ANALYSIS OF CASES OF TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN IN BOSNIA AND HERZEGOVINA

Council of Europe project
"Combating digital and sexual violence against women in Bosnia and Herzegovina II"

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Cover design and layout:
art studio DK

Picture
© Shutterstock

Council of Europe
F-67075 Strasbourg Cedex
www.coe.int

ANALYSIS OF CASES OF TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN IN BOSNIA AND HERZEGOVINA

Prepared by
Gorica Ivić and Selma Badžić

November 2025

Council of Europe

Table of contents

GLOSSARY AND ACRONYMS 5

EXECUTIVE SUMMARY 7

I. INTRODUCTION 12

Objectives of the study 14

Overview of the relevant laws and statistics in Bosnia and Herzegovina 15

Methodology 19

II. MAIN FINDINGS FROM THE CASE LAW ANALYSIS: COURT PRACTICE IN THE CONTEXT OF PROSECUTING DIGITAL VIOLENCE AGAINST WOMEN 21

Findings: Republika Srpska and Brčko District 21

Findings: Federation of Bosnia and Herzegovina 28

III. MAIN FINDINGS FROM KEY INFORMANT INTERVIEWS: JUDGES AND PROSECUTORS 34

Findings: Republika Srpska and Brčko District 34

Findings: Federation of Bosnia and Herzegovina 38

IV. MAIN FINDINGS FROM THE QUESTIONNAIRE: MINISTRIES OF INTERNAL AFFAIRS 41

Findings: Federation of Bosnia and Herzegovina 41

Findings: Republika Srpska 42

V. MAIN FINDINGS FROM THE IN-DEPTH VICTIM INTERVIEWS: WOMEN SURVIVORS 44

Findings: Republika Srpska 44

Findings: Federation of Bosnia and Herzegovina 46

VI. CONCLUSIONS AND RECOMMENDATIONS 49

Conclusions 49

Key recommendations 52

ANNEX I: NOTE ON TERMINOLOGY 55

ANNEX II: RESEARCH TOOLS – INTERVIEW QUESTIONS AND QUESTIONNAIRE 57

REFERENCES 61

Glossary and acronyms

Accused	Accused is the term used in this report to refer to a person who is believed to have committed a crime and has been charged with an offence, but has not yet been found guilty.
BiH	Bosnia and Herzegovina
CC	Criminal Code
Digital dimension of violence against women	The term "digital dimension of violence against women" is employed to emphasise the fact that this harmful behaviour disproportionately targets women and girls and forms a central element of their experiences of gender-based violence against women. It is violence perpetrated against women and girls that is rooted in the same context of women's inequality and men's sense of entitlement as the psychological, sexual and physical violence experienced by women and girls in the offline world[1]
Digital evidence	Digital evidence refers to the practice of recovery, seizure and investigation of material found across digital and electronic devices which store and capture data
Doxing	Doxing is the act of sharing online a target's personal information (phone number, e-mail address, home address, professional contacts) without consent, to encourage abuse
FBiH	Federation of Bosnia and Herzegovina
GREVIO	Group of Experts on Action against Violence against Women and Domestic Violence
GREVIO's baseline evaluation report on Bosnia and Herzegovina	GREVIO's (Baseline) Evaluation Report on legislative and other measures giving effect to the provisions of the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention) Bosnia and Herzegovina
Internet intermediaries	Internet intermediaries refer to entities that facilitate interactions on the internet between natural and legal persons by offering and performing a variety of functions and services and include internet service providers (ISPs), search engines and social media platforms.
IP	Internet Protocol
Istanbul Convention	The Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence
KM	Convertible mark (monetary unit in Bosnia and Herzegovina)

1 GREVIO General Recommendation No. 1 on the digital dimension of violence against women, paragraph 24.

Online technology-facilitated violence against women	GREVIO's understanding of the concept of violence against women in its digital dimension encompasses both online aspects (activities performed and data available on the internet, including internet intermediaries on the surface web as well as the dark web) and technology-facilitated (activities carried out with the use of technology and communication equipment, including hardware and software) harmful behaviour perpetrated against women and girls[2]
Perpetrator	Perpetrator is a non-legal term used in this report to refer to a person who commits violence against women. In this report, it also refers to those persons who have been convicted of a criminal offence, and therefore is used instead of such terms as "offender" or "convicted person"
SIM card	Subscriber Identity Module card
SMS	Short Message Service
Technological tools	Technological tools which may be misused by abusers to stalk, harass, surveil, and control victims include smartphones, cameras and other recording equipment, global positioning systems (GPS) or satellite navigators, other internet-connected devices such as smart watches, fitness trackers and smart home devices as well as software such as spyware or other mobile applications that may facilitate violence
VAW	Violence against women
Victim	Victim is the term used in this report to refer to the individual who has experienced digital violence but is not intended to convey a lack of agency on the part of the person victimised or to imply guilt with respect to an accused person

2 GREVIO General Recommendation No. 1 on the digital dimension of violence against women, paragraph 23.

Executive summary

The objective of this study is to analysis the justice institutional response to violence against women in its digital dimension in Bosnia and Herzegovina, using the GREVIO General Recommendation No. 1 on the digital dimension of violence against women as the analytical framework.[3] Digital violence against women, which includes forms of violence that take place partly or entirely in the digital sphere, is often accompanied by other forms of violence that occur in the offline world. Such violence encompasses a wide range of acts online or through technology that are harmful to women, including online harassment, threats, blackmail, revenge pornography, and misuse of personal data. GREVIO General Recommendation No. 1 emphasises the seriousness of the digital dimension of violence against women and the need for comprehensive judicial responses to provide adequate protection to victims and ensure perpetrator accountability.

This study was conducted by representatives of the Foundation United Women Banja Luka and the Centre of Women's Rights, Zenica, and implemented within the Council of Europe project "Combating digital and sexual violence in Bosnia and Herzegovina".

The study used quantitative and qualitative research methods. The quantitative study consisted of analysing a sample of 18 final judgments of cases involving violence against women and domestic violence in which there were elements of digital violence. The qualitative study involved three techniques: interviews with key informants from the judiciary and prosecution; questionnaires sent to relevant Ministries of Internal Affairs; and in-depth interviews with women survivors of digital violence.

3 GREVIO General Recommendation No. 1 on the digital dimension of violence against women, paragraph 18.

Findings

The key findings from this study are as follows.

A review and evaluation of more than 400 cases of violence against women, including domestic violence from the entities of the Federation of Bosnia and Herzegovina and Republika Srpska, and Brčko District, of which approximately 250 cases involved final verdicts, showed that only 18 final judgments were identified to include elements of online technology-facilitated violence against women. When compared with the fact that violence against women committed in the digital sphere has steeply risen in the last few years in Bosnia and Herzegovina, with 60% of calls received by the telephone helplines being related to such cases,[4] this number clearly indicates a significant lack of recognition and prosecution of online technology-facilitated violence within the justice system.

The case law analysis revealed the frequent practice of using plea agreements, which resulted in light sentences for the perpetrators, and the evidence not being thoroughly examined due to the summary procedure used in plea agreements. The study also found that in the cases where the criminal law sanctions were pronounced after a trial and conviction, such as in cases of domestic violence and exploitation of a child or minor for the purpose of pornography, the sentences were also relatively mild, most being suspended sentences. The case law analysis also revealed that in no case was an expert opinion used to assess the impact of online technology-facilitated violence on the mental health of the victims. This leads to the concern of whether the current criminal justice system is achieving the purpose of general and special prevention of digital violence and effective protection for its victims.

The study also found deficiencies in the procedural laws which make it challenging to effectively investigate and prosecute criminal acts of violence against women with a digital dimension. Interviews with judges and prosecutors revealed challenges in collecting, preserving, and evaluating digital evidence. Moreover, the lack of technical equipment, poor knowledge of digital evidence methods, and technological barriers often hindered effective case processing. Those interviewed also emphasised problems relating to the legality of the evidence, that is whether the evidence was obtained in the manner prescribed by law. Also discussed was the lack of technology experts who have an important role in managing digital evidence. The evidentiary action of searching computer systems, devices for storing computer and electronic data, mobile phones and other similar devices, according

4 GREVIO's baseline evaluation report on Bosnia and Herzegovina, paragraph 117.

to the provisions of the applicable criminal procedure law, can only be undertaken with the assistance of these persons. Furthermore, the interviews and questionnaires noted challenges due to the fact that the term "digital evidence" was not defined by the procedural legal framework in force in Bosnia and Herzegovina. A number of those interviewed believed it would be expedient to reform the procedural law to ensure it describe procedures in relation to digital data. The majority of those interviewed were of the view that the absence of a definition of "digital evidence" and clear procedures for the admissibility of such evidence represented a serious challenge to legal and proper judgments.

The study found that most victims interviewed did not feel protected, even after the institutions responded to their reports of digital violence. A number of victims also highlighted situations in which they were given wrong instructions about providing evidence of online technology-facilitated violence, which ultimately resulted in their cases being rejected by the courts and the accused persons' acquittal.

The study also found that most victims interviewed only reported the online technology-facilitated violence after they were exposed to continuous threats of death and blackmail, and when these threats included their family members. This indicates the need for greater awareness of the importance of recognising the first signs of digital violence, in order to avoid serious traumatic consequences. The majority of victims interviewed indicated that the digital dimension of the violence they experienced was often not isolated from violence in their offline world and that modern technologies gave the perpetrators the opportunity to abuse them continuously and for a long time, regardless of their physical separation from the perpetrator and leaving the violent relationship.

The questionnaire responses from the Ministries of Internal Affairs indicated that police structures confirmed the need for additional education of police officers. Their responses expressed the view that proper identification and preservation of digital evidence is key to conducting an effective investigation and achieving justice for victims.

Official statistics from the relevant Ministries of Internal Affairs on the number of reports of criminal acts of violence against women and domestic violence that have elements of digital violence are not publicly available, nor do they appear to be uniform at the national level. However, the data collected from the Ministries of Internal Affairs of Republika Srpska indicated a growing trend of reported cases of violence against women with a digital dimension, an increase of 30% in 2023 compared to 2022.

Recommendations

From these findings, recommendations follow.

In order to improve the response of judicial institutions to acts of digital violence against women, it is necessary to invest additional efforts to align legislation at all levels in Bosnia and Herzegovina with the requirements of international standards. More specifically, in order to provide victims of digital violence with consistent protection and support, it is necessary to harmonise the criminal laws with the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention) to ensure that all forms of online technology-facilitated violence against women are comprehensively covered.

