Landscape report on NCII abuse in Western Balkans

Date: March, 2026.
Prepared for FCDO
Written By David Wright & Boris Radanović
South West Grid for Learning

Contents

Foreword

For over a decade, South West Grid for Learning has worked directly with victims of non-consensual intimate image abuse through the UK Revenge Porn Helpline and, more recently, through the global StopNCII.org platform. One consistent lesson has emerged: while the technology enabling abuse is global, the systems supporting victims are local, and often uneven.

This report was developed to better understand that reality in the Western Balkans. It is not intended to be a definitive study, but a practical, time-bound assessment based on available data, stakeholder insight, and operational experience.

The findings point to a familiar pattern. Legal frameworks exist but are fragmented and provide indirect legal coverage. Victim support is often led by civil society rather than the state. Coordination mechanisms are still developing. And engagement with platforms remains inconsistent.

Yet there are also clear signals of progress. Policymakers are increasingly recognising the issue. Regional cooperation is possible. And tested models, from helplines to prevention technologies, already exist and can be adapted.

The purpose of this report is simple: to provide a foundation for action.

By strengthening legal clarity, improving victim pathways, and building coordinated systems, the region has an opportunity to move from fragmented responses to structured, survivor-centred approaches.

David Wright CBE

CEO, South West Grid for Learning

Acknowledgements

This Landscape Report was prepared by South West Grid for Learning (SWGfL) as part of a regional assessment examining readiness to prevent and respond to Technology-Facilitated Gender-Based Violence (TFGBV), with particular focus on Non-Consensual Intimate Image (NCII) abuse, across the Western Balkans. The report was written by David Wright and Boris Radanović, with SWGfL' s operational experience in addressing NCII abuse, including the work of the UK Revenge Porn Helpline and the StopNCII.org platform. The authors would like to thank the many stakeholders across Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia who contributed their time and expertise to this report. Insights from civil society organisations, government institutions, law enforcement bodies, digital rights organisations, and victim support providers were essential in shaping the analysis presented in this report. The report also benefited from questionnaire responses, consultations, and discussions with practitioners working directly on gender-based violence, digital safety, victim support across the region. Their perspectives helped identify practical challenges and emerging policy priorities related to NCII abuse.

The authors would also like to thank all individuals and organisations who participated in consultations and generously contributed their time and expertise to this report: Ali Hendy, FCDO; Rachel Grant, FCDO; Uglješa Vuković, UN Office Bosnia and Herzegovina; Abida Pehlić, President, Novi Put; Igor Jurić, President, Serbian CMEC; Altin Hazizaj, Executive Director, CRCA/ECPAT Albania; Dunja Bonacci Skenderović, Regional expert on gender-based violence, Samra Filipović-Hadžiabdić, Director, Agency for Gender Equality of Bosnia and Herzegovina; Amina Selimbegović Kreponić, UN Women; Anela Lemes, UN Women; Višnja Ljubičić, Ombudswoman for Gender Equality, Office of the Ombudsperson for Gender Equality of the Republic of Croatia; Svetlana Cvetkovska, North Macedonia; Lidija Sterjov, State Advisor for Equal Opportunities, Ministry of Labour and Social Policy of North Macedonia; Edi Gusia, Head of the Agency for Gender Equality of Kosovo; Biljana Pejović, Senior Advisor, Ministry of Human and Minority Rights of Montenegro; Irena Varagić, Montenegro; Brankica Janković, Commissioner for Protection of Equality, Commissioner for Protection of Equality of the Republic of Serbia; Tea Pokrajčić, Programme Manager, The Kvinna till Kvinna Foundation, Jovana Škorić, researcher.

This report was prepared for the UK Foreign, Commonwealth and Development Office (FCDO). While the report has benefited from the input of numerous stakeholders and partners, the views and analysis presented are those of the authors and do not reflect the official positions of the UK Government or other organisations involved in the consultation process. We thank all individuals and organisations for taking part in the consultation process, including those who preferred not to be named.

Executive Summary

Technology-Facilitated Gender-Based Violence (TFGBV), including harassment, threats, stalking, and the non-consensual intimate image (NCII) sharing, is increasingly recognised across the region as a serious form of harm affecting women, girls, and individuals active in public and digital spaces. Legal provisions addressing technology-facilitated harms are often fragmented, specialised victim support services remain limited, and coordination between public institutions, civil society organisations, and digital platforms is still developing. As a result, the region is experiencing a widening gap between the scale of digital harms occurring online and the readiness of institutional systems to respond effectively.

This report assesses regional readiness to prevent and respond to TFGBV, with a focus on NCII abuse, across Western Balkans Six (Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia).
Drawing on desk research, legal and policy analysis, online stakeholder questionnaire, interviews, workshops, events and consultations with regional stakeholders, the report evaluates readiness across six dimensions: legal and policy frameworks, institutional coordination, victim support services, platform cooperation and digital governance, prevention and awareness, and data collection and monitoring systems. The findings indicate that while awareness of NCII abuse is increasing among policymakers and practitioners, it remains limited amongst general public, while systemic responses across the region are still emerging and require further strengthening to provide consistent and survivor-centred protection.

Headline Findings

NCII abuse is increasingly recognised but remains underreported. Stakeholders across the region report growing prevalence of online harassment, threats, and NCII abuse. However, the absence of systematic monitoring mechanisms means the full scale and nature of TFGBV and NCII abuse remain poorly documented.

• Legal frameworks provide partial and indirect coverage but remain difficult to operationalise. Existing provisions (e.g. harassment, privacy, cybercrime) are used to address NCII, but the absence of explicit offences, reliance on indirect legal pathways, and procedural burdens limit consistent enforcement across jurisdictions.
• Victim support systems remain uneven and heavily reliant on civil society organisations. In Western Balkan countries, specialised assistance for survivors of online abuse is provided primarily by NGOs as a part of their broader activities.
• Institutional coordination mechanisms are still developing. Cooperation between law enforcement, prosecutors, social services, digital regulators, and civil society actors often occurs on an ad hoc basis rather than through structured national frameworks addressing NCII abuse.
• Stigma and lack of trust in institutional responses discourage reporting. Survivors frequently hesitate to seek support due to fear of victim-blaming, reputational harm, and uncertainty about whether institutions can respond effectively.
• Engagement with online platforms remains inconsistent and unstructured. Public authorities and civil society organisations report challenges in securing timely responses from digital platforms regarding content removal, and user safety interventions.
• Policy attention to digital violence is increasing across the region. Growing recognition of NCII abuse and TFGBV as a public policy issue presents an opportunity for governments, local women's rights organisations and international partners to strengthen institutional responses and develop coordinated strategies.

Despite increasing awareness, several structural gaps continue to limit the effectiveness of regional responses to NCII abuse:
• Insufficient legal clarity regarding emerging digital harms, particularly in relation to NCII distribution and other forms of NCII abuse.
• Implementation gaps in legal and institutional responses, including limited specialised expertise, inconsistent enforcement, and procedural burdens that discourage reporting and prosecution.
• Limited availability of specialised support services providing legal guidance, psychological support, and digital safety assistance tailored to victims of online abuse.
• Weak data collection and monitoring systems, resulting in fragmented evidence on the prevalence, nature, and outcomes of NCII cases.
• Lack of structured cooperation mechanisms between governments, civil society, and digital platforms, which limits coordinated responses and delays interventions.

