacks compared to their male counterparts. Regional evidence further underscores the profound impact of such abuse on women human rights defenders and women's organisations, whose credibility, safety, and ability to operate effectively are often undermined by sustained digital harassment and threats.

26 United Nations (2018), *Violence against women in politics: Report of the Secretary-General.* Seventy-third session of the General Assembly, Item 29 of the provisional agenda: Advancement of Women. A/73/301. Available at: https://undocs.org/en/A/73/301

27 Babović, M., Milinkov, S., Srdić, M. & Stepanov, B. (2021). *Nasilje nad političarkama u Srbiji: žene u politici na tromeđi roda, moći i političke kulture – Kratki izveštaj.* OSCE Mission to Serbia. Available at: https://www.osce.org/files/f/documents/2/8/502194.pdf

28 Vuković, N. & Raščanin, I. (2021). *Istraživanje o nasilju nad ženama u politici u Crnoj Gori. Podgorica: UNDP Montenegro*. Available at: https://www.undp.org/sites/g/files/zskgke326/files/migration/eurasia/UNDP-mne-istrazivanje-zeneupolitici-2021.pdf

29 DCAF. (2021). *Cyber Violence against Women and Girls in the Western Balkans: Selected Case Studies and a Cybersecurity Governance Approach.* Geneva Centre for Security Sector Governance. Available at: https://www.dcaf.ch/sites/default/files/publications/documents/CyberVAWG_in_WB.pdf

One of the participants from Serbia shared that even individuals working on femicide are frequently subjected to online hate. She explained that femicide cases often trigger a wave of hostile messages targeting feminists and activists, with comments such as: *"The same should happen to you," "Women like you provoke this," "Stop calling this femicide,"* and *"She brought it onto herself."* These reactions reflect deeply entrenched misogyny and widespread victim-blaming attitudes, which not only silence advocacy but also normalise violence against women in digital spaces.

Yet, despite the severity and lasting impact of TF GBV, institutions continue to underestimate its seriousness. Responses are often marked by a lack of appropriate response, insufficient prevention measures, and weak or non-existent support services, further isolating survivors and reinforcing patterns of impunity.[30]

3.2. Stakeholder Landscape in Addressing TF GBV Across the Western Balkans

In each of the Western Balkan countries, a variety of governmental and non-governmental stakeholders are involved in addressing technology-facilitated gender-based violence (TF GBV). While structures vary in terms of resources, mandate, and coordination, a shared pattern of fragmented responsibilities and underdeveloped specialisation emerges.

Gender Equality Mechanisms: All Western Balkans countries have gender equality agencies, departments, or offices either within ministries or acting as independent bodies. These institutions are typically mandated to coordinate national gender equality policy and monitor its implementation. However, their role in addressing TF GBV remains underutilised. While some have supported awareness campaigns or contributed to policy advocacy, few have systematically integrated TF GBV into national gender equality strategies or coordinated institutional responses across sectors.

Prosecutor's Offices: Public prosecutors across the region play a central role in charging and prosecuting TF GBV cases. However, as noted in interviews, many prosecutors lack specific training on the gendered aspects of digital violence, and their interpretation of legal provisions is often narrowly focused on conventional forms of endangerment or violence. In several cases, jurisdictional gaps between local prosecutors and high-tech crime units have resulted in delays, dismissals, or uncertainty over how to proceed.

Ombudsperson Institutions: Ombudsperson offices in countries such as Albania, Kosovo, Bosnia and Herzegovina, Serbia, Montenegro, and North Macedonia are legally tasked with safeguarding citizens' rights and addressing discrimination. They are increasingly recognised as important actors in the broader landscape of GBV prevention, but their engagement on TF GBV remains limited. Expanding their mandate to include digital rights and online violence could enhance accountability and victim protection.

Free Legal Aid Providers: Access to justice for TF GBV victims is frequently undermined by legal complexity and financial barriers. Free legal aid services exist in all Western Balkan countries, but their capacity to support TF GBV cases varies significantly. While legal professionals may assist in cases involving defamation, privacy breaches, or online harassment, few have been trained in the digital dynamics of GBV. In addition, access to free legal aid is often constrained

30 Bukvić, A., & Vasić, M. (2023). Rodno zasnovano nasilje učinjeno upotrebom tehnologije. Alternativni centar za devojke. Available at: https://altgirls.org/wp-content/uploads/2024/04/Rodno-zasnovano-nasilje-WEB-A5-1.pdf

by eligibility requirements such as low-income status or status of a victim of domestic violence. Civil society organisations often fill these gaps by offering legal aid tailored to the needs of survivors, but their services are limited in reach and sustainability.

Civil Society and NGOs: Civil society organisations remain the most dynamic stakeholders addressing TF GBV. Across the region, NGOs provide victim support, advocate for legal changes, lead awareness raising campaigns, conduct research, and engage in capacity building. However, their work is often project-based and dependent on international donors. Without state commitment to institutionalising these efforts, civil society's impact will remain constrained.

Multisectoral mechanisms for addressing domestic violence are present to varying degrees across the Western Balkans. However, they are generally not sufficiently prepared to respond to technology-facilitated gender-based violence (TF GBV). A participant from Albania noted that in some areas these mechanisms function well and also cover TF GBV cases. Still, responsibility for TF GBV most often lies with cybercrime police units. According to participants, these units do not have the necessary resources, training, or institutional support to deal with the growing complexity of such cases. Their focus is often limited to crimes involving children in online spaces, and they are not actively involved in multisectoral coordination. Similar concerns have been identified in a recent regional study[31] by UN Women.

Law Enforcement and Cybercrime Units: In most countries, cybercrime units exist within law enforcement structures, but their engagement with TF GBV cases is often limited by institutional mandates and their overwhelming focus on financial or organised crime. There is a need to equip these units with gender-sensitive protocols, training, and forensic tools to address TF GBV more effectively.

International Organisations: International actors such as UNDP, UNFPA, UN Women, OSCE, Save the Children and UNICEF play a vital role in supporting national efforts to combat TF GBV in all six Western Balkan countries. Their contributions include funding pilot projects, supporting legal and policy reforms, training professionals, and conducting public awareness campaigns. These organisations have helped catalyse recognition of TF GBV and have been instrumental in bridging gaps between civil society and state institutions. However, the sustainability of their interventions depends heavily on whether national authorities assume ownership and institutionalise these efforts.

The Western Balkans region is served by a diverse range of internet service providers, including both state-owned and private companies such as BH Telecom, Mtel, and Telemach in Bosnia and Herzegovina; Telekom Srbija and SBB in Serbia; Crnogorski Telekom and Mtel Crna Gora in Montenegro; Makedonski Telekom and A1 in North Macedonia; IPKO and Telekomi i Kosovës in Kosovo; and Vodafone Albania and ALBtelecom in Albania. These ISPs have a critical role to play in the prevention and mitigation of TF GBV. Their responsibilities could include implementing stronger privacy and security measures for users, responding swiftly to requests for content removal and evidence preservation, collaborating with law enforcement and civil society on

31 UN Women (2023). The Dark Side of Digitalization: Technology-Facilitated Violence Against Women in Eastern Europe and Central Asia. UN Women. Available at: https://eca.unwomen.org/en/digital-library/publications/2023/11/the-dark-side-of-digitalization-technology-facilitated-violence-against-women-in-eastern-europe-and-central-asia

awareness campaigns, and providing user-friendly reporting tools for online abuse. Additionally, internet service providers can support educational initiatives that promote digital safety and help create a safer online environment, particularly for women and marginalised groups.