Strengthening the judicial response to digital violence also requires strengthening of procedures and reforms to procedural rules. Specifically, all entities of Bosnia and Herzegovina should consider defining precise procedures for the recovery, seizure and investigation of material found across digital and electronic devices which store and capture data. A clear definition of the term "digital evidence" and the establishment of prescribed procedures for dealing with such evidence would assist prosecutors and judges in handling these cases.

In order to ensure effective prosecution and punishment for online technology-facilitated violence against women, there is a need to introduce mandatory training for judges, prosecutors and police officers. Such training could familiarise them with the digital forms of violence against women, increase their capacity in the effective use of digital evidence, and how to provide a victim-centered approach. Moreover, in order to strengthen the institutional capacity of judicial institutions there is need to consider the provision of modern technical equipment and specialised professional support for the analysis and preservation of digital evidence.

In order to ensure that protection measures are responsive to forms of domestic violence perpetrated online or via information communication technologies and to other digital manifestations of violence against women, all entities need to ensure that risk assessments include an understanding of the harm caused by the digital sphere and how the dynamics of digital violence contribute to risk.

In order to contribute to prevention and early recognition of online technology-facilitated violence, it is recommended that gender mechanisms and civil society organisations work with the justice institutions to conduct comprehensive

awareness campaigns and education of the general population, including those who are victims of digital violence. This could focus on the early recognition of various manifestations of violence against women that can take place partially or fully in the digital sphere. This is of importance in order to influence early reporting, reduce the negative stigma on the victim and stop such violence.

Considering the trend of growth and the continuous advancement of technology, it is recommended that the justice institutions develop tools and methodology for recording and accurately monitoring acts of online technology-facilitated violence against women. This data would enable evidence-informed practices, from the planning of prevention programs, to the improvement of the institutional response.

I. Introduction

Violence against women, including domestic violence, is one of the most serious forms of gender-based human rights violations. Technology, in particular the technology used in online and digital spheres, has been amplifying or facilitating gender-based violence against women for many years. Such violence encompasses both online activities and technology-facilitated activities that are harmful to women, including the use of digital devices to harass, stalk, intimidate, or humiliate women. Digital violence against women is often accompanied by other forms of violence that occur offline. In Bosnia and Herzegovina, it most often takes place on social networks, via e-mail, text messages, in the form of sending disturbing and threatening messages, spreading lies, publishing private information, including explicit sexual content.[5]

The Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) adopted General Recommendation No. 1 on the digital dimension of violence against women on October 20, 2021, to provide guidance to states parties to prevent and combat this phenomenon.[6] The GREVIO General Recommendation emphasises that the digital dimension of violence against women encompasses a wide range of acts online or through technology, which are part of the continuum of violence to which women and girls experience due to their gender, including domestic violence. It highlights the need for digital violence to be considered a legitimate and equally harmful manifestation of violence to which women and girls are exposed offline. In this regard, GREVIO indicates that the digital dimension of violence against women and girls includes activities carried out using the internet, data available online, such as on social networks and internet search engines, as well as activities carried out with the use of technology and communication equipment, that harm women

5 Based on interviews with beneficiaries of the specialised services of the Center of Women's Rights from Zenica and Foundation United Women Banja Luka, and based on interviews with women who have experienced digital dimension of violence against women.

6 GREVIO General Recommendation No. 1 on the digital dimension of violence against women, paragraph 18.

and girls. Technology and communication equipment include smartphones, cameras, other recording devices, GPS systems, or other equipment that can be connected to the internet and misused for stalking, harassment, monitoring, or controlling victims of violence.[7] The GREVIO General Recommendation emphasises the seriousness of the digital dimension of violence against women and the need for comprehensive judicial responses to provide adequate protection to victims and ensure perpetrator accountability.

While there is no universal typology or definition of behaviours or actions that covers all forms of violence against women perpetrated online or through technology, GREVIO, in its General Recommendation, lists the following behaviours as coming under the broad definition of gender-based violence against women: "Non-consensual image or video sharing, coercion and threats, including rape threats, sexualised bullying and other forms of intimidation, online sexual harassment, impersonation, online stalking or stalking via the Internet of Things as well as psychological abuse and economic harm perpetrated via digital means against women and girls".[8]

Bosnia and Herzegovina signed and ratified the Istanbul Convention. As such, Bosnia and Herzegovina has the obligation to take the necessary legislative and other measures to exercise due diligence to prevent, investigate, punish and provide reparations for "any act of gender-based violence against women that causes or may cause physical, sexual, psychological or material harm or suffering to women, including the threat of such violence, coercion or arbitrary deprivation of liberty, regardless of whether it occurs in public or private life".[9] GREVIO General Recommendation No. 1 confirms that the digital dimensions of violence against women falls within the scope of this definition. In addition, many of the forms of digital violence come within the remit of intentional behaviour which states parties to the Istanbul Convention are required to criminalise. These include online psychological violence, online or stalking committed in the digital sphere and sexual harassment online or through digital means.[10] Moreover, Bosnia and Herzegovina signed and ratified the Council of Europe Convention on Cybercrime (Budapest Convention) and thus committed itself to ensure the implementation of criminal policies aimed at protecting society from cybercrime,

7 GREVIO General Recommendation No. 1 on the digital dimension of violence against women, paragraph 23.

8 GREVIO General Recommendation No. 1 on the digital dimension of violence against women", paragraph 33.

9 Istanbul Convention, Article 3, paragraph a.

10 See Articles 33, 34 and 36, Istanbul Convention and GREVIO General Recommendation No. 1 on the digital dimension of violence against women", paragraphs 36-48.

especially through the adoption of appropriate legislation and improvement of international cooperation.[11]

Objectives of the study

The study is conducted within the Council of Europe project "Combating digital and sexual violence in Bosnia and Herzegovina" by representatives of the Foundation United Women Banja Luka and the Centre of Women's Rights, Zenica. The project supports reforms to the legal, policy and institutional frameworks, among other issues, that are focused on ensuring victims of digital violence are able to enjoy their rights in law and practice.

The overall purpose of the study is to support the development and holistic implementation of evidence-based laws and practices for combating digital violence. The overall objective of the study is to assess the justice institutional response to violence against women taking place in the digital sphere in Bosnia and Herzegovina, using GREVIO General Recommendation No. 1 on the digital dimension of violence against women as the analytical framework.

Specific objectives of the study are as follows:

- To review and evaluate domestic judicial practice in the entities of the Federation of Bosnia and Herzegovina and Republika Srpska, and the administrative unit of Brčko District.
- To examine how cases of violence against women, with an emphasis on digital dimension of violence, are treated in the courts of Bosnia and Herzegovina, to determine how the nature of online technology-facilitated violence against women is defined in the judicial procedure and what measures were taken and sentences given in these cases.
- To identify the approaches taken in processing cases of online technology-facilitated violence against women, such as in collecting and evaluating evidence.
- To propose recommendations for improving the justice institutional response in ensuring victims of digital violence can enjoy their rights in law and practice.

11 The Convention on Cybercrime entered into force with respect to Bosnia and Herzegovina on September 1, 2006; publication of the "Official Gazette of BiH" – International Treaties No. 06/2006) and the Additional Protocol to the Convention on Cybercrime, Concerning the Criminalisation of Acts of a Racist and Xenophobic Nature Committed through Computer Systems entered into force with respect to Bosnia and Herzegovina on 01 September 2006; publication of the "Official Gazette of BiH" – International Treaties No: 06/2006).

Overview of the relevant laws and statistics in Bosnia and Herzegovina

There are three distinct criminal justice systems that co-exist in Bosnia and Herzegovina, in addition to the Criminal Code of Bosnia and Herzegovina which regulates crimes against the state and crimes with an international element. These are Republika Srpska, the Federation of Bosnia and Herzegovina and Brčko District. Each criminal code contains general offences, such as domestic violence and endangering safety, that can apply to conduct that occurs in the digital sphere. This section highlights specific offences that articulate a digital element.

The Federation of Bosnia and Herzegovina Criminal Code

The Criminal Code of the Federation of Bosnia and Herzegovina does not contain specific criminal offences defining online technology-facilitated violence against women. However, the criminal offences of "unauthorised optical recording"[12] and "unauthorised tapping and sound recording"[13] could be used in certain cases of digital violence.

- The offence of "unauthorised optical recording" criminalises the taking of a photograph, film or other recording of another person in their personal premises without that person's consent, or the direct passing on or displaying such a photograph to a third person or enabling the third person in some other way to have direct access to the photograph. Aggravated forms of the offence are provided if the photograph or film is of a child with an aim of developing pornographic material.
- The offence of "unauthorised tapping and sound recording" criminalises using special devices without authorisation to tap or record a conversation or a statement which was not intended for them, or enables an uninvited person to have knowledge of such a conversation or statement that was tapped or recorded or to tap or record somebody else's messages from a computer without authorisation.

It should be noted that the above provisions are gender-neutral and do not acknowledge the structural nature of violence against women and girls.

12 Criminal Code of the Federation of BiH, Article 189.
13 Criminal Code of the Federation of BiH, Article 188.

Republika Srpska Criminal Code

The criminal legal protection for the digital dimension of violence against women in Republika Srpska is still in its infancy. Amendments to the Criminal Code of Republika Srpska in 2023 introduced two criminal offences enabling the prosecution and punishment of violence committed in the digital sphere.

- The offence of "unauthorised publication and display of another person's writing, portrait, or recording"[14] criminalises the publication or display of writings, portraits, photographs, videos, films, or sound recordings of a personal nature without the consent of the person who created the writing or to whom the writing relates, or without the consent of the person depicted in the portrait, photograph, video, or film, or whose voice was recorded on the sound recording, or without the consent of another person whose consent is required by law, and such publication or display had or could have had harmful consequences on the personal life of that individual[15]. Aggravated forms of the offence are provided if the act was committed against a family member or another person with the intent to harm that person's reputation[16], as well as if the commission of the act caused serious harm to the person's health or resulted in the victim's death[17].
- The offence of "abuse of sexually explicit photographs and videos"[18] allows for the prosecution of privacy violations through the sharing of sexually explicit photographs or recordings made with the person's consent for personal use, which are then shared with third parties by abusing the trust in that relationship and without the other person's consent[19]. Abuse is also recognised when the perpetrator violates the privacy of another person by creating a new or altering an existing sexually explicit photograph or recording and using it as if it were authentic[20]. The law provides for an aggravated form of this offence if it is committed "via a computer system or network or in another manner that makes the photograph or recording available to a larger number of people"[21], recognising the need for protection from abuse and violence through the digital sphere.