Priority Actions for the Next 24 Months

Strengthening regional readiness to address NCII abuse will require coordinated efforts by governments, civil society organisations, and international partners. Priority actions over the next two years should include:

- Reviewing and strengthening legal frameworks to ensure that NCII abuse and other forms of TFGBV are clearly defined, recognised as a separate criminal offence, and effectively addressed within legislation.
- Establishing national coordination mechanisms that bring together justice institutions, law enforcement, victim support providers, and digital governance authorities to respond to NCII abuse cases.
- Expanding specialised victim support services, including accessible reporting channels, legal assistance, and trauma-informed psychosocial support for victims of online abuse.
- Developing consistent data collection and monitoring systems to ensure that NCII abuse and TFGBV cases are systematically recorded and analysed within national violence-against-women frameworks.
- Developing and implementing broad and diverse awareness raising activities around NCII and TFGBV.

Cases involving the publishing, distribution or threat of sharing intimate images illustrate the broader systemic challenges institutions face when responding to digital harms. These cases often expose gaps in legal definitions, difficulties in collecting and preserving digital evidence, delays in securing content removal from online platforms, and limited availability of specialised support services for victims. As a result, strengthening responses to NCII abuse provides a practical entry point for improving wider institutional capacity to address technology-facilitated violence.
By developing clearer legal frameworks, coordinated reporting pathways, stronger victim support systems, and more effective cooperation with digital platforms, governments and partners can build institutional models that respond not only to NCII abuse but also to the broader spectrum of online gender-based violence affecting the region.

Introduction

Understanding Technology-Facilitated Gender-Based Violence

Technology-Facilitated Gender-Based Violence (TFGBV) refers to acts of gender-based violence that are committed, assisted, aggravated, or amplified through the use of digital technologies, online platforms, or electronic communication tools. It encompasses behaviours such as online harassment, cyberstalking, non-consensual intimate image sharing, threats to share non-consensual intimate images, digital coercive control, doxxing, synthetically generated sexual content, and gendered disinformation campaigns.

Non-Consensual Intimate Image (NCII) abuse

Within the broader TFGBV landscape, Non-Consensual Intimate Image (NCII) abuse, sometimes referred to as image-based sexual abuse, represents one of the most acute and rapidly expanding forms of digital violence . NCII abuse involves the sharing, distribution, or threat to distribute intimate images without the consent of the person depicted .

Importantly, contemporary international standards increasingly reject the term “revenge pornography” on the grounds that it misplaces responsibility and obscures the violation of consent at the core of the abuse. Instead, the preferred terminology, image-based sexual abuse or NCII abuse, centres the harm and the absence of consent .

Introduction

NCII may arise in a variety of relational, coercive, and technologically mediated contexts, including:

- Following the breakdown of an intimate relationship.
- As a form of coercion or blackmail (including sextortion).
- Through hacking or unauthorised access to devices.
- Via digitally altered or AI-generated synthetic content also known as “deepfakes ”.
- Within organised online groups dedicated to the sharing of intimate material .

Research demonstrates that women and girls are disproportionately targeted in cases of NCII, and that the consequences frequently include severe emotional distress, anxiety, depression and suicidal ideation .

TFGBV/NCII abuse, presents an emerging risk to democratic processes and national security. Across multiple contexts, online abuse, including coordinated harassment campaigns, gendered disinformation, and the non-consensual sharing of intimate images, has been used to silence women in public life , discourage political participation, and undermine trust in democratic institutions.

These risks are particularly pronounced during electoral periods, where spikes in online abuse targeting women candidates, journalists, and activists have been documented globally. Such dynamics can distort public discourse, suppress participation, and weaken democratic resilience. In this sense, TFGBV is not only a matter of individual protection but also a structural challenge to democratic integrity, governance, and societal stability.

The cross-platform and cross-border nature of NCII presents significant challenges for national legal systems, law enforcement agencies, and victim support services .

Introduction

The rapid growth of generative artificial intelligence has lowered the barrier for creation of synthetic media, a development that disproportionately affects women and exacerbates technology-facilitated violence.

The Role of SWGfL

South West Grid for Learning (SWGfL) is a United Kingdom-based charity with over two decades of experience in online safety, digital harm prevention, and victim support. SWGfL operates nationally and internationally, working with governments, law enforcement, educational institutions,
technology companies, and civil society organisations to strengthen digital safeguarding ecosystems.
SWGfL is the operator of the UK Revenge Porn Helpline , the first dedicated service of its kind supporting adult victims of NCII abuse. Through this work, SWGfL has developed extensive expertise in victim-centred case management, platform engagement, and cross-border content removal.

Technology-Facilitated Gender-Based Violence in the Western Balkans Context

Across the Western Balkans Six, rapid digital expansion has outpaced the development of legal, institutional, and support systems to address technology-facilitated abuse. While digital participation has accelerated,
the capacity of legal, policy, and support systems to prevent and respond to technology-facilitated harms remains uneven across the region. As a result, women and girls, alongside journalists, activists, political actors, and members of marginalised communities, are increasingly exposed to online harassment,
threats, NCII abuse, and coordinated digital intimidation.

TFGBV including NCII abuse, has emerged as a particularly harmful manifestation of this gap. These forms of abuse are used not only to harm individuals, but also to silence participation, damage reputations, and exert control in both private and public spheres. Often, digital abuse is closely intertwined with offline harms, including domestic violence, coercive control, workplace discrimination, and social exclusion.

Across the region, institutional responses to these risks are still developing. Existing legal frameworks often rely on provisions related to harassment, threats, privacy violations, or cybercrime, which may only partially capture the gendered nature of TFGBV. Operational challenges persist, including limited specialised training for law enforcement and judiciary, inconsistent victim support pathways, weak data collection systems, and fragmented coordination between institutions, civil society, and digital platforms.

At the same time, countries are engaged in processes of legal and policy harmonisation linked to European Union accession. This includes alignment with evolving EU frameworks on digital services, cybersecurity, and violence against women, as well as commitments under the Istanbul Convention and other international standards. These processes create a critical opportunity to integrate more explicit, coordinated, and survivor-centred responses to TFGBV within broader governance reforms.

Despite structural gaps, the region is not static. Awareness of digital forms of violence is increasing among policymakers and practitioners, civil society organisations continue to play a central role in providing support and advocacy, and initial legislative and policy developments are emerging in several countries. The Western Balkans are therefore at a transitional stage, where digital risks are rapidly evolving, and institutional systems are beginning to adapt.

This evolving context highlights a widening but addressable gap between exposure to digital harms and the readiness of systems to respond. Strengthening this readiness will require coordinated efforts across legal frameworks, institutional capacities, victim support services, and regional cooperation mechanisms.

The Regional Context

The WB6 countries share common features relevant to the assessment of TFGBV readiness in particular focus on NCII:

- Ongoing legal harmonisation processes linked to European Union accession;
- Complex governance structures in certain jurisdictions;
- Limited specialised digital forensic capacity;
- Underdeveloped cross-sector coordination mechanisms for online harms;
- Strong but often under-resourced civil society engagement.

Existing research and legal mapping exercises demonstrate that elements of TFGBV are addressed within criminal codes and domestic violence legislation. However, these provisions are frequently dispersed across general offences such as harassment, stalking, privacy violations, defamation, or data misuse. In most cases, there is no unified legal definition of TFGBV, and explicit criminalisation of NCII varies in scope and clarity

- Operational challenges remain significant:
- Inconsistent victim referral pathways;
- Limited specialised training for law enforcement, prosecutors, and judiciary;
- Weak or ad hoc cooperation with digital platforms;
- Limited disaggregated data collection;
- Procedural burdens placed on victims in certain offences requiring private prosecution;
- insufficient regional coordination mechanisms.