Organisations such as the National Center for Missing and Exploited Children (NCMEC), INTERPOL, and Europol play vital roles in addressing technology-facilitated gender-based violence (TF GBV), particularly in cases with cross-border elements. NCMEC, while primarily focused on protecting children, operates the CyberTipline and collaborates with technology companies and law enforcement to identify, report, and remove exploitative content. This model offers useful lessons for strengthening responses to TF GBV more broadly. INTERPOL supports member states, including those in the Western Balkans, by coordinating international information sharing, providing training, and facilitating joint investigations into online abuse and cyberstalking. Similarly, Europol's European Cybercrime Centre (EC3) enhances cooperation on digital crimes by offering technical and analytical support to national law enforcement and by fostering collaboration with internet service providers and online platforms. These international bodies demonstrate how centralised reporting systems, cross-jurisdictional coordination, and specialised cyber expertise can significantly improve national strategies to prevent and respond to TF GBV.

Data Protection Authorities and Regulatory Agencies: Each Western Balkan country has an independent data protection authority responsible for overseeing the implementation of personal data protection laws and ensuring compliance with data protection frameworks. These include:

- Albania: Information and Data Protection Commissioner
- North Macedonia: Personal Data Protection Agency
- Serbia: Commissioner for Information of Public Importance and Personal Data Protection
- Montenegro: Agency for Personal Data Protection and Free Access to Information
- Bosnia and Herzegovina: Personal Data Protection Agency
- Kosovo: Information and Privacy Agency

Although their potential role in addressing TF GBV is significant, especially in cases involving doxxing, data breaches, or the unauthorised sharing of personal information, they are rarely integrated into national GBV prevention and response strategies. Greater collaboration between data protection authorities and GBV actors could enhance digital safety and accountability.

Media Regulatory Authorities: Each country in the region also has media regulatory bodies in place. These include:

- Albania: Audiovisual Media Authority
- Bosnia and Herzegovina: Communications Regulatory Agency
- North Macedonia: Agency for Audio and Audiovisual Media Services
- Serbia: Regulatory Authority for Electronic Media
- Montenegro: Agency for Electronic Media
- Kosovo: Independent Media Commission

These institutions are responsible for monitoring broadcast content, ensuring media standards, and protecting against hate speech and harmful content. However, their role in addressing TF GBV, particularly when abuse occurs through media channels or public commentary, remains underdeveloped. Strengthening their mandate and cooperation with GBV actors could be an important step toward tackling online misogyny and media-enabled abuse.

Stakeholders Focused on Child Protection and TF GBV

Child protection stakeholders are essential in addressing technology-facilitated gender-based violence (TF GBV) against minors. These include Social Welfare Centres, which typically act as the primary responders in cases involving children. Educational institutions, particularly schools, along with school psychologists and educators, are also mandated to intervene when TF GBV occurs among peers. However, their response is often inconsistent due to a lack of training and clear guidance. Ombudspersons for Children tend to play an important advocacy role, but they are not always directly involved in individual cases. Oversight is provided by child protection units within Ministries of Social Policy and dedicated child welfare agencies, though these institutions are often underresourced. Specialised NGOs, such as Save the Children and UNICEF country offices, are critical actors in both policy advocacy and providing support to victims.

According to participants, children often receive stronger institutional protection from TF GBV than adults, particularly in cases involving organised exploitation or online networks. However, when individual incidents occur, responses are far less systematic. There is a pressing need for clear reporting procedures, improved intersectoral coordination, digital literacy education in schools, and accessible psychosocial support tailored to young people. Given the specific vulnerabilities of children in digital environments, targeted safeguards must be embedded within broader TF GBV prevention and response systems.

3.3. Institutional Gaps and Challenges in Addressing TF GBV

Technology-facilitated gender-based violence (TF GBV) is a rapidly growing yet underrecognised threat across the Western Balkans. A 2020 study on gender-based digital violence conducted by the Autonomous Women's Centre found that more than half of high school girls in Serbia had been exposed to online comments of a sexual nature, and one in ten experienced having their private photos or videos, originally sent to someone in confidence, shared publicly.[32] While digital technologies have expanded the means of expression, connection, and advocacy, they have also introduced new dimensions of harm especially for women, girls and children. From online stalking and harassment to the non-consensual sharing of intimate images, TF GBV manifests in a range of behaviours that often mirror, reinforce, or escalate offline abuse.

What emerges from this analysis is a landscape of fragmented and reactive systems—ones that have not yet adapted to the complex realities of digital violence. While civil society organisations play a critical role in offering support and pushing for reform, state institutions remain largely unprepared. Legal frameworks across the region are incomplete or inconsistently applied, frontline workers often lack the training or tools to respond effectively, and victims are frequently

32 Pavlović, S. (2020). Svest, iskustva i strategije srednjoškolki i srednjoškolaca za imenovanje problema digitalnog seksualnog i rodno zasnovanog nasilja – izveštaj za Srbiju. Autonomni ženski centar, jun 2020. Available at: https://www.womenngo.org.rs/images/publikacije-dp/2020/Digitalno_nasilje_i_mladi-izvestaj_za_Srbiju.pdf

blamed, disbelieved, or ignored. Addressing TF GBV requires not only legal reform, but also a fundamental shift in institutional attitudes, public awareness, and intersectoral cooperation.

This section provides a regional analysis of the systemic, institutional, and legal barriers to preventing and addressing TF GBV in Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia. Drawing on interviews with experts, practitioners, and civil society representatives, it highlights the persistence of gender bias in institutional responses, the absence of standardised procedures, the lack of training and digital forensics capacity, and the limited access to victim-centred support services. In doing so, it also identifies both gaps and emerging examples of good practice. The following Chapter outlines the most pressing challenges identified across the region and provides concrete examples of how these challenges affect the protection of victims, prosecution of perpetrators, and overall state accountability in combating digital gender-based violence.

1. Gaps in Legislative Alignment and the Need for Comprehensive Legal Reform

Legal frameworks across the Western Balkans remain insufficient to address the complexities of technology-facilitated gender-based violence. Participants across all countries emphasised that online forms of abuse are poorly defined in national legislation and that legal systems have been slow to adapt to the evolving nature of digital harm. Existing criminal codes often fail to incorporate provisions from international human rights conventions or the EU Directive on violence against women, leaving significant legal gaps. As a result, victims are frequently left without protection or access to justice, and perpetrators operate with relative impunity.

Participants from Bosnia and Herzegovina note that legal amendments do not keep pace with the real life. “We live in times when GBV is developing into new forms, but criminal legislation is so slow to change,” one expert stressed. This disconnects between legal frameworks and the lived realities of victims severely undermines institutional responsiveness.

In Kosovo, the Kosovo Women’s Network (KWN) opposed recent amendments to the Criminal Code, arguing that they are insufficient for addressing TF GBV. KWN proposed a separate article titled Gender Based Cyber Violence, outlining specific offences such as cyberstalking, doxxing, and deepfake pornography. The proposal also included expanded definitions of sexual harassment and mandatory offender rehabilitation programs. Additionally, KWN called for incorporating aggravating circumstances as outlined in the EU Directive on Violence Against Women, such as attacks on children, public figures, and journalists. Without such provisions, Kosovo cannot formulate a comprehensive national strategy or align its laws with EU standards.

2. Institutional Inertia and Unequal Protection

Experts across the region reported that institutional responses to TF GBV are still grounded in outdated perceptions of violence. One expert from Serbia described how professionals such as journalists and even prosecutors are left unprotected. She cited the case of journalist Jovana Gligorijević,[33] who endured an intense wave of online abuse, including threats and doxxing, without any institutional support. Similarly, a female prosecutor was harassed by the man she was prosecuting for domestic violence. He published her photos online and encouraged public threats against

33 Milivojević, A. (2024). Gender based digital violence in Serbia: A review of trends. SHARE Foundation. Available at: https://sharefoundation.info/wp-content/uploads/Gender-Based-Digital-Violence-in-Serbia.pdf

her. Yet, the High-Tech Crime Unit downplayed the situation, arguing that there was no clear threat to life or bodily integrity.