14 Criminal Code of Republika Srpska, Article 156a.
15 Criminal Code of Republika Srpska, Article 156a, paragraph 1.
16 Criminal Code of Republika Srpska, Article 156a, paragraph 2.
17 Criminal Code of Republika Srpska, Article 156a, paragraph 3.
18 Criminal Code of Republika Srpska, Article 170a.
19 Criminal Code of Republika Srpska, Article 170a, paragraph 1.
20 Criminal Code of Republika Srpska, Article 170a, paragraph 2.
21 Criminal Code of Republika Srpska, Article 170a, paragraph 3.

In Republika Srpska, amendments were also made to the provisions regulating the criminal offence of "sexual harassment"[22] recognising an aggravated form when it is "committed using a computer network or another form of communication"[23].

Earlier amendments to the Criminal Code of Republika Srpska in 2017 introduced a special chapter, Chapter XV, to regulate criminal offences of "sexual abuse and exploitation of children". A specific offence, "exploitation of a computer network or other technical means of communication for the commission of sexual abuse or exploitation of a child"[24] criminalises arranging a meeting with a child over the age of fifteen via a computer network or other technical means of communication, with the intention of committing sexual intercourse or other sexual acts, producing pornographic material, or other forms of sexual exploitation, and appearing at the agreed location for the meeting.[25] A more serious form of the offence exists if it is committed against a child under the age of fifteen.[26]

It should be noted that the above provisions are gender-neutral and do not acknowledge the structural nature of violence against women and girls.

Brčko District Criminal Code

While the Brčko District Assembly adopted amendments to the Criminal Code[27] in 2020 introducing new criminal offences and amending existing ones in accordance with the Istanbul Convention, such as the new criminal offences of female genital mutilation, forced sterilisation, stalking, psychological violence, sexual harassment and forced marriage; these did not specifically cover such violence in the digital dimension.

Existing statistics

The study was unable to collect specific data on the reporting and prosecuting of cases involving a digital dimension of violence against women for the Federation of Bosnia and Herzegovina and Brčko District. This is mainly due to differences in legislation and classification of offences.

22 Criminal Code of Republika Srpska, Article 170.
23 Criminal Code of Republika Srpska, Article 170, paragraph 3.
24 Criminal Code of Republika Srpska, Article 178.
25 Criminal Code of Republika Srpska, Article 178, paragraph 1.
26 Criminal Code of Republika Srpska, Article 178, paragraph 2.
27 Criminal Code of Brčko District of BiH.

The following data was collected from two official sources in Republika Srpska; however, a review reveals some inconsistencies. Data from the High Judicial and Prosecutorial Council of Bosnia and Herzegovina[28] on the structure of crime in the country indicate that between 2018 and 2023, police in Republika Srpska received 10 reports of the criminal offence of "exploitation of a computer network or other technical means of communication for the commission of sexual abuse or exploitation of a child". Of those, investigations were ordered in eight cases, the competent prosecutor's office issued orders to terminate investigations in three cases, and four indictments were filed. Courts in Republika Srpska delivered three guilty verdicts, including two prison sentences and one suspended sentence, while in one case, an acquittal was issued. In contrast, statistics from the Ministry of Internal Affairs of Republika Srpska indicate a significant increase in reports of this crime in 2023. A total of 12 cases were recorded, compared to only one case in 2022[29]. However, the available data is not sex-disaggregated for the victims and perpetrators, making it impossible to determine how many cases involved girl victims of sexual abuse or exploitation through digital means. Statistical data for the reporting and prosecution of the criminal offences introduced in 2023 are not yet available. The fact that the statistics from the various justice institutions reveal such different statistics highlights the need for reform to the criminal administrative database process to ensure recognition of these crimes.

Findings from the GREVIO baseline evaluation report on Bosnia and Herzegovina

In essence, GREVIO noted in its baseline evaluation report on Bosnia and Herzegovina that some degrees of alignment to the Istanbul Convention standards has been achieved in terms of criminal legislation and specifically notes the positive developments in Republika Srpska.[30] However, GREVIO also noted that in the absence of data on investigation and prosecution, it is difficult to assess to what extent general criminal provisions are applied to any digital manifestation of violence against women.[31]

28 High Judicial and Prosecutorial Council of Bosnia and Herzegovina, Annual Reviews of the Structure of Crime in BiH 2018-2023.

29 See information on the state of security in Republika Srpska for 2023, Ministry of Internal Affairs of Republika Srpska, page 9: https://mup.vladars.rs/index.php?vijest=66&vrsta=statistike&stat=1

30 GREVIO's baseline evaluation report on Bosnia and Herzegovina, paragraph 200.

31 GREVIO's baseline evaluation report on Bosnia and Herzegovina, paragraph 213.

Methodology

Taking into consideration the objectives, the study used quantitative and qualitative research methods.

The quantitative study consisted of analysing a sample of 18 final judgments of cases involving violence against women and domestic violence in which there are elements of digital violence. Out of the 18 case samples, nine judgments were from the Federation of Bosnia and Herzegovina and nine judgments were from Republika Srpska and Brčko District. The case sample involved the following categories of criminal offences: "domestic violence" (11 judgments); "endangering security" (2 judgments); "sexual harassment" (1 judgment); "exploitation of a child or minor for pornographic purposes" (2 judgments); "introducing a child to pornography" (1 judgment); and "murder" (1 judgment). The focus of the case law analysis was on the identification of criminal offences, the method of prosecution, defining the nature of online technology-facilitated violence against women, and the prescribed penalties and measures of the courts.

The qualitative study involved three techniques:

1. Interviews with the key informants from the judiciary and prosecution.
2. Open-ended questionnaire sent to the Ministries of Internal Affairs.
3. In-depth interviews with women survivors of digital violence.

Ten interviews were conducted with judges and prosecutors who had experience in prosecuting and adjudicating cases of violence against women in which a digital dimension was also present. Interview questions were prepared to seek their perspectives on the challenges they face when proving or processing these cases and to gain insight into the legislative framework and practices such as assessment of evidence, indictments, court procedure and sentencing.

A questionnaire was sent to entity and cantonal Ministries of Internal Affairs to gain insight into the issue of recording the digital dimension of violence against women by the police. The questionnaire consisted of five questions that covered issues such as challenges in recording and providing protection to the victims as well as opinions and positions on legal changes. Responses were received from 9 out of 10 cantonal ministries[32], and the Ministry of Internal Affairs of the Federation of Bosnia and Herzegovina and Republika Srpska.

32 No response was received from the Ministry of Internal Affairs of Una-Sana Canton.

Fifteen interviews were conducted with women who reported violence that involved a digital dimension. The women survivors who were interviewed had been beneficiaries of specialised support services of the Foundation United Women Banja Luka and the Center of Women's Rights from Zenica. Interview questions covered the victim's experience with digital violence, her reporting of such violence and her experiences or lack thereof with support and protection from Institutions. The interviews were conducted in a safe environment, respecting confidentiality principles and with the consent of the participants.

The research instruments that have been developed for the qualitative study are contained in Annex II.

II. Main findings from the case law analysis: Court practice in the context of prosecuting digital violence against women

A note about the selection of cases for the case law analysis

The final judgments that were the subject of this case law analysis were selected from a larger database that had been developed during a criminal trial monitoring project. Specifically, from 2021 to 2023, the Foundation United Women Banja Luka and the Center of Women's Rights from Zenica had collected data from 464 cases related to violence against women and domestic violence. While the digital dimension of violence has been noted in cases other than the 18 selected, predominantly in cases of domestic violence, these cases have not been included in this analysis as they have not reached final judgment. The analysis showed that from the database, which includes more than 250 final judgments in cases of violence against women, only 18 final judgments were identified as including elements of online technology-facilitated violence against women.

Findings: Republika Srpska and Brčko District

Percentage of completed VAW cases in court that have elements of digital violence

From April 2022 to September 2023, the Foundation United Women Banja Luka monitored criminal proceedings related to crimes recognised as gender-based violence, in which women and children of both sexes appeared as victims or injured parties.[33] This provided 154 cases for the database and came from twelve

33 The Foundation Udružene Žene from Banja Luka has been conducting court monitoring activities related to gender-based violence since 2011. The materials presented in this study are part of the fifth cycle of monitoring, carried out within the framework of the project "Prevention and Combating Gender-Based Violence in Bosnia and Herzegovina," which the Foundation implements with the financial support of the Kvinna till Kvinna Foundation from Sweden and SIDA.

district and basic courts in Republika Srpska.[34] An additional 110 cases of final judgment came from six district and basic courts in Republika Srpska, as well as the Basic Court in Brčko District.[35] Out of this database of 264 cases that involved gender-based violence crimes, only nine cases were able to be selected based on the criteria of being final judgments that had an element of digital violence. When compared with the fact that violence against women committed in the digital sphere has steeply risen in the last few years in Bosnia and Herzegovina, with 60% of calls received by the telephone helplines being related to such cases,[36] this number indicates a significant lack of recognition and insufficient processing of online technology-facilitated violence within the criminal justice system in Republika Srpska and Brčko District.

Types of court cases that have elements of digital violence

The nine judgments studied in Republika Srpska and Brčko District covered various criminal offences where the factual description of the crime, as set out by the indictment and judgment, included a digital dimension of violence against women and girls such as online acts of violence and those perpetrated through technologies.

The types of crimes before the courts that involve a digital dimension are as follows:

- Four cases of domestic violence[37] (two from the Basic Court in Sokolac, one from the Basic Court in Gradiška, and one from the Basic Court in Brčko District);
- Two cases of endangering safety[38] (one from the Basic Court in Gradiška and one from the Basic Court in Brčko District);
- One case of sexual harassment[39] in conjunction with the criminal offence of unauthorised photographing[40] (from the Basic Court in Gradiška, which involved three perpetrators);
- One case of exploitation of a child or minor for pornographic purposes[41] (from the Basic Court in Brčko District, involving two perpetrators);

34 This included the district courts in Banja Luka, Bijeljina and Doboj, as well as the basic courts in Banja Luka, Bijeljina, Doboj, Kotor Varoš, Mrkonjić Grad, Prijedor, Prnjavor, Teslić, and Višegrad.

35 This included the basic court and district court in Trebinje, the basic court of Brčko District of Bosnia and Herzegovina, the district court in Prijedor, the basic court in Sokolac, and the basic court in Gradiška.

36 GREVIO's baseline evaluation report on Bosnia and Herzegovina, paragraph 117.

37 Criminal Code of Republika Srpska, Article 190 and Criminal Code of Brcko District, Article 208.

38 Criminal Code of Republika Srpska, Article 150 and Criminal Code of Brcko District, Article 180.

39 Criminal Code of Republika Srpska, Article 170.

40 Criminal Code of Republika Srpska, Article 156.

41 Criminal Code of Brcko District, Article 208.

- One case of introducing children to pornography[42] in conjunction with the criminal offence of exploitation of children for pornography[43] (from the Basic Court in Gradiška).