At the same time, positive developments are visible. Certain jurisdictions have introduced specific offences related to NCII abuse or cyberstalking. Awareness among institutional actors is increasing. Civil society organisations are actively providing support services and advocating for reform. International partners are investing in capacity-building and policy development. The region is not static. It is in transition.

Purpose of This Report

This Landscape Report assesses the regional readiness of the WB6 to prevent, respond to, and support victims of TFGBV, with a particular focus on NCII abuse.

For the purposes of this Landscape Report, "readiness" refers to the capacity of national systems to:

- Prevent NCII abuse through awareness, education, and digital governance measures;
- Protect victims through accessible, survivor-centred support services;
- Prosecute perpetrators effectively and proportionately;
- Coordinate responses across ministries, law enforcement agencies, judiciary, regulatory bodies, and civil society actors;
- Engage constructively with online platforms and digital intermediaries;
- Collect, analyse, and monitor relevant data to inform policy development.

Readiness therefore extends beyond legislative provisions. It encompasses operational capability, procedural clarity, institutional coordination, and cross-border cooperation mechanisms. The objective is to provide a structured foundation for future policy development, targeted investment, and regional collaboration.

Scope and Focus

While TFGBV encompasses a broad spectrum of harmful behaviours, this report places particular emphasis on NCII abuse.

NCII abuse represents a highly illustrative case study for assessing institutional readiness because it:

- Combines criminal, privacy, technological, and gender dimensions.
- Often requires urgent platform cooperation.
- Involves complex evidentiary challenges.
- Frequently intersects with domestic violence contexts.
- Can involve cross-border digital dissemination.
- Produces severe and lasting psychological harm.

By examining NCII as a focal point, the report provides insights applicable to the broader TFGBV landscape.

The geographical scope covers:
- Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, Serbia

Methodology

The findings presented in this report are based on a mixed-methods approach, including:

- Desk-based analysis of available data on awareness, legislation and policy
- Review of existing regional and international assessments and literature
- Analysis of international normative frameworks, including:
    - o The Istanbul Convention (Prevention, Protection, Prosecution, Policies – 4Ps model);
    - o EU Directive 2024/1385 on combating violence against women and domestic violence;
- Stakeholder mapping
- Semi-structured interviews with institutional and civil society actors across the region.
- Questionnaire responses assessing perceived institutional capacity, reporting pathways, and coordination challenges.
- Comparative benchmarking to international best practices

Disclaimer

This report has been prepared using a combination of deep desk research, stakeholder consultations, questionnaire responses, and analysis of publicly available policy, legal, and institutional materials relating to TFGBV and NCII abuse across the WB6. Generative Artificial Intelligence (GenAI) tools were used during the drafting process to assist with structuring, language refinement, and synthesis of research materials. All substantive analysis, interpretation, and conclusions were reviewed and validated by the authors.

The findings presented reflect the information available at the time of writing and are based on sources considered reliable, including academic literature, policy documents, stakeholder inputs, official documentation and media reporting. Given the evolving nature of legal frameworks, institutional practices, and digital harms, some developments may occur after publication.

While every effort has been made to ensure accuracy and completeness, the authors acknowledge that gaps or omissions may remain. The report should therefore be understood as a snapshot of the current landscape rather than an exhaustive account. Any errors or omissions identified in future may be addressed in subsequent updates or related publications.

Benchmarking Framework

The analytical framework underpinning this report is anchored in internationally recognised standard of The Istanbul Convention's four-pillar model (Prevention, Protection, Prosecution, and Integrated Policies) and emerging global practices in responding to NCII.

This frameworks allows for structured comparative analysis while recognising the distinct contexts of each country.

Importantly, the report also considers the practical interface between national systems and global platform ecosystems, acknowledging that NCII is inherently transnational and cannot be addressed solely through domestic criminal law.

In addition to these, the analysis is further informed by practical operational models developed through direct service delivery. In particular, the report draws on the South West Grid for Learning (SWGfL) model for responding to NCII abuse, which integrates victim support, technology-enabled prevention, and cross-platform engagement. This model is referenced in later sections to illustrate how coordinated, survivor-centred approaches can be operationalised in practice across different contexts.

Regional Readiness Matrix

To operationalise the benchmarking framework outlined above, the report applies a comparative readiness matrix across the WB6. The matrix provides a high-level overview of institutional preparedness to prevent and respond to TFGBV, focusing on NCII abuse.

The assessment draws on desk research, legal and policy analysis, stakeholder consultations, available research, and questionnaire responses. Matrix categorises readiness using a three-level scale: Low, Developing, and Advanced. This approach reflects the evolving nature of NCII governance across the region and recognises that countries may demonstrate progress in some areas while still facing structural gaps in others.

The matrix evaluates readiness across six dimensions aligned with the benchmarking framework used in this study: legal and policy frameworks, institutional coordination, victim support services, data and monitoring systems, cooperation with online platforms, and prevention and awareness initiatives. These dimensions reflect internationally recognised approaches to addressing technology-facilitated violence against women and girls and are consistent with regional and global policy guidance on NCII governance.

Overall, the matrix highlights that while awareness of technology-facilitated abuse is increasing across the WB6, institutional systems are still adapting to address these forms of violence effectively. Most countries demonstrate developing levels of readiness, with civil society organisations playing a ignificant role in providing victim support and raising awareness. Legal frameworks and coordination mechanisms are gradually evolving, but specialised services, systematic data collection, and structured engagement with digital platforms remain limited across much of the region.

The Regional Readiness Matrix should be interpreted with caution, as the presence of legal frameworks, institutions, or services does not necessarily reflect their accessibility, effectiveness, or utilisation by victims. Findings from survivor narratives and stakeholder consultations indicate a consistent gap between formal system design and lived experience. In practice, victims frequently bypass institutional pathways, rely on civil society support, and encounter barriers related to trust, awareness, procedural complexity, and response effectiveness. As a result, readiness assessments in this matrix reflect not only the existence of structures, but also their operational functionality, coordination, and perceived accessibility from a survivor perspective.

Country	Legal clarity on NCII	Institutional coordination	Data & monitoring systems	Platform cooperation	Victim support services	Prevention & awareness
Albania	Developing	Low	Developing	Low	Low	Developing
Bosnia & Herzegovina	Advanced	Low	Developing	Low	Low	Developing
Kosovo	Developing	Low	Developing	Low	Low	Developing
Montenegro	Advanced	Developing	Developing	Low	Developing	Developing
North Macedonia	Developing	Low	Developing	Low	Low	Developing
Serbia	Developing	Low	Developing	Low	Low	Developing

Interpretation of Readiness Levels

Low readiness

Limited legal recognition of NCII, absence of specialised institutional structures, minimal or no data collection, and weak or informal cooperation with online platforms, low public awareness of NCII.

Developing readiness

Partial legal coverage through existing criminal or privacy laws, emerging policy discussions on digital violence, some coordination between institutions and civil society, and growing awareness initiatives, but still lacking specialised mechanisms and systematic data, developing public awareness of NCII.Advanced readiness

Clear legal definitions addressing NCII, established coordination mechanisms across justice and support institutions, specialised victim services, consistent data collection systems, and structured cooperation with digital platforms and high public awareness of NCII.