The persistence of violence against women in politics, including in online spaces, has a chilling effect on democratic participation, reinforces gender inequalities, and signals to the public that women's leadership is unwelcome or illegitimate. The problem is often normalised, underreported, and underestimated, especially in contexts where patriarchal attitudes dominate public discourse. Women who speak out or challenge dominant narratives are disproportionately subjected to threats, sexualised attacks, and smear campaigns, frequently amplified through digital platforms. To address this, states must adopt and enforce laws and policies that explicitly recognise and prohibit political violence against women, and ensure adequate protection mechanisms and accountability measures. This includes stronger regulation of online platforms, gender-sensitive training for public institutions and media, and public campaigns to challenge the cultural acceptance of violence against women in public life.

As the expert noted, institutions narrowly interpret the legal threshold for criminal endangerment, often refusing to consider the broader context or the intent behind such threats. The expert criticised this literal approach, calling it deeply disconnected from the lived experiences of victims. *"Perpetrators have advanced in TF GBV, but prosecutors have not,"* she said. A participant from Albania noted that legal proceedings for TF GBV remain inconsistent and vary depending on the severity of the violence, the type of technology used, and the broader context in which the abuse occurred.

These blind spots are not just institutional but structural. In cases involving male politicians or powerful figures, law enforcement and prosecutors respond swiftly. But when the victim is a woman, particularly from a marginalised background, responses are delayed or dismissed.

3. Discriminatory Institutional Practices and Victim Blaming

Across the region, victim-survivor blaming remains a systemic barrier. Institutions often scrutinise the behaviour of the victim rather than the perpetrator. Questions like "Why did she send those pictures?" or "Why was she speaking to an adult man?" are common. As an expert from Kosovo explained, *"Many women think if they send a photo to a boyfriend, they don't have the right to complain when he makes it public."*

In Albania also awareness of TF GBV remains low, and such cases are significantly underreported. Many girls affected by online harassment are afraid of being judged by their peers, communities, or schools, which discourages them from seeking help. Fear of stigma and reputational harm often silences victims in Albania. There is an urgent need for broader awareness-raising efforts to educate young people, families, and professionals about the risks of TF GBV, how to report it, and how to access support.

This culture of blame contributes significantly to underreporting, particularly among survivors who fear they will not be believed or taken seriously. In rural areas, where patriarchal norms tend to be more entrenched, the likelihood of reporting is even lower. Marginalised groups, including the LGBT+ community, face additional barriers. Interviewees noted that LGBT+ individuals are frequently targeted by TF GBV, yet responses from law enforcement often mirror prejudice. Some officials question why they 'need to be so public' about their identity, organise pride events, or express their sexual orientation, implying that such visibility invites online har-

assment rather than recognising it as a violation of rights. This pattern can largely be attributed to the lack of adequate and gender-sensitive training for law enforcement personnel, as well as the absence of clear measures to prevent secondary victimisation. Without such training, many officers lack the awareness or skills needed to respond appropriately to survivors of technology-facilitated gender-based violence.

Participants from Albania stressed the importance of the role of media in reinforcing harmful gender stereotypes and contributing to the normalisation of technology-facilitated gender-based violence (TF GBV). They noted that the media's coverage of TF GBV cases is often problematic and lacking in sensitivity. While some civil society organisations have implemented trainings for journalists to improve their reporting on gender-based violence, these efforts face persistent challenges. Public perception is greatly influenced by the way stories are presented in the media, although the majority of media sources continue to be primarily motivated by audience reach or political agendas. As a result, sensationalist reporting frequently prevails over responsible journalism, undermining public awareness efforts and contributing to a culture that downplays the severity of TF GBV.

An Albanian participant highlighted that media regulatory agencies often lack awareness of the impact of language used in reporting, particularly in cases involving domestic violence or harassment. Numerous online portals frequently publish sensitive information without ethical oversight, which causes further psychological harm to victims. The spread of unverified content across unregulated digital platforms allows harmful narratives and misinformation to circulate quickly. In many instances, especially those involving women and children, victims become targets of public attacks and hate speech. Although this concern was raised in the context of Albania, similar patterns were observed in other countries in the region. Mechanisms to prevent or address these violations are generally weak or lacking.

Interviewees across the region, particularly in Kosovo and Montenegro, also observed that young women have begun to internalise certain forms of TF GBV. Insults, slut-shaming, and gaslighting are often perceived as normal aspects of digital communication. Only extreme forms, such as the non-consensual distribution of intimate images, are widely recognised as abuse. This normalisation discourages reporting and fosters self-blame among survivors, many of whom are unaware that they have a right to protection. In strongly patriarchal environments, fear of stigma, shame, and not being believed further deters victims from seeking help.

Victims of TF GBV in Montenegro often face delays, lack of information, and procedural complexity. The need for enhanced institutional training, digital forensic capability, and interagency coordination is clear. Establishing standardised procedures and integrating TF GBV more explicitly into national laws and strategic frameworks will be essential to improving protection and accountability.

This discrepancy in response also reflects deeper inequalities in how victims are perceived and treated. Girls and women from marginalised communities, including Romani girls, drug users, and those living in poverty, face additional layers of discrimination. Their cases are less likely to be taken seriously by institutions and more likely to be met with stigma, disbelief, or outright blame. This results in significant disparities in protection, justice, and access to support services. Such unequal treatment reveals an implicit hierarchy of victimhood, where institutional concern

is disproportionately allocated based on the victim's age, background, and perceived social worth. While children may prompt a stronger institutional response, adult women, particularly those from marginalised communities, remain largely unprotected. The consequence is a fragmented and discriminatory system that fails to address the full scope of TF GBV, perpetuating impunity and leaving many victims without recourse.

4. Jurisdictional Avoidance and Fragmented Responsibility

In Serbia, practitioners noted that local prosecutors often refer TF GBV cases to the High-Tech Crime Unit. However, the Unit often dismisses these cases, claiming they are continuations of offline abuse and should remain under local jurisdiction. The result is a cycle of referrals with no one taking responsibility. Even when abuse is exclusively digital, such as in ongoing divorce cases, prosecutors may downgrade the offence to a misdemeanour.

One case involved a doctor who relocated after her abusive ex-husband continued to harass her online. Although both parties were questioned, the case stalled for months. No charges were filed, and the victim was left without protection, still living only 150 km from the perpetrator and in fear that he will harm her.

DELAYED INSTITUTIONAL RESPONSE TO TF GBV IN MONTENEGRO

In Montenegro, prosecutors and law enforcement frequently deal with TF GBV primarily through cases involving social media messages or mobile phone communications. These typically include threats to publish explicit content or direct harassment through vulgar messages. While some incidents reach the level of criminal offences, many are classified as misdemeanours, complicating victim access to justice. As one prosecutor noted, the line between a criminal offence and a misdemeanour in online violence is often a very thin one.

There is a reliance on the High-Tech Crime Unit for tracing IP addresses and gathering digital evidence. However, the process is perceived as slow and procedurally cumbersome, contributing to delays in prosecution. Prosecutors must provide specific legal qualifications for cases, which are then used by the cybercrime unit to determine investigative actions. In high-risk cases, including threats to journalists and political figures, handling is reportedly faster, though the systemic bottlenecks persist.

Most TF GBV offenses, such as sexual harassment and unauthorised sharing of private photos, are prosecuted through private lawsuits unless aggravating circumstances apply (e.g., the victim-survivor is a child, pregnant woman, or person with a disability). This places a significant burden on the victim-survivor to pursue justice independently.

There have been successful prosecutions in high-profile cases involving female journalists and politicians, particularly when threats were made publicly. However, systemic challenges remain, especially in distinguishing between criminal and misdemeanour offences, and in ensuring timely action.