The study found that in the four criminal cases of domestic violence, violence perpetrated through the use of communication technologies and in the online and digital sphere was an integral part of the description of the criminal acts. In two cases, the digital dimension of psychological violence was carried out by sending threatening SMS messages. In one of those cases, the perpetrator sent threats via SMS and the Viber application, while in the other case, the perpetrator used the Messenger application to make threats of death and violence. Out of the four cases of domestic violence, the victims in two cases were the perpetrators' wives; in one case, the victim was the ex-wife of the perpetrator; and in another case, the victim was the perpetrator's mother, although the threats also included other family members. In three cases, the messages sent by the perpetrators were direct threats to the victims' lives, as well as threats to other individuals close to the victim, thus endangering the peace and bodily integrity of family members. These cases highlighted the fact that digital experiences of violence in the context of domestic violence can be an extension of physical, sexual and offline psychological violence. This was seen in one case before the Basic Court in Sokolac, where the domestic violence was committed using technology, and was recognised as an extended criminal act.

Box 1. Case study: The digital dimensions of domestic violence

In one case, the perpetrator threatened the victim via audio calls and messages sent through the Viber application, stating that he would kill her. He wrote, "first pray for yourself, then for others", referring to the minor children who were under the victim's guardianship at the time of the offence. This case highlighted the need for protection orders to be responsive to forms of domestic violence perpetrated online or via communication technology. In that case, the perpetrator had previously been issued an urgent protective measure by the same court, which included a "prohibition of approaching and contacting the victim of domestic violence" for a period of 30 days[44], which he violated by contacting her.

42 Criminal Code of Republika Srpska, Article 177.

43 Criminal Code of Republika Srpska, Article 175.

44 The Law on Protection from Domestic Violence of Republika Srpska, Article 13, paragraph 4, item b.

In another case before the Basic Court in Sokolac, the perpetrator stalked the victim for a period of two weeks, continuously sending her threatening SMS messages. After she blocked the number from which he had sent the messages, he continued sending threats to the phone numbers used by their mutual minor children. In this case as well, the perpetrator had previously been issued an urgent protective measure prohibiting contact and communication with the victim, which he violated.

Similarly, in the two cases of endangering safety, the violence perpetrated using communication technologies was also recognised as an integral part of the description of the actions constituting the crime. Such digital violence was also seen alongside other actions through which the perpetrators committed violence, including stalking, tracking movements, and continuously sending threats to the victims of violence. In one case before the Basic Court in the Brčko District, the perpetrator stalked and tracked his ex-partner's movements for a period of two years, continuously sending death threats through calls. In another case, before the Basic Court in Gradiška, the perpetrator sent SMS messages threatening death to the victim and her close contacts.

In the case of the criminal act of sexual harassment in conjunction with the criminal act of unauthorised photography which was heard before the Basic Court in Gradiška against three perpetrators, in addition to actions of touching the victim in intimate areas (qualified as sexual harassment), the perpetrators took photographs of the victim with their mobile phones, which they exchanged among themselves and sent to others via a group, which was qualified as "unauthorised photography". The case file did not specified whether this was done through a phone application or sent via social media. The description of the criminal act indicates that the victim is a woman with difficulties in intellectual functioning and development.

In the two cases involving exploitation of a child or minor for pornography and introduction of children to pornography, before the Basic Court in Brčko District and the Basic Court in Gradiška, one perpetrator downloaded photographs and videos containing child pornography from the internet and shared them with a larger number of people via social media (Gradiška), while the other two perpetrators contacted multiple underage girls, asking them to send photographs of their intimate body parts, exchanging photographs among themselves through social media, and storing them in their memory on social networks. One of the perpetrators also blackmailed one of the minor victims by publicly releasing photographs (Brčko District). In both cases, the actions constituting the criminal acts

using digital spaces were detailed and indicated a lengthy period of commission over one to two years.

Types of evidence

Due to the fact that summary procedures were often used in these cases, this meant a lack of detailed explanations regarding the consideration of evidence which were often enumerated in a limited fashion. Evidence in the domestic violence cases typically contain police records, witness hearing minutes, extracts from criminal records for the suspects, medical documentation, social history, and risk assessments for the recurrence of violence. In only one case, before the Basic Court in Brčko District, a confirmation of the temporary confiscation of the item (the phone used to make the threats) was included among the evidence. In the cases of endangering safety, besides the minutes of the hearing of the accused and the victim, the judgment of the Basic Court in Gradiška included evidence such as confirmations of voluntary surrender of the items, an order to the telecom provider for a listing of incoming and outgoing calls on the victim's phone, and a CD/DVD with electronic listings of outgoing and incoming calls. In the case of sexual harassment in conjunction with unauthorised photography, the evidence listed in the judgment included screenshots of the photographs taken with the victim, as well as confirmations of the confiscation of items, but does not include other evidence indicating that the photographs of the victim were exchanged with others using digital spaces or other technologies. In the cases involving exploitation of a child or minor for pornography and introduction of children to pornography, the evidence listed in the judgments includes photographic documentation and CDs containing materials seized by court orders, with orders for their destruction.

Procedures used in handling these cases

The study revealed the frequent practice of entering into plea agreements, resulting in a summary procedure without merit or consideration of the evidence and ultimately leading to light sentences for perpetrators. In all of the cases involving domestic violence, expedited proceedings were used, based on a plea agreement and a criminal order. In both case of endangering safety involving digital dimensions, they concluded under expedited proceedings based on plea agreements reached with the respective prosecutor's offices. Similarly, in the case of sexual harassment in conjunction with unauthorised photography, the proceedings were conducted based on a plea agreement. Plea agreements were also done in the two cases involving exploitation of a child or minor for pornography and introduction of children to pornography.

The study found the frequent practice of qualifying domestic violence cases involving a digital dimension in the category that attracts a light sentence. In all cases, domestic violence was qualified under the basic qualification[45], while in two cases before the Basic Court in Sokolac, a more severe, qualified form of the act[46] was recognised in terms of violating urgent protective measures.

In terms of assessing the evidence and victim statements collected during the investigation procedures, the courts' written decisions in the judgments for domestic violence did not indicate a particular focus on the online and technology-facilitated actions and methods used for perpetrating violence. These written judgments appeared to reflect a lack of awareness of how digital violence can overlap with other forms of violence against women and exacerbate the traumatising impact of the gender-based violence.

Outcomes

The study found that the criminal law sanctions pronounced were relatively weak, with most being suspended sentences.

In the cases of domestic violence involving digital dimensions:

- In two cases before the Basic Court in Sokolac, the perpetrators were sentenced to both imprisonment and fines cumulatively for violating urgent protective measures (four-month prison sentence and a 600 KM fine, one-year and two-month prison sentence and a 500 KM fine);[47]
- In two cases before the Basic Court in Brčko District and the Basic Court in Gradiška, only monetary fines were imposed (700 KM, 800 KM).
- In one case before the Basic Court in Sokolac, the court also imposed a security measure of confiscation of the mobile phone and the associated SIM card[48], which were to be destroyed by officials upon the finalisation of the verdict.

45 The Law on Protection from Domestic Violence of Republika Srpska, Article 13, paragraph 1.

46 The Law on Protection from Domestic Violence of Republika Srpska, Article 13, paragraph 5.

47 For violation of protection measures imposed in connection with the criminal offence of domestic violence, the Criminal Code of Republika Srpska provides for the imposition of imprisonment and a fine according to Article 190, paragraph 5.

48 Criminal Code of Republika Srpska, Article 82, paragraph 1.

In the case of endangering safety involving digital dimensions:

- Both cases resulted in fines of 500 KM and 400 KM.

In the case of sexual harassment in conjunction with unauthorised photography:

- The perpetrators received individual fines of 2000 KM (with "unique" fines of 4000 KM each).

In the two cases involving exploitation of a child or minor for pornography and introduction of children to pornography:

- The courts imposed a fine of 4500 KM (Gradiška), and a prison sentence of three months with a suspended prison sentence of eight months, subject to a probationary period of three years, thereby mitigating their penalties below the legal minimum prescribed for these criminal acts. It is important to highlight the position of the Basic Court in Brčko District which rejected the request of the perpetrator sentenced to 3 months of imprisonment to have it replaced with community service, stating that "such a court decision would be a strong incentive for other potential offenders of this act to commit similar offences, as a serious criminal act with severe consequences would receive a mild criminal sanction".

The study revealed that no compensation was awarded for any of these victims. In three cases, the courts specifically referred the victims to civil litigation procedures for compensation, stating that the case file did not provide sufficient evidence for awarding the compensation, and that further discussion of the claim would lead to a prolongation of the criminal proceeding. In the one case of sexual harassment in conjunction with unauthorised photography (Gradiška), the judgment stated that a legal guardian of the victim did not come to the main hearing based on the invitation of the court as a reason for referring the victim to the litigation procedure. In the rest of the four cases analysed, the judgment do not make any specific reference to the issue of compensation.

Findings: Federation of Bosnia and Herzegovina

Percentage of completed VAW cases in court that have elements of digital violence

From January to December 2022, criminal cases for selected acts of gender-based violence were monitored before selected courts in the Federation of Bosnia and Herzegovina.[49] This provided 200 cases for the database and came from fifteen municipal and cantonal courts in the Federation of Bosnia and Herzegovina. Out of this database of 200 cases of gender-based violence, only nine cases were able to be selected to be studied based on the criteria of being final judgments that had an element of digital violence. This indicates that while online technology-facilitated gender-based violence occurs, there are only a small number of proceedings being conducted before the courts in which digital violence is an element.

Types of court cases that have elements of digital violence

The nine judgments studied in the Federation of Bosnia and Herzegovina covered various criminal offences where the factual description of the crime, as set out by the indictment and judgment, included a digital dimension of violence against women and girls such as online acts of violence and those perpetrated through technologies.

The types of crimes before the courts that involve a digital dimension are as follows:

- Seven cases of domestic violence[50] (one judgment from each of the following courts: the Municipal Court of Zenica, the Municipal Court of Bihać, the Municipal Court of Konjic, the Municipal Court of Gračanica, the Municipal Court of Bugojno, one case each, and two judgments from the Municipal Court of Tuzla);
- One case of exploitation of a child or minor for the purpose of pornography[51] (judgment from the Municipal Court in the Federation of Bosnia and Herzegovina);
- One case of murder[52] (judgment from the Sarajevo Cantonal Court).