Advanced readiness

Clear legal definitions addressing NCII, established coordination mechanisms across justice and support institutions, specialised victim services, consistent data collection systems, and structured cooperation with digital platforms and high public awareness of NCII.

Regional Pattern

The matrix illustrates a consistent regional pattern. Across the WB6, legal and institutional frameworks addressing technology-facilitated abuse are still evolving, with most countries demonstrating developing levels of readiness. While legal provisions relating to harassment, threats, stalking, or privacy violations may be applied in cases of online abuse, explicit recognition of NCII abuse remains uneven and is often addressed through indirect legal provisions, leading to inconsistent interpretation and enforcement across jurisdictions. Montenegro has introduced explicit criminal provisions addressing the non-consensual distribution of intimate images, with penalties of up to five years' imprisonment, reflecting emerging legislative recognition of NCII abuse within national criminal law.

Serbia has submitted changes to its criminal code to recognize "revenge pornography" as a separate crime and is awaiting a response from the European Commission. Bosnia and Herzegovina formally criminalises NCII; however, the legal framework remains fragmented across entities and Brčko District. While all jurisdictions recognise misuse of sexually explicit content, penalties vary significantly, with different maximum and aggravated sanctions applied for comparable conduct. This results in unequal protection for victims, legal uncertainty in cross-jurisdictional cases, and inconsistent prosecutorial practice. The lack of harmonisation weakens deterrence and undermines a coherent, rights-based response, highlighting the need for alignment with international standards, including the Istanbul Convention.

Civil society organisations continue to play a central role in supporting victims and raising awareness, often compensating for limited specialised services within public institutions. At the same time, formal mechanisms for cooperation between governments and online platforms remain underdeveloped across the region, and systematic monitoring of NCII incidents is largely absent.

Taken together, the findings suggest that while the policy environment is gradually adapting to address digital forms of violence, further institutional development will be required to ensure consistent and survivor-centred responses to NCII across the WB6.

Digital Adoption Context

The Western Balkans six demonstrate relatively high levels of digital connectivity and social media use, aligning with broader European trends. However, regulatory and institutional readiness to address technology-facilitated harms remains uneven. While countries are progressing in aligning with EU digital and cybersecurity frameworks, gaps persist in enforcement capacity, cross-sector coordination, and specialised responses to TFGBV.

Prevalence and Forms of Technology-Facilitated Gender-Based Violence in the Western Balkans

TFGBV is increasingly recognised as a widespread and evolving challenge across the WB6. As digital connectivity has expanded rapidly across the region, so too have opportunities for online harassment, coercion, surveillance, and NCII abuse. These forms of violence occur across social media platforms, messaging applications, and other digital communication environments, often extending and amplifying existing patterns of gender-based violence in offline contexts. Evidence suggests that technology-facilitated abuse is widespread across the region. Research indicates that over half of women aged 18 and older who are active online report experiencing some form of digital abuse in their lifetime, including threats, unwanted sexual messages, or hacking of personal accounts. Regional research demonstrates that TFGBV affects a significant proportion of women and girls who participate in digital spaces. A recent regional assessment of legal, policy, and institutional responses to TFGBV in the Western Balkans found that digital harassment, online threats, stalking, and the non-consensual sharing of intimate images are among the most reported forms of abuse. Survivors frequently face psychological distress, reputational damage, and social isolation following incidents of digital abuse.

Within the broader TFGBV landscape, NCII abuse and online blackmail have emerged as particularly harmful forms of digital violence.

Prevalence and Forms of Technology-Facilitated Gender-Based Violence in the Western Balkans

Surveys conducted across the region indicate that between 10 and 12 percent of young women report experiencing some form of online blackmail or coercion involving intimate images or videos.
These incidents frequently involve threats to distribute private images without consent and can result in significant emotional trauma and withdrawal from education, employment, or public participation. Importantly, evidence from survivor accounts indicates that such abuse often follows a pattern of escalation, beginning with monitoring or coercive communication within intimate or trust-based relationships, progressing to pressure to share content, and culminating in threats or distribution of intimate material without consent.

Several high-profile incidents have highlighted the scale of NCII abuse in the region. For example, Telegram groups in North Macedonia and Kosovo were found to be sharing intimate images of women and girls without consent among thousands of users, demonstrating how digital platforms—particularly closed or encrypted group environments—can facilitate rapid and large-scale dissemination of abusive content beyond public visibility and oversight. In the Western Balkans six, technology-facilitated abuse also frequently targets women involved in politics, journalism, and public advocacy. Studies conducted by the Kvinna till Kvinna Foundation and regional partners indicate that women politicians and public figures across the region regularly experience gendered harassment, threats, and disinformation campaigns online aimed at undermining their credibility or discouraging their participation in public life.
In Kosovo, emerging evidence suggests that women in political and public life are disproportionately targeted through coordinated online harassment, misogynistic disinformation, and reputational attacks.

During recent election cycles, women candidates faced significant levels of gendered abuse on social media, including sexist insults, character attacks, and coordinated trolling campaigns aimed at discouraging participation in public life. This pattern reflects a broader trend where digital violence is used as a tool to silence women and restrict their political engagement, particularly during high-visibility periods such as elections.

Recent research further illustrates the scale and nature of this violence in practice. A 2024 study on violence against women in politics in Montenegro found that over 60% of respondents recognise the issue as present, with online and digital abuse identified as the most prevalent form, affecting nearly 60% of women in political life.

This abuse frequently includes sexist insults, threats, and attacks on personal life, appearance, and credibility, often amplified through social media and online comment spaces. Qualitative findings highlight that such violence is not only widespread but also normalised, with limited accountability and inconsistent institutional responses. Women interviewed described persistent exposure to harassment that extends beyond political disagreement into targeted, gendered attacks, contributing to self-censorship, emotional distress, and in some cases withdrawal from public life.

Similarly, research by the OSCE Office for Democratic Institutions and Human Rights (ODIHR) highlights that women in political and public life are frequently subjected to online harassment, sexist attacks, threats, and intimidation on social media, often intended to discourage their participation in political engagement. A study further found that 58.2% of women parliamentarians surveyed had experienced sexist online attacks on social networks, demonstrating the scale of digital harassment targeting women in political life.

National-level studies also reveal concerning patterns among younger populations. Research conducted in Serbia found that more than half of high school girls had experienced sexualised comments online, while approximately one in ten reported that private photos or videos shared in confidence had later been distributed without their consent.

Findings from the stakeholder questionnaire conducted for this landscape report reinforce these patterns. Respondents from across Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia consistently identified social media platforms and messaging applications as the primary environments where NCII occurs. Platforms such as Facebook, Instagram, TikTok, WhatsApp, Viber, and Telegram were most frequently cited as spaces where harassment, coercion, and the non-consensual sharing of intimate images take place. Stakeholders also emphasised that women and girls are the groups most commonly targeted by NCII abuse. Several respondents noted that adolescents and young women
face heightened risks due to the intersection of social media use, digital relationship dynamics, and peer pressure. LGBTQ+ individuals and young people were also frequently identified as vulnerable groups within online environments.

At the same time, stakeholders repeatedly highlighted that the true scale of NCII in the Western Balkans six is likely significantly underreported. Survivors often choose not to report incidents due to stigma, fear of retaliation, lack of awareness of available support services, or lack of confidence in institutional responses. As a result, many cases remain invisible within official statistics and are instead addressed primarily by civil society organisations providing victim support services and advocacy.