Across the region, police capacity to address TF GBV remains limited. According to one of the participants from Albania, law enforcement officers generally lack the necessary knowledge and show little interest in engaging with the issue. A new unit by the name of the National Authority on Cyber Security has been established within the Police Directorate and is seen as a positive development, but it still falls short of meeting the needs on the ground. In smaller municipalities with lesser population, often there are only one or two police officers available, and none specifically trained to handle TF GBV. Most cases are referred to Tirana, which reflects the lack of trained professionals, specialised knowledge, and appropriate equipment at the local level. This results in a significant gap in timely and effective protection for victims-survivors.

5. Data Gaps and Lack of Monitoring

Across the Western Balkans, institutions lack reliable and disaggregated data on TF GBV. Ministries of interior, prosecutor's offices, and statistical agencies often collect data on broader categories such as domestic violence or cybercrime, but do not identify or track TF GBV specifically. As a result, there is no clear understanding of how widespread or severe this form of violence is, or who is the most affected. The absence of intersectional data further limits insight into how TF GBV impacts women from minority or marginalised communities.

When institutions are asked to provide statistics, many simply respond they "have none," reflecting a systemic failure to prioritise data collection, monitoring, and accountability. This absence of data severely limits informed policymaking, budget planning, and the ability to assess the effectiveness of interventions. At the same time, prevalence studies[34] reveal alarming rates of technology-facilitated gender-based violence across the region. Among women who reported experiencing such violence, the most common forms include receiving unwanted or offensive messages (39.7%), inappropriate sexual advances or content on social media (30%), and the hacking of personal accounts or web pages (25.4%). While 40.4% of women experienced this type of violence at least once, one in seven reported being subjected on a daily or weekly basis.

6. Technical and Capacity Gaps in Law Enforcement

In Bosnia and Herzegovina, law enforcement acknowledges that they often rely on open-source tools for collecting digital evidence due to the lack of licenses for professional forensic software. Digital evidence is frequently gathered through screenshots, which may not meet evidentiary standards in court. Harmful content is often deleted by perpetrators before it can be preserved, and there is no real-time system for evidence preservation.

Despite police instructions to "secure" digital content, officers face significant human and technical limitations. One expert in BiH noted that up to 20 reports a day may be received, many

34 UN Women (2023). The Dark Side of Digitalization: Technology-Facilitated Violence Against Women in Eastern Europe and Central Asia. UN Women.

vague or anonymised, stretching the already scarce resources. Further, there are no trained officers in cybercrime units certified to work with minors, despite clear legal obligations under the Law on Juvenile Protection.

Digital evidence, particularly screenshots, is commonly submitted, but their evidentiary value depends on verification through forensic analysis. In cases involving children or especially vulnerable victims, prosecutors have more discretion to proceed ex officio.

7. Inconsistent Cooperation with Online Platforms

Cooperation with platforms like META (Facebook and Instagram owner) was described as slow and red-taped. Requests for content removal or user data must go through court orders, translations, and legal channels, taking five to ten days or longer. Even then, platforms often reject requests unless the offence involves terrorism or child sexual exploitation.

A police expert from Bosnia and Herzegovina highlighted that statements like "You'll see once that day comes" are often dismissed by institutions as too vague to constitute a real threat, unless there is an explicit plan to cause physical harm. This reflects a broader legal and procedural challenge when addressing TF GBV. Content that is deeply offensive, sexist, or misogynistic may not meet the threshold for criminal prosecution, especially on platforms governed by the U.S. law, where such speech may be protected under freedom of expression. As a result, many harmful acts are not addressed in practice, reinforcing a culture of impunity for online gender-based abuse.

Participants from across the region shared that procedures for working with platforms such as Facebook and Instagram are not formalised but rely on ad hoc communications through Interpol and official requests. While such routes can yield results in high-risk situations, the lack of standardised protocols makes response times unpredictable and inconsistent.

A participant from Albania noted that cooperation with Meta remains unclear, and raised concerns about recent changes to the company's content moderation policies. Following shifts in the U.S. administration, Meta reportedly reduced the number of offices responsible for content oversight. In early 2024, announcements regarding the removal of certain moderation filters raised concern among civil society organisations in Albania. They expressed fears that these changes could lead to an increase in hate speech and allow online platforms to disseminate harmful narratives with fewer restrictions, potentially exacerbating the risks of TF GBV.

8. Absence of Standard Operating Procedures (SOPs) and Institutional Ownership

Across the region, SOPs for TF GBV are either inexistent or treated as non-binding. There have been efforts by NGOs, such as Save the Children, to create SOPs in BiH but these were ultimately not adopted. In Serbia, one former official recalled how she distributed a guidance manual to colleagues, only for it to be ignored.

Without binding protocols, police and prosecutors rely on informal practices that vary by jurisdiction. Responsibility is often unclear, whether TF GBV should be handled by cybercrime, domestic violence, or general criminal units. As one expert bluntly stated: "No one really cares about this topic."

Despite the absence of written protocols for platform cooperation and digital case handling, Montenegrin prosecutors operate within a framework of discretionary practice guided by national and institutional instructions. However, this leaves room for inconsistency and inadequate responses, especially in lower-profile cases.

CASE STUDY: KOSOVO – FRAGMENTATION, CROSS-BORDER GAPS, AND INSTITUTIONAL INERTIA

In a case supported by the Kosovo Women's Network (KWN), a survivor of technology-facilitated gender-based violence (TF GBV) faced a complex maze of legal and jurisdictional obstacles that revealed the challenges of cross-border digital abuse in the Western Balkans.

After ending a relationship with a man from Montenegro, a woman living in Kosovo was subjected to a deeply violating form of retaliation. The perpetrator shared intimate photos and videos of her with her husband and later uploaded them to pornographic websites. Devastated and unsure where to turn, the woman contacted KWN for support. The organisation explained the legal options available and assisted in seeking protection—but when she approached Kosovo's institutions, officials told her that because the perpetrator lived in Montenegro, she would need to file a complaint there.

Left with little support at home, the woman travelled to Montenegro and filed a report. The police there responded quickly: the perpetrator was arrested, his devices were confiscated, and he was detained for six months. However, after his release, he resumed threatening her. With persistence and help from KWN, the survivor eventually succeeded in having the online content removed. Yet the experience highlighted major institutional gaps: minimal cross-border coordination, weak engagement from Kosovo's authorities, and no clear pathway for victims of international digital abuse to seek justice or protection.

A second case further illustrates these systemic weaknesses. In the notorious AlbKings Telegram group, nude photos of women—along with their names and contact information—were circulated in a form of digital exploitation that pressured them to engage in sexual acts for money. Despite repeated shutdowns, the group kept resurfacing. The main administrator was briefly arrested but reopened the group upon release and even issued threats against a well-known Kosovar woman. Only after she filed a report was he detained again.

While police authorities claim to have strong cooperation with platforms like META, NGOs and women's rights organisations report otherwise. Content removal procedures remain slow and largely ineffective without formal court orders. In the meantime, victims are left exposed, traumatised, and without meaningful institutional support.

These cases from Kosovo underscore critical weaknesses in the regional response to TF GBV—particularly when the abuse goes beyond borders. Survivors face a maze of disconnected systems, minimal victim-centred protection, and prolonged exposure to harm, even after taking legal action. The lack of coordination and slow institutional response continue to leave women vulnerable in the face of digital violence.

9. Strained Service Delivery and Overdependence on Civil Society

Across the region, support systems for TF GBV victims-survivors are fragmented and uneven. Public services, particularly Social Welfare Centres, are often described as ineffective or overwhelmed. In Serbia, social protection workers are frequently on strike, protesting years of institutional neglect.

Mental health services are unequally distributed. While some urban centres have access to specialised trauma support (e.g., Mental Health Institute in Belgrade), adult women face long waitlists, stigma, and underresourced care. In smaller towns, services, if any, are inadequate.