49 This included the cantonal courts of Bihać, Novi Travnik, Sarajevo, Tuzla and Zenica and the municipal courts of Bihać, Bugojno, Gračanica, Jajce, Konjic, Tešanj, Tuzla, Zavidovići, Zenica and Sarajevo.

50 Criminal Code of the Federation of Bosnia and Herzegovina, Article 222.

51 Criminal Code of the Federation of Bosnia and Herzegovina, Article 211.

52 Criminal Code of the Federation of Bosnia and Herzegovina, Article 166.

Of the seven domestic violence cases involving digital violence, victims or injured parties were: perpetrators' ex-wives in three cases; perpetrators' current wife in three cases; and perpetrator's mother in one case.

Box 2. Case Study: The digital dimension of domestic violence

A case involving the criminal offence of domestic violence was brought before the Zenica Municipal Court against the accused alleging that, in a state of mental incapacity due to mental illness, paranoid schizophrenia, he committed violence against the injured party, his ex-wife, with whom he no longer lives with in the same household. This case showcases how forms of psychological violence in the context of domestic violence can take radical forms when coupled with new technologies. Specifically it shows the use of modern information and communication technologies in the commission of the offence.

The accused repeatedly called the victim via mobile phone and demanded that she come to his apartment and then sent a message threatening to beat her if she did not come.

> Do you believe me that I will kill you to death these days, do you believe me?
>
> I swear by God I will make a huge problem and go to prison, I promise you that.
>
> If you don't want to give it to me (*referring to sexual intercourse*) you will be in bruises.
>
> I will drink your blood.

The Zenica Municipal Court found that in a state of mental incapacity he threatened the peace, physical integrity and mental health of a member of his family with whom he does not live in the same household.

When the victim attended at his apartment, he grabbed her hand with his hand and pulled her into the apartment, and then hit several times with his hands, as a result of which she suffered physical injuries.

This study raises the concern that the perpetrator, although it was established that he committed the crime in a state of mental incapacity, was not referred for psychiatric treatment. Based on the evaluation of the evidence presented during the procedure, the medical documentation of the accused and the findings of the expert neuropsychiatrist, the court

determined that there was no need to impose a measure of compulsory psychiatric treatment on the perpetrator because he regularly receives therapy. This judgment appears to reflect a lack of awareness of how digital violence can overlap with other forms of violence against women and exacerbate the traumatising impact of the gender-based violence.

Box 3. Case Study: Using online and technology-facilitated activities in the commission of sexual exploitation of a child or minor

The proceeding held before the Tešanj Municipal Court alleged that the accused, at a specific time and place, in the immediate vicinity of the disco-club using his white Samsung Grand Neo Plus mobile phone with SIM card user number XXX recorded the minor who was half-naked, and made audio-visual material of pornographic content and sent the video to a third party. Such pornographic material was available to a large number of people and was on the Internet, therefore, it was alleged he recorded a minor for the purpose of creating audio-visual material of pornographic content, and possessed such material, with which he committed the criminal offence of exploitation of a child or minor for the purpose of pornography. The victim did not know the perpetrator.

Box 4. Case study: The digital dimensions of the offence of murder

A murder case was processed before the Sarajevo Cantonal Court. In December of 2020, the perpetrator entered the offices of the victim with the intent of killing her, and shot her four times, from which the victim died several days later. This incident had been preceded by threats made, on several occasions, by the perpetrator toward the victim in person and by phone stating: "I will set fire to your car, I will go and take a gun from my father and I'll kill you, if you reconcile with your ex-husband I'll kill you, etc." The threats were made because in the previous period the victim refused to be in a romantic relationship with the perpetrator and it was alleged that the victim had borrowed money from the perpetrator. The perpetrator worked for a time as a member of the security agency that secured the building of the company where the victim was employed and killed.

Types of evidence

The study found that in only one of the seven domestic violence cases was an expert examination of mobile telephones and SIM cards performed. That expert opinion was used to prove the sending of messages with threatening content to the injured party. In the other six cases, expert examination was not conducted. The evidence that was produced and which provided support for the convictions of the accused in those cases were as follows: records of the hearing of the accused, records of the hearing of the injured parties, records of the hearing of witnesses, extracts from criminal records, records of the deprivation of freedom of the accused, records of the release of a person deprived of freedom, medical findings of the injured party, and in one case, the order of the prosecution for a medical examination of the accused and the findings and opinion of a medical expert on the circumstances of the accused's mental (in)capacity. In only one case, a copy of a text message sent by the accused to the victim was presented as evidence.

In the case of exploitation of a child or minor for the purpose of pornography, numerous types of material evidence were presented that support the allegations of the indictment, as well as evidence on the circumstances of the official actions taken by the authorised officials who made them. Among the evidence presented in this case is the expert opinion of the mobile phone with the SIM card of the user number XXX, based on which data was received and sent content was obtained. This evidence, when brought into connection with the material evidence conducted during the procedure and with the statements of the witnesses heard during the investigation, as well as with the confession of the accused, indicated that the accused committed the criminal offence charged in the indictment. In the case of murder, numerous types of material evidence were presented that supported the allegations of the indictment, as well as evidence of the circumstances of the official actions taken by the authorised officials who made them. Among the evidence presented in this case were the official notes of the competent Ministry of Internal Affairs, from which it can be seen that the accused on several occasions sent threats to the victim directly and by telephone.

Procedures used in handling these cases

In the seven domestic violence cases, the accused plead guilty, which was considered as a mitigating circumstance when deciding on the criminal legal sanction. Similarly, In the case of exploitation of a child or minor for the purpose of pornography, and in the case of murder, the accused entered into plea agreements.

Outcomes

In six out of the seven domestic violence cases, the perpetrators were given suspended sentences, with set prison sentences ranging from three to six months with a probationary period ranging from one to two years. In two of those cases, criminal orders were issued and the perpetrators were sentenced to a suspended prison sentence of three months, which will not be carried out on the condition that the perpetrator does not commit new crime. In one case, it was established that the accused had committed the crime of domestic violence in a mental incapacity of a perpetrator.

In none of the seven domestic violence judgments were the victims awarded compensation. They were referred to initiate their own civil litigation. The reason for referring them to litigation was that not enough facts and evidence had been presented to the court for the court to decide on the compensation claim within the criminal proceedings. Furthermore, it was observed that in none of these cases was an expert opinion requested by the authorities regarding the circumstances of the traumas the victims suffered as a result of the threats they were exposed to by the accused.

In the case of exploitation of a child or minor for the purpose of pornography, the perpetrator was sentenced to a suspended sentence and conditionally sentenced to imprisonment for a period of one year, in which the sentence will not be carried out on the condition that the perpetrator does not commit a new criminal offence within two and a half years from the date of entry into force of this judgment. The victim was referred to civil litigation if they wanted to pursue a compensation claim. In this case, during the investigation, the victim's request for compensation for material and non-material damages was made, but without indicating the amount of damages claimed, so the court referred them to litigation.

In the case of murder, the fact that the perpetrator previously threatened the victim with death, that is, that he addressed her with the words that he was going to kill her, was considered an aggravating circumstance in this case. He was sentenced to prison for eleven years. In the criminal case, the injured parties, the daughters of the victim, submitted a written proposal for compensation requesting material damages in the name of funeral expenses and non-material damages, in the name of mental pain due to the death of a close person. In the written proposal, they proposed that the prosecution issue an order for

a neuropsychiatric expert opinion on the circumstances of the mental pain suffered as it is necessary in order for the court to have sufficient information and evidence in the file at the stage of the criminal proceedings to be able to order a compensation award at the criminal trial. They also argued that having an expert opinion would thereby avoid additional costs for the injured parties that would inevitably arise if the court refused to decide on the compensation claim due to the lack of evidence in the criminal proceeding. However, during the investigation, a medical expert report was not done. The court referred the injured parties to civil litigation to make their compensation claim.

III. Main findings from key informant interviews: Judges and prosecutors

Findings: Republika Srpska and Brčko District

Frequency and nature of cases of VAW in its digital dimension

The majority of interviewees were of the view that the number of cases of online technology-facilitated violence in Republika Srpska and Brčko District, including gender-based violence, was not high, with an estimate of up to twelve criminal cases per court in the last five years. Furthermore, the interviewees from the District Prosecutor's Office of Brčko District noted that out of 20 indictments for domestic violence over a period of two years, only two included violence in its digital dimension. Their perception of the relatively low frequency of these kinds of cases in the criminal justice system is similar to the findings from the available statistics and case law analysis. However, interviewees were of the view that there is the potential for an increase in these cases due to the growing availability of technology.

Interviewees from the judiciary identified the most common forms of online technology-facilitated violence seen in their courts. These were: sexual harassment through the use of computer networks; abuse of photographs and video content; exploitation of children in pornography; violations of children's privacy, and public incitement to violence and hatred through digital media. Additionally, interviewees from the District Public Prosecutor's Office in Bijeljina noted that the most common forms of gender-based violence against women in its digital dimension occurred in cases of stalking and domestic violence, where violence is perpetrated through social networks or applications. These cases most often involve former or current partners and resulted in convictions, although mostly resulted in conditional sentences. In some cases, the violence was repeated, leading to submissions for the revocation of the conditional sentences.

Prosecution of cases of violence against women with elements of online technology-facilitated violence

Many interviewees from the judiciary noted that over the past three years cases of gender-based violence against women which had a digital dimension most often ended in plea agreements, and therefore were concluded without a full hearing.

It was suggested that such cases may not be fully processed in court and can indicate challenges in their prosecution. The observations by the interviewees are supported by the case law analysis, which showed that all nine cases from Republika Srpska and Brčko District were concluded in expedited proceedings.

Assessment of digital evidence and challenges in evidentiary procedures

Online and technology-facilitated threats and intimidation are considered relevant evidence in cases of violence against women; nevertheless, their legality must be clearly established in accordance with the Republika Srpska Criminal Procedure Code. This means that the search for and seizure of all electronic evidence must be authorized by law. However, there are significant challenges in obtaining and assessing this evidence. As one interviewee noted:

> The challenges in accepting such evidence often relate to the legality of the evidence—whether the evidence was obtained in a manner prescribed by law. In addition to the prosecutor, who manages, conducts, and supervises the investigation, a significant role in handling digital evidence is played by so-called experts. According to the provisions of the applicable criminal procedure law, the evidence-gathering act of searching computer systems, storage devices for computer and electronic data, mobile phones, and other similar devices can only be conducted with the assistance of these experts.