Prevalence and Forms of Technology-Facilitated Gender-Based Violence in the Western Balkans

Although available data remains limited, existing studies consistently demonstrate that TFGBV and NCII abuse are widespread across the Western Balkans six.

Research indicates that more than half of women active online have experienced some form of digital abuse, ranging from threatening messages and harassment to hacking of personal accounts and NCII abuse. These findings suggest that digital spaces increasingly reproduce and amplify gendered patterns of violence already present offline, particularly in contexts where institutional responses and legal protections remain underdeveloped.

Taken together, existing research and stakeholder insights suggest that TFGBV, and NCII abuse in particular, should not be understood as isolated incidents but rather as part of a broader pattern of gendered violence increasingly mediated through digital technologies. The persistence of abuse across platforms, the difficulty of removing harmful content, and the ongoing psychological impact on survivors indicate that digital violence is not only immediate but enduring. The rapid expansion of digital communication platforms, combined with gaps in institutional capacity, legal clarity, and victim support infrastructure, has created an environment in which online abuse can proliferate while responses remain fragmented or reactive.

Who is most affected and where abuse occurs

Findings from stakeholder consultations, survivor testimonies, and questionnaire responses indicate that TFGBV in the Western Balkans six most frequently occurs within widely used digital communication environments. Social media platforms and messaging applications were consistently identified as primary spaces in which online harassment, threats, and NCII abuse take place. In addition, stakeholders and case evidence highlight the growing role of closed digital ecosystems, including private messaging groups and encrypted platforms, where non-consensual intimate content is shared, circulated, and amplified beyond public visibility. Platforms enabling rapid sharing of images, videos, and private communications facilitate not only the distribution of intimate content without consent, but also coordinated harassment, reputational attacks, and sustained patterns of abuse.

Prevalence and Forms of Technology-Facilitated Gender-Based Violence in the Western Balkans

The speed, scale, and cross-platform nature of digital environments significantly increase both the reach and persistence of harm, making containment and removal particularly challenging. While TFGBV can affect a broad range of individuals, evidence consistently shows that certain groups experience disproportionate exposure. Women and girls are the primary targets of online harassment and NCII abuse, particularly in contexts where gender stereotypes and discriminatory attitudes are embedded within both online and offline discourse.

Survivors navigating intimate relationships are also identified as a high-risk group, with NCII abuse frequently emerging in the context of current or former partnerships, where trust, coercion, and control intersect with digital technologies. At the same time, individuals with high public visibility face distinct forms of targeted abuse. Journalists, civil society activists, women human rights defenders, women in politics, and other public-facing figures are frequently subjected to coordinated harassment campaigns, threats, and gendered disinformation aimed at undermining their credibility and discouraging participation in public life. LGBTQ+ individuals and young people are also identified as particularly vulnerable, often experiencing both targeted harassment and broader patterns of online exclusion and abuse.

These patterns reflect the intersection between digital communication environments and existing social power dynamics. Individuals who are highly visible online or engaged in public discourse face increased exposure to coordinated attacks, while those in private or intimate digital interactions may be more vulnerable to coercion, manipulation, and non-consensual sharing of content.

The concentration of abuse within both open and closed digital environments underscores the importance of platform governance, digital literacy, online safety education, and accessible reporting mechanisms as part of broader responses to TFGBV. Understanding both who is most affected and where abuse most commonly occurs is essential for designing effective prevention strategies, improving victim support pathways, and strengthening collaboration between governments, civil society organisations, and digital platforms operating within the region.

Media-Reported Cases of NCII Abuse in the Western Balkans

Media reporting over the past five years highlights several high-profile incidents involving the non-consensual sharing of intimate images across the Western Balkans six. In Serbia, it has been revealed that multiple Telegram groups with tens of thousands of members exchanging explicit photographs of women without their consent. Similar patterns emerged in North Macedonia during the "Public Room" scandal, where thousands of intimate images of women and girls were circulated through Telegram groups. These cases demonstrate how NCII abuse frequently occurs in large digital networks,

Media overview snapshot

• An investigation in Serbia revealed multiple Telegram groups where thousands of users exchanged explicit photos and videos of women without consent. Such Telegram groups have become digital spaces where perpetrators anonymously exchange intimate images of women and girls without consent.

• One of the most prominent cases of digital sexual abuse in the region from North Macedonia. Members of the group circulated images alongside victims' phone numbers and social media profiles, encouraging harassment and sexual requests.
• A large Telegram network in Kosovo distributing intimate images of women and girls without consent. The group distributed intimate images and videos of women and girls without their permission and was later subject to criminal investigations.
• A recent high-profile case in Montenegro further illustrates the risks of NCII abuse. In 2026, explicit videos involving senior official circulated online.
• Female activists from the town of Kula (Serbia) reported in 2026. that their private intimate photos and videos were circulated online without consent following their participation in local protests and civic activism.

Key Findings

Regional Readiness to Address Technology-Facilitated Gender-Based Violence

The analysis conducted for this landscape report indicates that the Western Balkans region is in a transitional stage in responding to TFGBV, particularly NCII abuse. While awareness of digital forms of violence is increasing and some legislative progress has been made, institutional responses remain fragmented and uneven across countries. Findings from survivor narratives and practitioner insights further indicate that while systems are evolving, they are not yet experienced by victims as accessible, coordinated, or effective, with many survivors relying on informal or civil society-led support pathways rather than formal institutional responses.

The findings suggest that existing responses to NCII are largely embedded within broader gender-based violence or cybercrime frameworks rather than addressed as a distinct policy area. As a result, legal provisions, institutional responsibilities, and support mechanisms often operate without clear coordination or specialised protocols tailored to NCII abuse.

Key Findings

Legal and Policy Frameworks

Across the Western Balkans six, elements of technology-facilitated abuse are addressed through existing criminal codes, cybercrime legislation, and domestic violence frameworks. However, explicit legal recognition of NCII varies between jurisdictions, and in many cases the legal provisions addressing these offences remain fragmented across multiple legal domains, including criminal law, anti-discrimination legislation, domestic violence frameworks, cybercrime provisions, and data protection regulations. Regional legal assessments have found that many Western Balkan countries rely on broader criminal provisions rather than specific offences addressing digital forms of gender-based violence (*UNDP, Assessment of Legal, Policy, Institutional and Technological Frameworks on Technology-Facilitated Gender-Based Violence in the Western Balkans).*

Across the Western Balkans Six, legal provisions relevant to TFGBV are typically embedded within broader criminal offences such as harassment, stalking, threats, cybercrime, or violations of privacy and personal data. In practice, this results in reliance on indirect legal pathways, including harassment, coercion, and privacy violations, which do not fully capture the specific nature of NCII, particularly in cases where consent was initially given but later withdrawn.

Key Findings

Legislative reviews across the region also highlight the fragmentation of legal definitions and protections across different legal frameworks. Technology-facilitated violence may be addressed through a combination of criminal law, anti-discrimination legislation, domestic violence statutes, communications regulations, and data protection laws. However, these frameworks were largely developed before the emergence of widespread digital abuse and therefore do not consistently address harms committed through information and communication technologies. As a result, similar forms of abuse may be treated differently depending on the legal pathway used, creating uncertainty for investigators and prosecutors and limiting consistent protection for victims (UNFPA, *Legislative Roadmap for Preventing ICT-Facilitated Gender-Based Violence in Bosnia and Herzegovina, North Macedonia, Serbia and Kosovo*).