In all Western Balkan countries, support for victims-survivors of gender-based violence (GBV) is largely provided through partnerships with civil society organisations (CSOs), offering legal aid and psychological support. However, formalised institutional structures specifically designed to support victims-survivors of technology-facilitated gender-based violence (TF GBV) are lacking.

CSOs continue to fill this gap, despite limited resources. In Serbia, organisations such as the Autonomous Women's Center and ATINA provide direct services and advocacy. In Bosnia and Herzegovina, the Centre for Women Zenica, United Women Banja Luka, and the Foundation for Local Democracy Sarajevo support women and girls affected by TF GBV. However, their ability to influence how cases are handled remains limited, and their reach is constrained by funding shortages and heavy reliance on donor support.

A participant from Albania shared that emergency shelters for women, children, and victims-survivors of trafficking, organised by the NGO Nisma ARSIS, play a crucial role in addressing gaps in state-provided support. The organisation offers shelter to children without parental care, allowing them to remain in the centre until their cases are resolved. Children referred for psychological assistance receive long-term counselling and support services at no cost.

Nisma ARSIS also supports parents by providing guidance on how to assist their children and navigate difficult situations. The organisation works in close collaboration with child protection services to ensure that all required support is delivered. As a member of the multidisciplinary team, Nisma ARSIS contributes to joint assessments and coordinated service provision. Each case is addressed individually, and the organisation's work is integrated into a broader institutional response. Its role includes helping to close protection gaps by working with families to ensure that parents assume responsibility and provide proper care for their children.

Although based in Tirana, Nisma ARSIS delivers services across Albania. The organisation also ensures that a psychologist is present during interviews conducted by the police or prosecutors with child victims-survivors, providing psychological support throughout the process.

10. Training Gaps Across Sectors

Across the Western Balkans, training on technology-facilitated gender-based violence (TF GBV) remains fragmented, inconsistent, and heavily donor-dependent. While some professionals receive ad hoc education through international workshops or civil society-led initiatives, there is little institutionalisation of knowledge within state systems. Training programs still overwhelmingly focus on traditional forms of gender-based violence, with minimal adaptation to address the digital dimension, its gendered dynamics, or the evolving tactics used by perpetrators online.

In North Macedonia, for example, a state-developed training module with support from UNFPA included a brief session on digital abuse, but it was never institutionalised or scaled across relevant institutions. In Montenegro, judges and prosecutors receive limited instruction on cybercrime through the national judicial training centre, but experts note that participation is low and content does not address the specific realities of TF GBV. Law enforcement agencies across the region often receive training on high-tech crime, but these focus on financial fraud or hacking, without addressing how control, coercion, and harassment are weaponised online in gendered ways. As one regional expert explained, “They’re trained to follow IP addresses, not to understand how digital spaces are used to intimidate and silence women.”

Beyond the criminal justice system, key frontline sectors such as social welfare, education, public health, and child protection are frequently left out of TF GBV training. School staff, psychologists, and social workers often lack the tools to identify, document, or respond to digital forms of abuse among youth, and few prevention or referral protocols are in place. In some areas, these professionals are unaware of what constitutes TF GBV, let alone how to intervene or support survivors. Survivors themselves report facing scepticism, minimisation, or confusion when seeking help from institutions unfamiliar with digital harm.

A cross-sectoral, survivor-centred, and gender-sensitive training approach is urgently needed. This includes developing standardised curricula on TF GBV for law enforcement, prosecutors, judges, teachers, mental health professionals, and social workers. Training should focus not only on legal definitions and evidence handling, but also on digital safety, trauma-informed communication, and strategies to prevent secondary victimisation. Without such coordinated capacity building, institutional responses to TF GBV will remain patchy, reactive, and disconnected from the lived experiences of survivors.

Conclusion

The Western Balkans region faces deep and persistent challenges in addressing technology-facilitated gender-based violence (TF GBV). Insufficient funding, limited expertise, and inadequate investigative tools continue to hinder effective responses. Although awareness of TF GBV is gradually increasing and several isolated efforts have been made, primarily by civil society organisations, legal, institutional, and cultural barriers remain firmly in place. In the absence of legal reform, enhanced institutional capacity, and stronger coordination among relevant agencies, survivors will continue to lack adequate support, and perpetrators will remain largely unaccountable.

To break the cycle of inaction, governments must first recognise technology-facilitated gender-based violence (TF GBV) as a distinct and serious form of violence and explicitly incorporate

it into national criminal codes with clear definitions, sanctions and recourse. This requires the development and implementation of binding standard operating procedures (SOPs) across sectors, as well as investments in digital forensic capacities, psychosocial support systems, and survivor-centred approaches within law enforcement, prosecution, and social services.

Equally crucial is raising public awareness about the nature, prevalence, and impact of TF GBV. Widespread understanding of the issue can help drive political will, build pressure for legal and institutional reform, and reduce stigma for survivors. National campaigns, school-based education, and collaboration with media, influencers, and civil society can amplify public discourse and create an informed constituency that demands action. In contexts where political decision-makers are reluctant or slow to act, a well-informed public can play a vital role in generating momentum and accountability.

Governments should also prioritise formal partnerships with civil society organisations, particularly those already supporting victims-survivors, raising awareness, and developing innovative tools for prevention and redress. Integrating their expertise and good practices into public systems will strengthen service delivery and ensure more equitable access to support. Only through a combination of legal reform, institutional investment, public awareness, and gender norm transformation can TF GBV be effectively addressed, as both a human rights violation and a growing threat to safety, equality, and democracy in the digital age.

The next chapter outlines concrete recommendations to advance this goal and build a more coordinated and resilient regional response to TF GBV across the Western Balkans.

04 Recommendations for Addressing Technology-Facilitated Gender-Based Violence in the Western Balkans

4. Recommendations for Addressing Technology-Facilitated Gender-Based Violence in the Western Balkans

This report highlights the growing need for a more coordinated, cross-sectoral, and survivor-focused response to technology-facilitated gender-based violence (TF GBV) in the Western Balkans. While certain legal progress has been made in addressing cybercrime and digital harm, TF GBV is still not clearly defined or consistently addressed in national laws or institutional practice. As a result, the current response remains fragmented, with limited accountability and inadequate protection for those affected.

The recommendations in this section draw on insights from legal analysis, desk research, stakeholder mapping, and interviews with representatives from institutions such as the law enforcement, judiciary, social services, civil society organisations, and digital safety experts. They aim to respond to the most pressing gaps identified throughout the research and to promote a more effective, coordinated, and inclusive approach to preventing and responding to technology-facilitated gender-based violence in the Western Balkans.

The focus areas include strengthening legal and policy frameworks, building institutional capacities, enhancing support and protection services for survivors, improving coordination with technology companies and the private sector, and investing in data collection, training, awareness-raising, and social norm change. Together, these measures are designed to support a system that is capable, survivor-centred, and responsive to the evolving realities of digital violence.

To provide a clear overview, recommendations are grouped into six thematic areas, each addressing a key pillar of prevention, protection, and accountability. The table below summarises the priority areas and the key actions proposed. Each theme is elaborated in greater detail in the sections that follow.