Other interviewees also raised the legality of obtaining digital evidence as a key challenge, as it requires the involvement of experts in reviewing computer systems and devices. They noted there is a lack of procedural legal regulation for dealing with digital evidence, that is, the practice of recovery, seizure and investigation of material found across digital and electronic devices which store and capture data. Some of the interviewees recommended a more precise terminology to better define technological procedures within the legal framework. As one interviewee noted:

> It certainly poses a challenge to prove technology-facilitated violence because, for the prosecutor, linking an online space, which is often imaginary for most, to the real world and making it linguistically and legally understandable is difficult. However, for any prosecutor, achieving the goal of reaching the end user and proving that the suspect committed violence via the internet is a significant success.

One of the biggest challenges mentioned by the interviewees was proving the connection between a specific social media profile and the accused, as well as locating the accused via their Internet Protocol (IP) address. Limitations in the legal regulation of internet space further complicates the process, especially since many users utilise "floating" IP addresses that hinder the identification of end users. Technological advancements have allowed users to create false identities and profiles, which further complicates the collection of relevant evidence. In practice, forensic methods are crucial for gathering digital evidence, but the challenge lies in the use of these tools and their availability. One of the challenges for prosecutors cited in the interviews is the easily accessible and uncontrolled purchase of mobile network numbers without the identification of the individual purchasing them, which are used to facilitate the commission of criminal acts via digital technologies. As one interviewee noted:

> Every IP address assigned to the end user should be non-transferable and clearly indicated with the name and surname, as well as the location or geographical area. I also believe that all mobile phone numbers with SIM cards that can be freely purchased at kiosks or stores should only be available with an identified personal ID. This was one of the initiatives and is being implemented in various countries.

Legislative Framework

In response to the question of whether there was a need for a specific legal article criminalising digital violence, most of the interviewees believed that the existing legislative frameworks in Republika Srpska and Brčko District allowed for the criminalisation of online technology-facilitated violence. Particularly, the interviewees from Republika Srpska noted the following criminal offences as being relevant for prosecuting violence against women in its digital dimension: sexual harassment; abuse of photographs and videos of sexual explicit content; exploiting children for pornographic performances; introducing children to pornography; exploiting computer networks or communication by other technical means to commit crimes of sexual abuse or exploitation of children; violating the privacy of a child; defamation; disclosure of personal and family circumstances; public incitement and promotion of violence and hatred. However, the interviewees believed there was need for a more consistent application of the existing legal framework and that better legal regulation was necessary in a procedural sense, with a special focus on aligning the term "digital evidence" in a normative context.

They also note that within the criminal legislation of Republika Srpska and Brčko District, the use of information and communication technologies often constituted an aggravated form of a criminal offence, which entails stricter penalties. Online technology-facilitated violence is classified as a more serious form of criminal acts, such as stalking or sexual harassment. For instance, sexual harassment conducted via computer networks is punished more severely than in other circumstances[53], as is the case for the abuse of photographs and videos containing explicit content[54].

Legal changes needed to improve victim protection and prosecution of digital violence

In response to the question about what legislative changes would be needed to better protect victims of digital violence, a number of interviewees believed that more precise regulation of digital violence would not necessarily significantly enhance victim protection. Rather what is needed is a more consistent uniform application of the law, one that considers the severity of circumstances (such as hate crimes, repeat offenders) would encourage victims to report such cases and improve enforcement.

A number of interviewees noted that the term "digital evidence" is not defined within the current procedural legal framework, and therefore it would be appropriate to ensure that the legal terminology used in procedural law encompasses technologically precise terms that would describe procedures related to digital evidence. A number of interviewees noted a positive development in the Criminal Code of Republika Srpska[55] wherein movable property was defined as any produced or collected energy for providing light, heat, or movement, telephone impulses, as well as recorded data resulting from electronic data processing (computer data or programs). However, it was further noted that what constitutes digital evidence is not further defined, nor are there specific legal criteria prescribed for the admissibility of digital evidence. It was suggested that this should be addressed in the future to regulate clear procedures for the admissibility of such evidence. As one interviewee noted:

> I believe that introducing a specific legal provision that would criminalise technology-facilitated violence is unnecessary because everything that happens on the Internet is already covered by the existing legislative

53 Criminal Code of Republika Srpska, Article 170, paragraph 3.

54 Criminal Code of Republika Srpska, Article 170a.

55 Criminal Code of Republika Srpska, Article 123, paragraph 1, item 18.

framework. When it comes to defining information and communication technologies as means, methods, and procedures for committing criminal offences, including violence against women, I think that additional training, especially for judges, would help in understanding the Internet as a space where any criminal act can be committed in countless different ways. With the development of modern technologies, these possibilities are increasing and can even be more alarming, especially when we consider the advancement of artificial intelligence, its application, and the domain it currently occupies, which is still in its infancy.

Findings: Federation of Bosnia and Herzegovina

Frequency and nature of cases of VAW in its digital dimension

All of the interviewees were of the view that, given the existing legal framework in the Federation of Bosnia and Herzegovina, they did not often encounter cases with elements of digital dimension of violence against women. They noted that the number of online technology-facilitated violence against women cases was extremely small when compared to the total number of cases conducted before the courts. However, a number of interviewees believed that taking into account the rapid development of digital technologies, it is quite realistic to expect that the number of court proceedings in this regard will increase significantly in the future.

As one interviewee noted, when discussing the nature of these cases,

> One of the more significant indictments that resulted in a final conviction is the indictment filed against Jurica Pavlović from Ljubuški, for the criminal offence of inciting ethnic, racial and religious hatred, discord or intolerance, committed to the detriment of Martina Mlinarević, columnist and Ambassador of Bosnia and Herzegovina to the Czech Republic. What is significant is the fact that it was the first indictment in the West Herzegovina County for the aforementioned criminal offence.

That case involved Martina Mlinarević, is a columnist from Bosnia and Herzegovina, a poet and a socially engaged activist, who wrote about various social taboos and harshly criticised political elites. After Martina Mlinarević announced on her Facebook profile that she was forbidden to present the book "Huzur" in Čitluk at a Festival, in which she described her fight against a serious disease, breast cancer, she received a series of serious and violent threats and insults on social networks from a part of the public who did not approve of her views.

Assessment of digital evidence and challenges in evidentiary procedures

A number of interviewees expressed the view that considering the existing criminal legislation in the Federation of Bosnia and Herzegovina, it is very difficult to prove the existence of online technology-facilitated violence against women. The biggest challenge noted in proving digital violence, or violence committed using information and communication technologies, was in identifying the perpetrators of these criminal acts. Perpetrators are most often identified through social networks, IP addresses and mobile phone base stations, and rarely through witnesses, so these indictments are mostly based on material evidence.

As one interviewee noted:

> A separate problem is the lengthy process of obtaining data from service providers, such as Meta. After issuing an order for expert examination and seizing evidence, and unless the defence objects to the legality, in the procedures conducted so far after obtaining a decision to seize the phone and conduct expert examination in order to ensure that the evidence was obtained legally, phones, listings, SMS, Viber, Messenger correspondence, video clips were used, and each piece of evidence is individually presented.

Legislative Framework

A number of interviewees believed that it is urgently necessary to specifically define cases of stalking and harassment on the Internet, sexual and explicit messages, threats of sexual violence, publishing pornographic content without the victim's consent, and hate speech on the Internet, as has been done since 2014 in some European countries such as Germany and France. It was their view that this was needed because victims of online technology-facilitated violence are not protected and suffer from behaviour by perpetrators that are not currently classified as criminal offences. A number of interviewees also noted that in addition to these amendments to the criminal legislation it is necessary to accompany this with education, especially for forensic departments, in order to make investigations efficient and effective.

As one interviewee stated:

> For example, in the Federation of Bosnia and Herzegovina you do not have criminal protection against persecution, stalking, harassment, while in the Republic of Srpska, the Republic of Serbia, the Republic of Croatia, the

Republic of Slovenia, Montenegro you have criminal protection. In FBiH, you must be in a close relationship with the perpetrator in order to be protected from persecution and harassment, for the criminal offence of endangering security to exist. Therefore, if you are not in a close relationship, nor were you in such a relationship with the perpetrator, you do not have criminal protection. In FBiH, you are not even protected from publishing your intimate photos on social networks. For example, in the FBiH, you do not have criminal protection if you send someone your intimate photo and later that photo is published on a social network without your permission. In the Republic of Croatia, there is a criminal offence of misuse of a sexually explicit recording, which protects you from a sexually explicit recording recorded with your consent for personal use being made available to a third party. In Bosnia and Herzegovina, you are not protected from false representation, that is, identity theft, because false representation implies representing yourself as an official or military person. In Bosnia and Herzegovina, you are not protected from unauthorised access to the computer system or computer data. For example, in Bosnia and Herzegovina you are not protected if someone has hacked your Instagram profile, if they have taken control of your Instagram profile. In the Republic of Croatia, there is a criminal offence of unauthorised access, which protects you from unauthorised access to the computer system and computer data. In the Federation of BiH, there is a criminal offence of computer fraud, which, in addition to unauthorised access, requires that the unauthorised access was made with the aim of obtaining illegal property benefits, if it was not done with that aim, then the behaviour of the perpetrator cannot be brought under the criminal offence of computer fraud or any other criminal offence.

IV. Main findings from the questionnaire: Ministries of Internal Affairs

Findings: Federation of Bosnia and Herzegovina

Recording reports of online technology-facilitated violence against women

In response to the question regarding data on the prevalence, issues and difficulties in recording and processing acts of violence against women in which the digital dimension of violence is also present, all of the questionnaire respondents stated that police officers of the Criminal Police Sector of the Ministries of Internal Affairs handle all reports of violence against women and that a single record is kept for all reports. There is no separate record of reports of violence against women committed using information and communication technologies.

As one questionnaire noted:

> Police officers of the Federal Police Administration, Department for Combating Computer Crime, encounter reports of criminal offences committed using information and communication technologies (as a means of commission) on a daily basis, which are often directed at women as potential victims. The Federal Police Administration does not keep separate records of reports in relation to the parameters of the victim (gender, age, belonging to a certain group, etc.), nor in relation to the means of commission of criminal offences, and in this regard, they are unable to provide data on the number of reports for the specified time period.