While some countries have introduced legislative provisions that may apply to the nonconsensual sharing of intimate images, explicit and clearly defined NCII offences remain limited or inconsistently formulated across jurisdictions (UNDP, *Assessment of Legal, Policy, Institutional and Technological Frameworks on Technology-Facilitated Gender-Based Violence in the Western Balkans).*

Council of Europe monitoring reports on the implementation of the Istanbul Convention similarly note that many states address forms of online violence through existing offences such as harassment, stalking, or privacy violations rather than through dedicated provisions targeting technology-facilitated abuse (Council of Europe, *GREVIO Monitoring Reports on the Istanbul Convention*).

Key Findings

Some legislative developments within the region demonstrate emerging recognition of digital forms of violence. For example, North Macedonia's Law on Prevention and Protection from Violence against Women and Domestic Violence explicitly recognises sexual harassment carried out through electronic communications, including online environments. Montenegro has introduced explicit criminal provisions addressing the non-consensual distribution of intimate images, with penalties of up to five years' imprisonment, reflecting emerging legislative recognition of NCII abuse within national criminal law.

Serbia has announced changes to its Criminal code to include unauthorised dissemination or threats to disseminate private photographs and sexually explicit videos. Such provisions represent early attempts to address technology-facilitated abuse more directly within legal frameworks, although similar explicit provisions remain limited across much of the region (UNFPA, Legislative Roadmap for Preventing ICT-Facilitated Gender-Based Violence).

Absence of clearly defined offences specifically addressing the non-consensual sharing or threats to share, of intimate images can create legal ambiguity and procedural challenges for investigators and prosecutors. In several jurisdictions, procedural frameworks also place additional burdens on victims, including requirements for private prosecution or repeated evidentiary submissions, which can deter reporting and prolong harm. Legislative analyses have also noted that many legal systems do not explicitly address situations where intimate images shared within consensual relationships are later distributed without consent following relationship breakdown, a pattern commonly observed in cases of NCII abuse.International research on NCII abuse highlights that reliance on general criminal provisions can complicate evidence collection, prosecution strategies, and victim protection in cases involving digital distribution of intimate content (DCAF, *Combating Image-Based Sexual AbuseOnline*).

The lack of consistent legal definitions across jurisdictions can also complicate cross-border cooperation in cases involving the online dissemination of intimate images. Technologyfacilitated violence frequently involves digital platforms operating across national boundaries, making effective responses dependent on legal clarity and cooperation between national authorities and technology companies
(UN Women, *The Dark Side of Digitalization: Technology-Facilitated Violence Against Women in Eastern Europe and Central Asia).*

Key Findings

Despite these challenges, recent policy discussions and legal reforms across the Western Balkans six indicate growing recognition of digital violence against women and girls as an emerging policy concern. Civil society organisations, international institutions, and regional initiatives have increasingly highlighted the need for clearer legal frameworks and coordinated responses to technology-facilitated abuse (Kvinna till Kvinna Foundation, *Women's Rights in the Western Balkans 2024*).

Stakeholder responses collected through the regional consultation further reinforce the challenges identified in the legal and policy landscape. Practitioners across the Western Balkans six frequently highlighted the absence of clear legal provisions, including reliance on general offences rather than specific NCII legislation and procedural complexity in applying existing laws, addressing TFGBV and NCII abuse as a key barrier to effective prosecution, particularly in cases involving digital evidence, cross-platform dissemination of images, and jurisdictional challenges. Several respondents noted that existing legislation often requires cases to be pursued through broader criminal offences or civil procedures, creating uncertainty for investigators and placing additional procedural burdens on victims seeking justice. Stakeholders also identified gaps in legal procedures related to digital evidence. Collection, cross-border cooperation, and the removal of harmful online content. In addition, many respondents emphasised that limited specialised training among law enforcement, prosecutors, and judges can further complicate the application of existing legal provisions in cases involving online abuse.

These findings suggest that while legal frameworks in the region contain provisions that may apply to NCII, the absence of clearly defined offences, specialised investigative protocols, and consistent institutional capacity continues to limit the effectiveness of legal responses to technology-facilitated abuse.

Several countries in the region are currently undergoing legislative reforms aimed at addressing digital harms more explicitly. Draft criminal code amendments and newly adopted laws on violence against women are expected to introduce clearer provisions related to technology-facilitated abuse. However, the absence of implementing bylaws, institutional capacity, and enforcement mechanisms remains a key barrier to their practical impact.

Key Findings

Institutional Capacity and Coordination

A recurring finding across stakeholder consultations relates to institutional fragmentation in responding to NCII cases. Responsibility for addressing digital violence is often distributed across multiple entities, including police cybercrime units, domestic violence services, prosecutors' offices, and gender equality bodies.

Stakeholders noted that coordination mechanisms between these institutions are often informal or case-dependent for NCII abuse. In practice, survivors encounter unclear reporting pathways and overlapping mandates, resulting in cases being redirected between institutions without clear ownership or resolution. In many instances, NCII cases fall between existing institutional mandates, with cybercrime units focusing primarily on financial or technical crimes and gender-based violence services focusing on offline forms of abuse. Stakeholder responses further suggest that coordination between government institutions and civil society organisations remains inconsistent across countries, with respondents reporting moderate to low levels of cooperation when addressing NCII cases.

Victim Support Infrastructure

Survivor evidence further indicates that victims frequently bypass formal institutions altogether, seeking support through personal networks or civil society organisations as a first step. This reflects both accessibility gaps and a broader lack of trust in institutional responses, with many survivors perceiving NGOs as more responsive, confidential, and capable of providing immediate support. Many organisations offer legal assistance, psychological counselling, and advocacy services related to digital violence.

However, stakeholders emphasised that specialised services specifically addressing NCII or other forms of digital abuse remain limited. In many cases, victims must navigate existing domestic violence services or general victim support mechanisms that may not be equipped to handle digital evidence, online harassment dynamics, or platform-related procedures. The absence of dedicated reporting mechanisms or specialised helplines for NCII abuse in several countries further complicates access to support for victims.

Key Findings

Survivor Pathways and Reporting Behaviour

Across the Western Balkans six, survivor pathways are non-linear and frequently systemavoiding. Rather than engaging formal institutions as a first step, victims most commonly seek support through friends, family members, or civil society organisations. Reporting to law enforcement or judicial authorities is often delayed or avoided altogether due to stigma, fear of victim-blaming, concerns about confidentiality, and lack of clarity regarding reporting procedures. In addition, survivors frequently report uncertainty around how to navigate both institutional systems and digital platforms, particularly in cases involving evidence collection or content removal. These dynamics contribute to underreporting, fragmented case handling, and prolonged harm, reinforcing the gap between formal system design and lived experience.

Technology-facilitated gender-based violence (TFGBV) cases, particularly those involving NCII abuse, often follow complex and fragmented response pathways. While legal frameworks and institutional actors exist across the Western Balkans six, survivors frequently encounter unclear reporting mechanisms, low awareness, overlapping institutional mandates, and limited specialised support services. Importantly, many survivors do not initially recognise their experiences as abuse, particularly when early behaviours occur within intimate or trustbased relationships. This delayed recognition significantly shapes the timing and nature of help-seeking.