Summary of Recommendations to Address TF GBV in the Western Balkans

RECOMMENDATION AREA	KEY ACTIONS
1. Legal Frameworks	Define TF GBV, criminalise digital-specific offences, ensure both adult and children victim-survivors protection, integrate into domestic violence laws, regulate platforms, expand legal aid, provide TF GBV training for judiciary.
2. Institutional Capacities	Train criminal justice and social sector professionals, establish SOPs, equip with digital tools for evidence collection, strengthen specialised police units, improve coordination.
3. Victim Support Services	Adapt social and mental health services to TF GBV, engage schools, support CSOs, expand legal aid, build on SOS hotlines, create online support tools.
4. Data and Monitoring	Integrate TF GBV in national data systems, disaggregate data, enable coordination, support research, publish anonymised statistics, ensure ethical safeguards.
5. Engagement with Platforms	Develop cooperation protocols, assign law enforcement PoCs, enforce platform obligations, engage private sector and CSOs in prevention and investigation.
6. Awareness and Prevention	Run public campaigns, educate youth via schools and social media, train journalists, promote gender equality, support parents with digital tools and skills.

1. Strengthen and Modernize Legal Frameworks to Address TF GBV

While countries in the Western Balkans have made incremental progress in regulating digital spaces, legal frameworks remain fragmented and outdated in relation to the evolving nature of technology-facilitated gender-based violence (TF GBV). This analysis shows that TF GBV is, at best, indirectly addressed through existing legal provisions, with only a few notable exceptions. For example, Montenegro and North Macedonia have introduced explicit provisions criminalising the non-consensual sharing of intimate images. In contrast, in Serbia, victims-survivors are often required to initiate civil lawsuits, a burden that significantly hinders access to justice, particularly in rural or conservative communities.

TF GBV has devastating consequences. More than half of women (18+) present online in the region have experienced some form of technology-facilitated violence in their lifetime.[35] Recent surveys across the region show that up to 10 to 12% of young women have experienced some form of online blackmail or image-based abuse, with psychological trauma, reputational damage, and withdrawal from public life as common outcomes. Such impacts demand legal systems that are clear, comprehensive, and survivor-centred.

To close the gaps, governments should take concrete and coordinated legal steps, informed by international human rights standards (e.g., Istanbul Convention, CEDAW) and examples of best practices from within the region. These include:

35 UN Women (2023). The Dark Side of Digitalization: Technology-Facilitated Violence Against Women in Eastern Europe and Central Asia. UN Women. Available at: https://eca.unwomen.org/sites/default/files/2023-11/research-tf-vaw_executive_summary_26-november.pdf

- **Explicitly defining TF GBV** in criminal codes as a standalone form of gender-based violence. The definition should cover cyberstalking, online harassment, digital coercion, image-based abuse, and the use of deepfakes, drawing on models such as Article 175a of the Criminal Code of Montenegro, which criminalises misuse of sexually explicit content.
- **Expanding legal protection beyond minors** to include adults subjected to image-based abuse. For example, revising criminal codes to remove age restrictions or civil lawsuit requirements, as seen in North Macedonia's recent 2023 reforms on stalking and harassment.
- **Integrating digital abuse into domestic violence legislation,** including psychological and economic abuse through surveillance apps, account control, or public shaming via social media.
- **Mandating ex officio prosecution** of TF GBV-related crimes to reduce the burden on victims-survivors and ensure consistency in enforcement.
- **Introducing regulatory obligations for platforms** to cooperate with law enforcement, respond swiftly to content takedown requests, and transparently report moderation practices, inspired by elements of the EU's Digital Services Act.
- **Ensuring access to free legal aid** for TF GBV survivors, especially in underserved areas, and simplifying digital reporting procedures via secure apps or websites.
- **Institutionalising regular training** for police, prosecutors, and judges on digital abuse patterns, gender-sensitive investigation techniques, and the use of digital forensics in TF GBV cases.

By anchoring legal change in clear definitions, institutional accountability, and survivor-friendly processes, countries in the Western Balkans can begin to dismantle the culture of impunity that surrounds online violence and offer meaningful protection in the digital age.

2. Strengthen Institutional Capacities to Effectively Address TF GBV

The capacity of institutions to respond to technology-facilitated gender-based violence (TF GBV) across the Western Balkans remains limited and uneven. While some progress has been made in integrating TF GBV into criminal legislation, institutional responses often lag behind, hindered by a lack of awareness, digital competencies, tools, and coordinated procedures.

This study confirms that frontline institutions, particularly law enforcement agencies, judicial bodies, and social protection services, often lack the necessary resources, training, and internal protocols to recognise, investigate, and prosecute TF GBV effectively. Responses are frequently reactive, case-by-case, and dependent on individual initiative rather than grounded in institutional strategy.

- To effectively address technology-facilitated gender-based violence (TF GBV), governments must prioritise institutional accountability and gender-responsive governance across sectors. One concrete mechanism to support this is the **UNDP Gender Equality Seal for Public Institutions,**[36] which serves as a powerful tool to sensitise government bodies, strengthen gender mainstreaming, and promote institutional change. By participating in

36 As public institutions embark on a journey towards gender equality excellence, the Gender Equality Seal measures their progress against internationally validated standards. It also supports them every step of the way, offering innovative tools and tailored guidance. UNDP. Available at: https://www.gendersealpublicinstitutions.org/the-seal/

the Gender Seal certification process, public institutions can assess and improve their internal policies, training systems, and service delivery with respect to gender equality, including their capacity to prevent and respond to TF GBV. Integrating such mechanisms into broader national strategies can help embed survivor-centred, rights-based responses to digital violence across justice, security, education, and social protection systems.

- **Develop and implement specialised training programmes** for law enforcement, prosecutors, judges, and social workers, focusing on the specific characteristics of TF GBV, digital evidence handling, gender-sensitive approaches, and survivor-centred communication;
- To effectively investigate and prosecute technology-facilitated gender-based violence (TF GBV), law enforcement agencies should have **access to appropriate digital forensic tools and open-source intelligence (OSINT) techniques**. These include publicly available methods such as social media profiling, reverse image searches, metadata extraction, and network analysis, which can help identify perpetrators and preserve digital evidence. Law enforcement officers and prosecutors must be equipped with the necessary software, equipment, and technical expertise to track online threats and link them to individuals, particularly in cases where perpetrators operate anonymously or across multiple digital platforms.

However, the use of such tools must always be consistent with each country's legal and procedural safeguards, including national laws on privacy, data protection, and criminal procedure. More intrusive techniques, such as accessing private data, monitoring encrypted platforms, or tracing IP addresses, must be subject to judicial oversight and permitted only where national legislation explicitly allows so.

To ensure that these methods are applied in a responsible and effective manner, states should invest in training for law enforcement and prosecutors on the legally compliant use of digital forensic and OSINT tools. It is also essential to develop clear internal protocols and ethically grounded guidelines that govern the investigation of online harms while safeguarding fundamental rights. Institutional cooperation with digital platforms should be formalised to allow for timely evidence preservation, content removal, and support in identifying perpetrators, all in line with legal procedures. Investments in digital investigative capacity must also prioritise a gender-sensitive and survivor-centred approach, with mechanisms in place to regularly evaluate compliance with national and international legal standards.

- **Establish internal protocols and standard operating procedures** within relevant institutions to guide the identification, documentation, and referral of TF GBV cases, ensuring consistent and coordinated responses; Existing protocols for GBV or domestic violence can be updated with a knowledge and procedures on TF GBV.
- **Create or strengthen specialised units within law enforcement and prosecution services** that focus on cybercrime and gender-based violence, with dedicated staff trained in handling TF GBV cases;
- **Strengthen cooperation between local police units and central cybercrime departments** to ensure faster, more coordinated, and effective investigation of TF GBV cases.
- **Facilitate cooperation between institutions and digital platforms**, by developing contact points and formal protocols for urgent content removal, evidence preservation, and perpetrator identification in online environments;

- **Improve coordination between institutions**, particularly between law enforcement, social protection services, and civil society actors, to ensure holistic support for survivors and better information sharing;
- **Facilitate regional exchange and joint learning opportunities** among law enforcement, prosecutors, and social service providers to strengthen institutional knowledge of TF GBV and promote the sharing of good practices in digital evidence collection, survivor protection, and prosecution strategies;
- **Invest in long-term institutional capacity**, rather than ad hoc responses or donor-driven projects, by integrating TF GBV into national strategies, budgets, and institutional mandates.