Introduction of a special article of the law that would criminalise online technology-facilitated violence against women

A number of questionnaire respondents believed that specifically criminalising digital violence in the Criminal Code would significantly facilitate the actions of police officers in receiving reports and investigating these cases. Such legislation would provide a clear legal framework for recognising, reporting and processing cases of violence against women committed online or through the digital sphere

or through digital means. Furthermore, respondents noted that such a law would encourage awareness-raising of the seriousness of online technology-facilitated violence and its consequences. Other respondents also were of the view that it was crucial to adopt a clear definition of online technology-facilitated violence and its various manifestations, to achieve more efficiency in the reporting, investigation and prosecution of these cases. Moreover, they noted that a key step would be to introduce specific penalties for perpetrators of online technology-facilitated violence and better protection measures to ensure the privacy and safety of victims.

Findings: Republika Srpska

Recording reports of online technology-facilitated violence against women

In response to the question regarding data on prevalence, the questionnaire respondents indicated that data from the Ministry of Internal Affairs of Republika Srpska showed a significant increase in recent years in the number of reports of violence against women in which information and communication technologies were used, such as SMS messages, phone calls, and social networks and applications like Facebook, Instagram, Messenger, WhatsApp, and TikTok. It was noted that police officers are increasingly encountering such reports, and the rapid pace of technological development requires constant improvement of their knowledge and skills. A number of questionnaire respondents were of the view that although the police are equipped and trained to handle these challenges, continuous training and a comprehensive approach are necessary to ensure effectiveness in identifying and documenting such cases.

The questionnaires revealed data from 2021 to 2024 that recorded the total number of reports of violence against women involving information and communication technologies, including SMS messages, phone calls, and various social media platforms and messaging apps. The number of reports per year is as follows:

- 2021: 71 reports
- 2022: 76 reports
- 2023: 105 reports
- 2024: 83 reports in the first 10 months

Challenges in recording and investigating reports of online technology-facilitated violence against women

According to the questionnaire respondents, the main challenges in receiving reports and investigating cases of violence against women involving a digital dimension included the rapid technological advancements and changes in security and privacy policies of social platforms, which complicated the gathering and verification of evidence. Another further complication for investigations mentioned in the questionnaire responses was the challenge in identifying perpetrators, who often use fake or anonymous accounts.

Cooperation with internet providers and platforms was also mentioned as being crucial, as information is often only available with their assistance. Additionally, protecting the privacy of victims and witnesses needs to be a priority while ensuring all necessary data for investigations. Victims often feel fear or shame due to digital violence, highlighting the need for legal and psychological support to empower them to report the violence and participate in proceedings. Public education on recognising digital violence and available protection mechanisms is key, both for potential victims and for society as a whole, to create an environment that does not tolerate violence and is familiar with reporting methods.

V. Main findings from the in-depth victim interviews: Women survivors

Findings: Republika Srpska

Of the ten women interviewed from this entity, they had all experienced forms of violence with a digital dimension and all had been users of specialised support services for women victims of violence, such as counselling centres and safe houses.

Experiences with digital violence against women

All interviewees shared their experiences of violence that began in the offline world and then continued online. They were all victims / survivors of intimate partner violence, and described how online and technological tools served as a means for the manifestation, extension, and escalation of domestic violence. This indicates that digital violence is often not an isolated phenomenon, but rather a continuum of different forms of violence against women that can first manifest offline and be amplified and facilitated by technology. The interviewees noted how online and technology-facilitated violence overlapped with violence in their lives, primarily experiencing threats, blackmail, and intimidation through messages and social media.

Common forms of online technology-facilitated violence against women

The most common forms of online technology-facilitated violence experienced by the interviewees were reported to be: threats via messages (for example, SMS, Viber, and Messenger); the publication of private information and communications on social media; and online psychological intimidation. In some cases, threats were directed not only at the interviewee but also at her loved ones, for example children or family members, increasing the traumatic impact of the violence. The most frequent form of violence mentioned by the interviewees was the digital dimension of psychological violence, namely verbal and psychological violence through digital communication channels, with messages containing threats and intimidation. They all expressed how violence committed in this way caused ongoing fear

for their safety, anxiety, and a sense of constant availability and exposure to the perpetrator.

Experiences in reporting and receiving support and protection from institutions

The study found that the willingness to report and experiences in reporting generally depended on the relationship between the victim and the perpetrator. A number of interviewees described reporting the violence only after the most serious and repetitive threats to life, murder, or suicide, while generally not reporting what they viewed as "milder forms" of online technology-facilitated violence. They noted the primary reason for not reporting was due to the fear of escalation of violence and retaliation from the perpetrator.

Although most interviewees expressed satisfaction with the institutional response, they did point to numerous obstacles to accessing justice. Some of the challenges they listed related to the use of digital evidence to prosecute the criminal act, such as concerns regarding the legality of its acquisition and the disregard of victims' statements in court when they testify about threats and blackmail received via phone or social media. As one interviewee stated:

> The threatening and offensive messages started when he went to Germany. During his travels, he used multiple phone numbers from different countries, and the messages via Viber and WhatsApp were daily, sometimes 20 or 30 per day. The messages always started with a gentle question, but then he would continue with insults and threats. He kept the sexually explicit messages which I sent him while he was traveling, along with photographs, and then blackmailed me, saying he would post them online and send them to my colleagues. Following the police's advice, I submitted printed copies of the messages, but these were not considered as evidence in court because they were not obtained in a lawful manner. No one from the police asked me to hand over my phone, where the messages were stored. My testimony about the threats made through Viber and WhatsApp was not considered in court, and he was acquitted.

Violence against women committed in the digital sphere can serve as a basis for imposing urgent protective measures according to the Law on Protection from Domestic Violence in Republika Srpska. These are protective measures as opposed to being criminal sanctions. However, a number of interviewees indicated that the threats did not stop after reporting to the police, and the sense of fear for their

safety persisted even after protective measures were issued. This raises the concern of effectiveness in enforcement of protection measures. Although institutions often did take certain protective measures, the victims continued to live in fear of potential violence and did not feel protected, especially from prolonged forms of digital violence that involve intimidation and threats through information technologies.

Findings: Federation of Bosnia and Herzegovina

Experiences with digital violence against women

All of the five women interviewed from this entity stated that the violence first started in the offline world and then continued online. They all experienced violence in intimate partner relationships. The interviews indicate that online technology-facilitated violence against women is often part of a continuum of violent behaviour that can first manifest offline and then be amplified and facilitated using internet and technological tools. As one interviewee stated:

> He sent me messages that if I leave him I will be like that woman from Gradačac. That's what he wrote to me. It started first in real life. We lived in a marriage, arguments and disagreements began. When I wanted to leave him he started threatening me. I left and then he wrote me a message saying 'if you take my child out and leave, you will be like that woman in Gradačac. You know what happened to her, it will happen to you too, and feel free to take these messages to the police'.

Box 5. The wider impacts of online technology-facilitated violence against women – the Gradačac case

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

long uptime of the video revealed substantial weaknesses in Instagram's mechanisms of reporting and removing harmful content, including filters designed to automatically flag and remove violent content. The source reports that the BiH cybercrime department of the Federal Police requested removal of the video to Instagram's parent company immediately upon receiving reports of the video, but the company took two hours to remove the video".[56]

Common forms of online technology-facilitated violence against women

The most common forms of online technology-facilitated violence noted by the interviewees included threats via SMS, Viber, Messenger, and psychological intimidation. As described by one interviewee:

> I suffered psychological violence every day, culminating in physical violence. The final straw was when he called our minor daughter on Viber and threatened to kill her and her sister, and that they would find me dead in a container.

Experiences in reporting and receiving support and protection from institutions

All of the interviewees stated that they did not report the perpetrator immediately. They noted that the violence occurred several times before they decided to make a report. Reasons for not reporting was fear for their lives, that the perpetrator would threaten them if they reported him, and that he would do something worse.

The majority of interviewees noted that they were satisfied with the reaction of the institutions they contacted. As one interviewee stated:

> They provided protection, they immediately took measures to prevent him from coming near me. When he started threatening me again on the phone, they issued him with the stalking and harassment order [so] that he was not allowed to contact me even on the phone. But that fear of him is still present.

56 UN Women. 2024. "The Dark Side of Digitalisation: Technology-facilitated violence against women in Eastern Europe and Central Asia".

However, there were also some interviewees who expressed dissatisfied with the reaction of the institutions, mainly raising their concern that the institutions did not take the threats via information and communication technologies seriously. As noted by one interviewee:

> They stated that they would talk to him and warn him, and that I should have had more evidence about the cyberattack. I only had word of mouth, because everything I talked to anyone at home, he knew everything. As for the threats, they did not consider it a real, big threat to life. They didn't consider it worrisome because it seems to happen to everyone, a lot of women report it that way.

VI. Conclusions and recommendations

Conclusions

A review of more than 250 final judgments involving violence against women, including domestic violence, processed before basic/municipal and district/cantonal courts in Bosnia and Herzegovina revealed only a small number of cases of online technology-facilitated violence against women. Just 18 final judgments involved digital violence. When compared with the fact that violence against women committed in the digital sphere has steeply risen in the last few years in Bosnia and Herzegovina, with 60% of calls received by the telephone helplines being related to such cases,[57] this number indicates a significant lack of recognition and prosecution in the judicial system.

The case law analysis also found that evidence such as data from mobile phones or SIM cards, applications, are often not considered, which makes it difficult to effectively prove the criminal offences.

Furthermore, the case law analysis found that in the two entities and administrative unit of Bosnia and Herzegovina, most cases were completed in a shortened procedure through a plea agreement, which resulted in relatively mild sentences, most involving suspended sentences. Moreover, the use of plea agreements meant the reduced need to conduct a thorough examination of the evidence. In none of the cases analysed was the victim awarded a compensation claim within the criminal proceedings, rather the criminal court often suggested that the victim could initiate civil proceedings. This further exposes the victims to additional traumatisation and costs, if they decide to go the civil law route. The case law analysis raised the concern of whether the current criminal justice system is achieving the purpose of general and special prevention and effective protection of victims of digital violence.

57 GREVIO's baseline evaluation report on Bosnia and Herzegovina, paragraph 117.

The study also found that no professional assessments have been conducted to determine the psychological impact of the digital dimension of violence on women on the victims. This left the victims who have experienced trauma and fear without an adequate response. In order to reduce secondary victimisation and ensure adequate compensation for victims, it is necessary to include expert reports during the investigation. In part, this would provide a stronger basis for compensation claims for damages and contribute to the alleviation of the financial and emotional burden on victims, such as from having to initiate separate civil litigation.