In many cases, the first point of disclosure is informal rather than institutional. Survivors commonly confide in friends, family members, or trusted peers before approaching formal support mechanisms. When victims seek external assistance, they are most likely to contact civil society organisations, helplines, or online support services, which often act as first responders in cases of technology-facilitated abuse. Research across the region indicates that civil society organisations frequently provide legal advice, psychosocial support, and assistance navigating reporting procedures, compensating for gaps in formal institutional support systems.

Barriers to engaging with formal systems are not only procedural but also social and psychological. Survivors frequently report feelings of shame, self-blame, and fear of stigma or public exposure, particularly in cases where intimate images were initially shared consensually. Concerns about victim-blaming, reputational harm, and lack of confidentiality especially in smaller communities further discourage reporting and contribute to underreporting across the region.

Victim Journey and Response Pathways in NCII Cases

Where cases do enter formal reporting systems, victims may approach law enforcement agencies, cybercrime units, or prosecutors offices, particularly when the abuse involves threats, extortion, or large-scale distribution of intimate images. However, stakeholders across the Western Balkans six noted that institutional responses can be inconsistent, partly due to limited specialised training in digital evidence collection and the interpretation of legal provisions applicable to technology-facilitated abuse. In some cases, jurisdictional uncertainty between cybercrime units and general criminal investigators has resulted indelays or difficulties determining how cases should be pursued.

Another frequently cited challenge concerns content removal and platform engagement. Victims seeking to have intimate images removed often encounter complex reporting procedures on digital platforms, limited access to human support, and inconsistent outcomes. Survivors frequently perceive these processes as slow, impersonal, and ineffective, reinforcing a sense that once content is shared, it cannot be fully removed or controlled. As a result, civil society organisations, digital rights advocates, and international initiatives increasingly play a role in assisting victims with evidence preservation, reporting to platforms, and securing the removal of harmful content.

Cases frequently break down at early stages. Survivors report dismissive initial responses, limited understanding of digital evidence, and unclear procedures. In many instances, civil society organisations act as de facto coordinators, providing legal guidance, psychological support, and assistance with platform reporting where state mechanisms are insufficient. The absence of structured referral pathways results in duplication, delays, and retraumatisation, as victims are required to repeat their experiences across multiple institutions.

These patterns illustrate a broader structural challenge: while multiple institutions are involved in responding to NCII abuse, coordination between them is often limited. Existing gender-based violence response mechanisms, which were primarily designed to address offline violence, are not always equipped to manage the technical, legal, and cross-border dimensions of digital abuse. Strengthening referral pathways, improving coordination between law enforcement, victim support services, and digital platforms, and ensuring that survivors can access clear and trusted reporting mechanisms will be critical to building effective responses to NCII and broader forms of TFGBV.

Snapshot from Regional Consultations
Visit to Montenegro and Serbia

Stakeholder discussions in Belgrade highlighted systemic challenges in responding to technology-facilitated abuse. Participants emphasised that reported cases may represent only a small fraction of actual incidents, with estimates suggesting that as little as 2% of cases reach formal reporting channels. Institutional responses were described as fragmented and, at times, dismissive. Victims often encounter a lack of understanding at the first point of contact, leading many to seek support from civil society organisations instead of state institutions. Significant gaps were identified in support systems, particularly for adults, where services often diminish after the age of eighteen. Judicial processes were also noted as insufficiently prioritising victim safety, even in cases where perpetrators are convicted.

Participants stressed the importance of stronger regulatory frameworks, including enforceable obligations on technology platforms, such as defined takedown timeframes and meaningful financial penalties for non-compliance. The discussion also highlighted the need for scalable, technology-driven solutions, including proactive prevention tools, centralised reporting mechanisms, and cross-border cooperation frameworks.

Consultations in Podgorica reflected a growing recognition of technology-facilitated violence as a policy issue, alongside persistent challenges in implementation. While legal frameworks have advanced, stakeholders noted that institutional coordination remains limited, and operational responses are often reactive rather than proactive.

Participants highlighted gaps in professional capacity, particularly among law enforcement and judiciary, in handling digital evidence and understanding the dynamics of online abuse. Victim support services were described as uneven, with civil society organisations continuing to play a central role in providing assistance. Awareness levels among the public and professionals are increasing, but stigma and fear of reputational harm continue to discourage reporting. Stakeholders emphasised the need for clearer referral pathways, improved inter-agency coordination, and stronger engagement with digital platforms toensure timely content removal.

Overall, Montenegro was seen as demonstrating progress in legislative development, but requiring further investment in implementation, training, and system coordination.

Recommendations

The findings of this Landscape report suggest that future action in the Western Balkans six should be guided by a survivor-centred, rights-based, and whole-of-society approach that reflects both the Istanbul Convention's four-pillar model and emerging international practice on NCII abuse. As set out in SWGfL's Model National Framework for addressing NCII, effective responses require more than criminalisation alone: they depend on prevention strategies that address harmful norms and digital consent, protection systems that offer timely and trauma-informed support, prosecution pathways that are clear and enforceable, and integrated policies that connect government, civil society, law enforcement, regulators, educators, and industry. In the Western Balkans context, this means moving beyond fragmented or reactive responses towards coordinated systems that can prevent abuse, support victims quickly, hold perpetrators accountable, and engage digital platforms as part of the response architecture. Recent Council of Europe guidance on technology-facilitated violence against women calls for explicit criminalisation of NCII abuse, improved victim support systems, and stronger cooperation with digital platforms.

Best practice examples

The following examples illustrate emerging and established approaches to addressing TFGBV, including non-consensual intimate image (NCII) abuse. While no single model is universally transferable, these cases demonstrate key components of effective response systems, including legal clarity, institutional coordination, victim-centred services, and enforceable platform accountability.

United Kingdom – Integrated Victim Support and Platform Cooperation

The United Kingdom has developed one of the most operationally mature responses to NCII abuse, combining specialist victim support, law enforcement engagement, and platform cooperation.
The UK's Revenge Porn Helpline provides direct assistance to victims, including case management and support with reporting and content removal. Complementing this, StopNCII.org enables individuals to create a secure digital fingerprint (hash) of their intimate images on their own device, which is then used by participating platforms to proactively prevent the content from being uploaded globally. This integrated model demonstrates a full lifecycle approach to NCII, combining prevention, response, and platform engagement within a coordinated system. The United Kingdom has a clearly defined legal framework addressing NCII abuse, supported by criminal offences and strengthened by platform accountability measures under the Online Safety Act.

Best practice examples

Australia – Regulatory Enforcement and Platform Accountability

Australia provides a leading example of a regulatory approach to online harms through the Office of the eSafety Commissioner. The eSafety Commissioner has statutory powers to issue legally binding takedown notices, require platforms to remove harmful content within defined timeframes, and impose financial penalties for non-compliance. The office also provides direct reporting pathways and support services for victims of NCII abuse and other forms of online harm. This model demonstrates how regulatory frameworks can shift platform responses from voluntary cooperation to enforceable obligations, strengthening accountability and improving response times.

European Union – Harmonised Legal Framework for Cyber Violence

The European Union has introduced a comprehensive legal framework through Directive (EU) 2024/1385 on combating violence against women and domestic violence. The Directive explicitly recognises forms of cyber violence, including non-consensual sharing of intimate images, cyberstalking, and online harassment. It requires Member States to criminalise these behaviours, establish accessible reporting mechanisms, strengthen victim protection measures, and enhance cross-border cooperation. This framework is particularly relevant for Western Balkan countries engaged in EU accession processes, as it sets a clear standard for future legislative alignment.