Without sufficient institutional capacity, even the best-designed legal frameworks cannot be implemented effectively. Strengthening frontline responses is essential to ensuring timely, accountable, and survivor-sensitive protection and justice for those affected by TF GBV.

CASE STUDY: INSTITUTIONALISING TF GBV TRAINING IN INDONESIA'S POLICE CURRICULUM

A compelling example of institutional commitment to addressing technology-facilitated gender-based violence (TF GBV) comes from Indonesia. Through the UNDP Police Capacity Building Support Programme for Combatting GBV in the Digital Sphere, and with support from the Korean National Police Agency, the Indonesian National Police successfully integrated six specialised TF GBV training modules into its official police training curriculum. This initiative demonstrates how sustained technical cooperation can lead to systemic change by equipping law enforcement with tools to understand, investigate, and respond to TF GBV effectively.

The six modules include:

1. **Gender-Based Violence in the Digital Sphere** – introducing key concepts, forms of online GBV, and strategic institutional responses
2. **Legal Frameworks for Addressing TF GBV** – presenting national legislation and legal mechanisms to combat online abuse
3. **Victim Support in TF GBV Cases** – outlining protocols for trauma-informed support to survivors, based on the Law on Sexual Violence Crimes
4. **Evidence Gathering in TF GBV Cases** – providing best practices for collecting and preserving digital evidence for use in legal proceedings
5. **Interviewing Witnesses, Experts, and Suspects** – training in survivor-cantered techniques in support of effective investigations
6. **Mitigation Strategies** – exploring tools and multi-stakeholder cooperation to reduce the prevalence and impact of TF GBV

This case illustrates how integrating TF GBV content into national police training systems can strengthen institutional accountability, ensure sustainability, and build capacity to protect survivors more effectively.

3. Strengthen and Expand Victim-Survivor Support Services for TF GBV

Survivors of technology-facilitated gender-based violence (TF GBV) face sharp barriers in accessing protection, justice, and psychosocial support. In the Western Balkans, support services for gender-based violence continue to focus predominantly on physical or domestic abuse, leaving gaps in addressing the psychological trauma, reputational damage, and online safety threats associated with TF GBV. Interviews conducted to inform this assessment revealed that survivors often struggle to identify where to turn for help—particularly when the harm occurs in digital spaces, is inflicted by anonymous perpetrators, or extends across borders.

Across all countries assessed, professionals in social services, mental health centres, and civil society organisations act as first line responders for survivors. However, these actors frequently report lacking the tools, knowledge, or institutional mandates to support victims-survivors of digital violence. In a 2024 regional NGO survey, less than 15% of service providers indicated they had received training on TF GBV or were familiar with protocols for supporting survivors of online abuse.

To build a more inclusive, survivor-cantered support system, the following targeted measures should be prioritised:

- Social services and mental health providers, particularly Social Welfare Centres and community-based counselling units, should explicitly integrate TF GBV into their mandates. Staff must be trained in trauma-informed care and digital safety. For example, in Montenegro and North Macedonia, pilot trainings by women's organisations on image-based abuse have improved survivor outcomes and institutional awareness.
- Civil society organisations with experience in GBV should be financially and structurally supported to extend their services to TF GBV cases. These organisations often act as the first point of contact for victims-survivors, particularly among marginalised groups, and many are already offering support such as legal aid, psychosocial counselling, and accompanying in legal proceedings. In Serbia, for instance, the organisation Atina has supported over 100 survivors of digital abuse since 2022, offering legal and psychological support.
- Legal aid must be guaranteed and expanded. Legal aid providers should be trained to assist survivors with criminal complaints, data removal requests, and protective orders in online environments.
- Existing helplines, including child support hotlines such as the *Plavi telefon* in Bosnia and Herzegovina and SOS lines for domestic violence across the region, should be expanded to include TF GBV response. Staff should receive training on online abuse dynamics and referral procedures, and operate under confidentiality and digital security protocols.

Support platforms must prioritise creating a safe and welcoming environment for those seeking help, ensuring their privacy is protected, identities remain confidential, and sensitive information securely handled. Online support platforms should be developed or expanded to allow confidential, 24/7 access to assistance. These may include:

- Chat-based or app-based counselling services with anonymity features;
- Online portals where victims-survivors can access information on evidence preservation, legal rights, and psychological recovery;
- Self-help digital toolkits with guidance on protecting digital footprints;
- Virtual referral systems linking victims-survivors with psychologists, legal aid, and support networks.

Special attention must be given to ensuring access for Roma women, LGBTQ+ individuals, women with disabilities, and rural populations, who face structural and digital exclusion. Services should be mobile-accessible, linguistically diverse, and advertised through trusted community channels.

By modernising and scaling up support systems, governments and stakeholders can ensure that survivors of TF GBV receive timely, relevant, and respectful assistance, whether the harm occurs in person or online.

4. Improve Data Collection, Monitoring, and Reporting on TF GBV

The lack of systematic data collection on technology-facilitated gender-based violence (TF GBV) across the Western Balkans significantly undermines the ability of institutions to understand the scope of the problem, develop effective responses, and track progress. Most countries do not collect disaggregated data on TF GBV incidents, and available information is often scattered across law enforcement, judicial, and social service institutions, with little or no coordination or consistency.

In the absence of accurate and reliable data, TF GBV remains largely invisible in official statistics, resulting in underreporting, poor institutional prioritisation, and limited resource allocation.

To strengthen data and monitoring systems for TF GBV, the following actions are recommended:

- **Integrate TF GBV indicators into existing gender-based violence monitoring systems**, including within police databases, court information systems, and social protection records. Institutions should be able to flag cases involving digital violence for tracking and analysis;
- **Collect disaggregated data** that reflects key variables such as type of digital violence (e.g. cyberstalking, image-based abuse), gender, age, location, and relationship to the perpetrator. This should also include information on case outcomes, including whether cases are dismissed, prosecuted, or result in convictions;
- **Establish coordination mechanisms between relevant institutions**, including law enforcement, judiciary, social services, health services, and civil society organisations, to enable consistent and secure data sharing while respecting survivors' privacy and data protection laws;

- **Empower national statistical offices and ministries of justice, interior, and social affairs** to lead the development of TF GBV data frameworks, in collaboration with women's organisations and digital rights experts;
- **Encourage regional collaboration in data collection and monitoring** by harmonising TF GBV indicators and sharing anonymised, standardised data across borders, while respecting privacy and ethical standards;
- **Support civil society and academic institutions** in conducting research on the prevalence, patterns, and impact of TF GBV, particularly among underrepresented groups such as adolescents, LGBTQ+ individuals, and women from rural or marginalised communities;
- **Countries should invest in public-facing tools (online dashboards or interactive websites) that report anonymised TF GBV** trends, and support independent research on underreported forms of TF GBV affecting adolescents, LGBTQ+ individuals, Roma women, and rural communities. All data systems must adhere to strict ethical standards, ensuring that collection methods do not endanger survivors or expose sensitive personal information.

5. Strengthen Engagement with Digital Platforms

Technology-facilitated gender-based violence (TF GBV) is enabled and often amplified by the architecture of digital platforms and communication technologies. Despite their central role, most global tech companies operate with limited transparency or accountability in preventing, identifying, and responding to online abuse. Across the Western Balkans, law enforcement and service providers report ongoing barriers in engaging with platforms—such as difficulties in obtaining user data, removing harmful content, and securing digital evidence, especially in time-sensitive or cross-border cases.

Currently, no country in the region has a binding national protocol for formal cooperation with technology companies in TF GBV cases, and reporting tools on platforms are often not available in local languages or fail to categorise TF GBV types appropriately. In Bosnia and Herzegovina, for example, several law enforcement officers interviewed noted they rely on lengthy international procedures to request content removal from platforms like Meta, which delays investigations and victim protection.