Argentina – Integrated Legal Recognition of Digital Violence

Argentina has taken a comprehensive approach by integrating digital violence into broader legislation on violence against women. Through amendments commonly referred to as the "Olimpia Law", digital violence is explicitly defined as a form of gender-based violence, covering behaviours such as online harassment, coercion, and non-consensual image sharing. The law embeds these harms within existing frameworks for prevention, protection, and prosecution. This approach demonstrates the value of integrating technology-facilitated violence within wider gender-based violence frameworks, rather than addressing it solely through fragmented or isolated provisions.

Regional Priorities and Recommendations

Prevention

Prevention efforts across the Western Balkans should move beyond general online safety messaging and address the gendered drivers of technology-facilitated abuse. Drawing on the SWGfL Model National Framework, prevention should include age-appropriate education on privacy, bodily autonomy, consent, healthy relationships, and respectful digital behaviour, translated clearly into online contexts. Public awareness campaigns should also communicate that NCII abuse and related forms of abuse are harmful and, where applicable, criminal offences, while signposting victims and bystanders to available support services. In line with broader TFGBV prevention practice, these efforts should involve schools, parents, community actors, and where possible men and boys, while being culturally adapted and accessible across languages and formats.

Protection

Protection responses should be strengthened through survivor-centred, trauma-informed support pathways that recognise the urgency and distinct harms of digital abuse. The SWGfL framework highlights the importance of specialised services, helplines, legal support, and coordination between organisations supporting survivors of domestic violence, sexual violence, stalking, trafficking, and NCII abuse. For the Western Balkans, this suggests the need to adapt existing victim support systems so they can respond to digital evidence, privacy risks, rapid content dissemination, and the psychological consequences of NCII abuse. Sustained and diversified funding for specialised services is essential, particularly in under-resourced or institutionally fragile settings, so that support does not depend solely on short-term project cycles.

Regional Priorities and Recommendations

Prosecution

In line with the prosecution pillar of the Istanbul Convention, legal and justice responses should provide clear pathways to accountability for perpetrators of NCII abuse. This includes improving legal clarity around digital-specific offences and reducing reliance on indirect legal provisions (e.g. harassment, privacy violations) which currently limit consistent prosecution of NCII cases, reducing ambiguity in the treatment of non-consensual image sharing, threats to share, and creation of synthetic sexual content, and ensuring that police, prosecutors, and judges have the training and tools needed to investigate and prosecute such cases effectively.

The SWGfL framework also underscores that responses should not stop at formal criminalisation: implementation guidance, platform cooperation, trusted reporting channels, and the use of privacy-protective technological tools are necessary to make justice systems operationally effective in a cross-border digital environment. This is particularly relevant in the region, where existing analysis already points to fragmented and indirect legal coverage approaches, uneven institutional capacity, and the need for stronger coordination with private-sector actors and digital platforms.

Regional Priorities and Recommendations

Integrated Policies

The strongest lesson from both the stakeholder consultations and the SWGfL model is that NCII abuse cannot be addressed through isolated interventions. Integrated policies are needed to connect law, victim support, education, data systems, and platform governance within a coherent national and regional response. The SWGfL framework emphasises multistakeholder coordination, ethical data governance, international cooperation, and engagement with industry to improve reporting, takedown, transparency, and safety-bydesign measures. For the Western Balkans six, this points to the need for national coordination mechanisms, common referral protocols, improved data collection, stronger cross-border cooperation, and clearer engagement with technology companies.

It also suggests that governments and regional actors should consider supporting trusted flagger arrangements, platform protocols, and the adoption of privacy-preserving tools such as image hashing, where appropriate, while ensuring such measures remain grounded in human rights and survivor protection. Overall, the regional priority should be to build systems that are not only legally compliant, but practically usable, survivor-centred, and institutionally coordinated. The Istanbul Convention's 4Ps provide the normative structure for this work, while the SWGfL Model National Framework offers a practical operational lens for addressing NCII within the broader TFGBV landscape. Together, they suggest that progress in the Western Balkans six will depend on combining prevention and societal norm change, accessible protection and support services, credible accountability mechanisms, and integrated public policy and legislation that reflects the realities of a fast-moving digital environment.

References

Assessment of Legal, Policy, Institutional and Technological Frameworks on Technology-Facilitated Gender-Based Violence in the Western Balkans. United Nations Development Programme (UNDP), 2025.

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

UN Women. Repository of UN Women's Work on Technology-Facilitated Gender-Based Violence. UN Women, 2024.

UNFPA. Legislative Roadmap for Preventing ICT-Facilitated Gender-Based Violence in Bosnia and Herzegovina, North Macedonia, Serbia and Kosovo. United Nations Population Fund.

DCAF. Combating Image Based Sexual Abuse Online: Legal Frameworks and Policy Responses. Geneva Centre for Security Sector Governance.

Council of Europe. Convention on Preventing and Combating Violence Against Women and Domestic Violence (Istanbul Convention) – Country Monitoring and Implementation Reports.

Council of Europe. Recommendation CM/Rec(2026)2 on Combating Technology-Facilitated Violence Against Women and Girls.

International Telecommunication Union (ITU). Digital Development Country Profiles: Serbia and North Macedonia. ITU Regional Office for Europe.

UNDP Kosovo. Digital Development Profile. United Nations Development Programme. Western Balkans InfoHub. Kosovo in the Digital Agenda of the Western Balkans.

References

Western Balkans InfoHub. Kosovo in the Digital Agenda of the Western Balkans.
Kvinna till Kvinna Foundation. Women's Rights in the Western Balkans. 2024 and 2025.

Revenge porn Helpline reports 2015 - 2024

National Democratic Institute (NDI). Violence Against Women in Politics in Southeast Europe.

OSCE Office for Democratic Institutions and Human Rights (ODIHR). Strategies for Preventing Violence Against Women in Politics.

What Works to Prevent Violence Against Women and Girls Global Programme. Research and evidence reviews on gender-based violence prevention.

CARE. Foundational Elements for Gender-Based Violence Programming in Development.
USAID.

The Prevention Collaborative. Rapid Guide to Collecting Survey Data on Gender-Based Violence.

Pornographic Deepfakes: The Case for Federal Criminalization of Revenge Porn's Next Tragic Act – Delfino, 2019.

Global Women's Institute. Gender-Based Violence Research, Monitoring, and Evaluation: A Manual and Toolkit for Researchers and Practitioners. George Washington University.

References

UNICEF. Research on gender-based violence and its impacts on women and girls in digitaland social environments.

McGlynn, C., Rackley, E., & Houghton, R. (2017). Beyond 'Revenge Porn': The Continuum of Image Based Sexual Abuse. Feminist Legal Studies.

World Bank, Global Women's Institute, and Inter-American Development Bank. Violence Against Women and Girls Resource Guide.

VAWG Helpdesk. Mainstreaming Gender-Based Violence in Development Programmes.
Foreign, Commonwealth & Development Office.

National criminal codes, legal provisions, and legislative materials of Albania, Bosnia and Herzegovina, Kosovo, Montenegro, North Macedonia, and Serbia relating to privacy, harassment, cybercrime, and sexual offences.

Stakeholder consultations, expert interviews, and questionnaire responses collected during the preparation of this report.

Landscape report on NCII abuse in Western Balkans

Date: March, 2026.
Prepared for FCDO
Written By David Wright & Boris Radanović
South West Grid for Learning