To close these gaps and promote platform accountability, the following measures are recommended:

States should establish formal national cooperation protocols with major digital platforms, designating specialised contact points within cybercrime units and prosecution services to streamline requests for evidence preservation, content removal, and user data related to TF GBV. Where applicable, these procedures should align with international standards, such as the Budapest Convention's tools for cross-border cooperation in cybercrime cases.

Regulatory frameworks must be strengthened to require timely platform responses to reports of TF GBV, ensure transparency of moderation policy, and require platforms to report annually on the volume and nature of gender-based abuse cases they manage. Countries can draw from the European Union's Digital Services Act,[37] which mandates due diligence from platforms, including in relation to illegal content and systemic risks like TF GBV.

37 In 2022 the European Union adopted the Digital Services Act (DSA) as an essential regulation to enhance accountability, transparency and safety while users navigate the online space. European institutions were committed to regulate the space which was until recently supervised only by the internal policies introduced by big platforms themselves (for example META, Google or Amazon).

Technology companies operating in the region should be encouraged or required to offer survivor-friendly reporting mechanisms, available in local languages and with specific tagging for TF GBV categories (e.g. image-based abuse, deepfakes, stalking). Partnerships with local civil society organisations can help develop context-appropriate safety resources and digital literacy campaigns tailored to women and marginalised groups.

Police and prosecutors should appoint or train digital liaison officers with the technical and legal knowledge to engage with platforms, telecom providers, and cybersecurity companies. These officers can facilitate urgent cooperation requests and improve evidence handling in real time.

Governments and international donors should also support innovation in protective digital technologies, such as AI-based abuse detection tools, consent management features, and flagging mechanisms developed in consultation with survivors and rights groups. Tech companies should be incentivised to invest in regional trust and safety teams and collaborate in public education efforts, including workplace trainings and school-based prevention campaigns.

Finally, meaningful platform engagement should be grounded in human rights and survivor-centered principles, ensuring transparency, due process, and non-discrimination in all actions involving user data or moderation decisions.

6. Promote Awareness, Prevention, and Supportive Social Norms to Address TF GBV

Technology-facilitated gender-based violence (TF GBV) is rooted in broader social norms that tolerate online misogyny, normalise digital abuse, and fail to equip communities—especially youth—with tools to recognise or resist such harm. This challenge is amplified in the Western Balkans, where digital literacy remains uneven, media narratives often reinforce harmful stereotypes, and schools, families, and communities lack coordinated prevention strategies. According to the research conducted in Serbia, more than half of the girls surveyed (53.2%) reported experiencing violence in digital spaces, and many also knew a peer who had gone through similarabuse.[38]

To prevent TF GBV and build resilience at the community level, multi-sectoral action is needed.

Governments and partners should invest in **large-scale, age-appropriate public awareness campaigns** explaining what constitutes TF GBV, how it affects victims-survivors, and how to seek help. These campaigns should be tailored for platforms like TikTok, Instagram, and YouTube, using short-form videos, influencer-led content, and storytelling formats that engage adolescents while challenging gender stereotypes.

Education systems play a critical role. Ministries of Education should integrate TF GBV into digital literacy, civic education, and IT classes, covering consent, boundaries, and respectful communication, while also training teachers, school psychologists, and youth workers to recognise and respond to signs of online abuse. In Bosnia and Herzegovina, early pilot initiatives in schools have shown promise but lack scale and sustainability.

Digital opinion leaders need to be engaged in efforts to prevent TF GBV. Governments and civil society should actively engage bloggers, influencers, and other online opinion leaders in

38 ATINA (2022) „Ispred ekrana - Istraživanje o rodno zasnovanom nasilju u digitalnom prostoru". Available at: https://serbia.unfpa.org/sites/default/files/pub-pdf/ispred_ekrana_sa_koricom.pdf

awareness and prevention campaigns on technology-facilitated gender-based violence. These individuals play a powerful role in shaping online narratives and can help amplify messages that promote digital respect, challenge harmful gender norms, and support survivors. Their platforms offer direct access to wide and diverse audiences, particularly youth, making them valuable allies in shifting attitudes and building safer online spaces.

Media professionals and content creators must be mobilised. Newsrooms should receive training on ethical reporting of online abuse, avoiding sensationalism and victim-blaming. National press councils can adopt editorial standards for covering TF GBV, aligned with CEDAW and other rights-based frameworks. Promoting gender-sensitive media literacy among the public can also help counteract misinformation and online hate.

Changing norms requires engaging men and boys, influencers, and online creators in campaigns that question harmful masculinity and promote equality. Peer-led workshops, youth ambassador initiatives, and community-based dialogues—especially in conservative or rural areas—can create space to challenge stigma, reduce victim-blaming, and promote allyship.

Parents and caregivers, often left out of digital safety strategies, need better support. Schools should partner with parents through workshops and handbooks on how to set up parental controls, talk to children about sexting, and spot signs of distress. Anonymous helplines or digital guides could help parents get expert advice without fear of judgment. For example, Safer Internet Centre[39] in Bosnia and Herzegovina offer easy-to-use materials for non-tech-savvy adults and children. Initiatives like Serbia's National Contact Centre for Child Safety Online[40] offer a valuable model, providing expert advice and direct support to families navigating these challenges. Importantly, if parents want to protect their children from harmful online influences, the first step is to critically reflect on the values and attitudes they themselves convey at home. Behaviours and messages that normalise any form of gender-based violence within the family context can shape children's perceptions of what is "normal"—even when those norms contradict the principles of equality, non-violence, and democracy. Addressing TF GBV therefore requires not only equipping parents with digital tools, but also fostering reflection and dialogue on the social norms reproduced in everyday life.

To make prevention efforts more effective, it is essential to draw from existing good practices in the region. In Serbia, preventive initiatives such as *"Mogu da neću"*[41] (I Can Say No) and *"Cyber Intimacy"*[42] offer promising examples of youth-centred approaches to tackling technology-facilitated gender-based violence (TF GBV). The *Mogu da neću* platform, developed by the Autonomous Women's Centre, focuses on educating adolescents about digital consent, emotional manipulation, and online boundaries through interactive quizzes, videos, and school-based workshops. Meanwhile, Share Foundation's *Cyber Intimacy* site provides accessible, rights-based information on digital privacy, sexting, online relationships, and protection against image-based abuse, offering young people tools to navigate intimacy and sexuality in the digital age safely

39 With a goal of preventing sexual exploitation and abuse of children in digital environment and ensuring information and tools for safe and responsible use of informational and communication technologies, we established Safer Internet Centre in Bosnia and Herzegovina through innovative and improved web platform www.sigurnodijete.ba.

40 The National Contact Centre for Child Safety Online, established by the Serbian government, serves as a central hub for reporting harmful online content, accessing educational materials, and receiving expert advice on safe internet use. Open to all citizens via web, email, or the toll-free number 19833, the Centre offers support in protecting children's rights in digital environments through reporting, education, and counselling. https://www.srbija.gov.rs/tekst/en/129990/child-safety-on-the-internet.php?utm_source=chatgpt.com

41 Autonomni ženski centar. https://mogudanecu.rs

42 SHARE Foundation https://cyberintimacy.sharefoundation.info

and responsibly. Both initiatives emphasise prevention, consent, and digital literacy as core strategies in addressing TF GBV and could serve as models for similar programming across the Western Balkans.

By anchoring prevention in education, media, parenting, civil society and community dialogue, countries can address the root causes of TF GBV, not just its symptoms. Shifting social norms, improving digital literacy, and building informed, empathetic communities are critical to ensuring that the online space becomes safer, especially for women and girls.