The study found certain gaps in the criminal legal frameworks in the two entities and Brčko District of Bosnia and Herzegovina. Since general forms of criminal offences can be used to cover digital dimensions of violence against women, as seen in the case studies of domestic violence and murder, it is important to note that not all forms of violence against women (for example rape, stalking, forced marriage, genital mutilation, unauthorised publication and abuse of sexually explicit content) are uniformly criminalised in Bosnia and Herzegovina. Unlike Brčko District and Republika Srpska, which enacted recent amendments to the substantive criminal legislation criminalising forced marriages, genital mutilation, stalking and abuse of photographs and videos with sexually explicit content, the Criminal Code of the Federation of Bosnia and Herzegovina does not contain similar provisions. However, on a positive note, it was announced by the authorities that there are plans to more closely align the Federation of Bosnia and Herzegovina Criminal Code with the Istanbul Convention and that a working group has been established in the Federation of Bosnia and Herzegovina Parliament to this end.[58]

Furthermore, the study found that while the criminal laws did not contain specific criminal offences to comprehensively cover online technology-facilitated violence against women, the Criminal Codes in the two entities did include a number of offences that focused on digital violence. For instance, the Criminal Code of the Federation of Bosnia and Herzegovina included the criminal offences of "unauthorised optical recording" and "unauthorised tapping and sound recording". The Criminal Code of Republika Srpska included the criminal offences of "unauthorised publication and display of another person's writing, portrait, or recording" and "abuse of sexually explicit photographs and videos". In Republika Srpska, amendments were also made to the provisions regulating the criminal offence of "sexual harassment" recognising an aggravated form when it is "committed using a computer network or another form of communication". It should be noted that the above provisions are gender-neutral and do not acknowledge the structural nature of violence against women and girls.

58 GREVIO's baseline evaluation report on Bosnia and Herzegovina, paragraph 200.

The study also found deficiencies in the procedural laws which make it challenging to effectively investigate and prosecute criminal acts of violence against women with a digital dimension. Interviews with judges and prosecutors revealed challenges in the collection, storage and evaluation of digital evidence. Moreover, the lack of technical equipment, poor knowledge of digital evidence methods, and technological barriers often hindered the efficient processing of these cases. Those interviewed also emphasised problems relating to the legality of the evidence, that is whether the evidence was obtained in the manner prescribed by law. Also discussed was the lack of high-tech experts who are needed because the search of computer systems, devices for storing computer and electronic data, mobile phones and other similar devices, according to the provisions of the applicable criminal procedure law, must be undertaken by a person competent to seize electronic evidence. Furthermore, the interviews and questionnaires noted challenges due to the fact that the term "digital evidence" was not defined by the procedural legal framework in force in Bosnia and Herzegovina. A number of those interviewed believed it would be expedient to reform the procedural law to ensure it describes procedures in relation to digital data. Defining "digital evidence" and regulating a clear procedure for the acceptance of such evidence is believed to contribute to legal and proper judgments.

The study found that most victims interviewed only reported violence against women with a digital dimension when such violence was of a serious nature, such as continuous death threats, blackmail and threats to third parties close to the victims. The majority of victims expressed a certain degree of satisfaction with the institutional responses to their reports, in the sense that the system reacted and recognised these forms of violence as criminal offences. However, it was also noted that during the investigation and prosecution they encounter numerous obstacles as they believed that they had been unclearly or incorrectly advised with respect to the submission of digital evidence, often key to the process.

Official statistics from the relevant Ministries of Internal Affairs on the number of reports of criminal acts of violence against women and domestic violence that have elements of digital violence are not publicly available, nor do they appear to be uniform at the national level. However, the study was able to obtain from the Ministry of Internal Affairs of Republika Srpska data on the number of violence against women cases from 2021 to 2024 that involved the use of information and communication technologies, including text messages, phone calls and various social networks and applications for messaging (Facebook, Instagram, Messenger, WhatsApp, TikTok). It should be noted that the ministries at the cantonal level were not able to provide similar data.

Key recommendations

Harmonisation of legislation with the Istanbul Convention:

- It is necessary to further align the legal framework in Bosnia and Herzegovina with the requirements of international standards, particularly the Istanbul Convention and the Budapest Convention, in order to provide effective protection from and prosecution for all forms of violence against women and domestic violence, including in the digital dimension. It is proposed that the Federation of Bosnia and Herzegovina consider following the example of law reforms that have taken place in Republika Srpska and Brčko District.

Introduce or modify risk assessments to include digital dimension

- In order to ensure that protection measures are responsive to forms of domestic violence perpetrated online or via information communication technologies and to other digital manifestations of violence against women, all entities need to ensure that risk assessments include an understanding of the harm caused by the digital sphere and how the dynamics of digital violence contribute to risk. Furthermore, it is proposed that the Federation of Bosnia and Herzegovina follow the recent reform in Republika Srpska in introducing a mandatory obligation of police officers to carry out a risk assessment in certain cases.

Reform procedural rules and procedures

- In order to ensure that perpetrators of digital violence against women are held accountability, all entities of Bosnia and Herzegovina should consider defining precise procedures for the recovery, seizure and investigation of material found across digital and electronic devices which store and capture data. A clear definition of the term "digital evidence" and the establishment of a prescribed procedure for its acceptance would assist prosecutors and judges in handling these cases.

Increase the capacity of judges and prosecutors in handling cases of violence against women with a digital dimension

– In order to ensure effective prosecution and punishment for online technology-facilitated violence against women, it is proposed that there be an increase in capacity-building efforts for judges and prosecutors. Namely, the High Judicial and Prosecutorial Council and Centres for the Education of Judges and Prosecutors should consider providing mandatory and continuous capacity building, education, and training for judges and prosecutors, to familiarise them with the digital forms of violence against women, to increase their capacity to respond to women and girls as victims without causing secondary victimisation and re-traumatisation, and, where relevant, to familiarise them with the existing legal frameworks and international co-operation mechanisms relating to the digital dimension of violence against women, as well as the gathering and securing of electronic evidence.

Improve the professional capacities of professionals involved in the investigation and prosecution of criminal acts of online technology-facilitated violence against women

– In order to improve cooperation and coordination among criminal justice and law enforcement professionals with experts in cybercrime services, Bosnia and Herzegovina should consider strengthening the capacity for staff in the criminal justice system and law enforcement agencies so they have the necessary knowledge and resources to apply the existing legal framework to the digital dimension of violence against women and to develop their forensic capabilities for collecting and securing electronic evidence without secondary victimisation and re-traumatisation of the victim.

Prevention and early recognition of online technology-facilitated violence against women

– Gender mechanisms, non-governmental organisations, and ministries responsible for law enforcement should work together to implement comprehensive preventive campaigns and education on the various dimensions and manifestations of digital violence against women, including early recognition and reporting of different forms of violence in the online space. Campaigns should also provide information about available protection mechanisms against digital violence within the institutional system.

Improve monitoring

– Considering the trend of growth and the continuous advancement of technology, it is recommended that the justice institutions develop tools and methodology for recording and accurately monitoring acts of online technology-facilitated violence against women. This data would enable evidence-informed practices, from the planning of prevention programs, to the improvement of the institutional response.

Annex I: Note on terminology

In Bosnia and Herzegovina, there is no uniform terminology in the criminological and normative sense when it comes to on-line technology-facilitated violence against women.

Technology, especially that used in the online or digital world, has been amplifying or facilitating gender-based violence against women. However, violence against women and domestic violence committed in the digital sphere, whether as an isolated act or as part of a continuum of volence experience by women in the offline and online worlds is not comprehensively criminalised in the legislative framework of Bosnia and Herzegovina.

The alignment of the criminal laws in Bosnia and Herzegovina with the provisions of the Istanbul Convention and further articulated in GREVIO General Recommendation No. 1 on the digital dimension of violence against women in order to ensure criminalisation of all forms of online technology-facilitated violence against women does not appear to be a priority for the authorities. This has resulted in the lack of legally regulated ways of protecting citizens from online technology-facilitated violence at the state level, particularly in the entity of the Federation of Bosnia and Herzegovina and Brčko District.

While the Criminal Code of Republika Srpska recognises several forms of digital violence, its provisions are gender-neutral and do not acknowledge the structural nature of violence against women and girls. Moreover, the terms used in the criminal law such as 'digital sphere', 'through use of technology', 'computer network' leaves room for interpretation as well as not comprehensively encompassing both online apsects and technology-facilitated aspects of the harmful behavour perpetrated against women and girls, as required by the Istanbul Convention and further articulated in the General Recommendation No. 1.

The failure to incorporate a comprehensive understanding of the digital dimension of violence against women into the criminal laws directly influences procedures for reporting, investigating, collecting and securing evidence and proving the digital dimension of violence against women. Without properly defining the terms and forms of behaviours in line with international standards, the institutions responsible for the protection of victims and ensuring justice face obstacles, women are left without protection and support, and perpetrators remain free to continue to commit violence against women without consequences.

Annex II: Research tools – Interview questions and questionnaire

INTERVIEWS WITH JUDGES AND PROSECUTORS

Courts

1. Cases of digital violence:
   - How many cases involving digital violence have you handled to date? Please provide a numerical range or estimate.
   - Have you handled cases of gender-based violence with elements of digital violence, i.e., violence involving threats, intimidation through information and communication technologies, in the past three years?
   - How often do courts handle digital violence cases, and what are the most common forms of such violence?

2. Assessment of evidence:
   - Are threats and intimidations via information and communication technologies considered relevant evidence in gender-based violence proceedings?
   - What are the challenges in accepting and assessing such evidence during trials?

3. Legislative framework:
   - Would the introduction of a specific legal article criminalising digital violence and defining information and communication technologies as a means, method, and procedure in the commission of criminal offences, including violence against women, help in preventing and/or impacting the digital dimension of violence and stricter penal policy?
   - What impact would such a legislative change have on the work of courts and the protection of victims?

Prosecutor's Office

1. Indictments for digital violence:
   - Have you had confirmed indictments for cases of gender-based violence that include digital violence, i.e., violence committed using modern information and communication technologies?
   - How often are indictments raised for digital violence, and what are the main challenges in this?

2. Challenges in proving
   - How challenging is it to prove digital violence, i.e., violence committed using information and communication technologies?
   - What types of evidence are most commonly used in such cases, and how is their credibility assessed?

3. Legislative changes
   - Would the introduction of a specific legal article criminalising digital violence and defining information and communication technologies as a means, method, and procedure in the commission of criminal offences, as well as violence against women, help in preventing and/or impacting the digital dimension of violence?
   - What legislative changes do you consider key to better protecting victims of digital violence?

Interviews with Women

1. Experiences with digital violence:
   - Have you experienced violence, threats, intimidation via modern information and communication technologies? Did violent behaviour started on social media and continued in real life, or if it started in real life and continued online?
   - What were the most common forms of digital violence you experienced? (cyberstalking, online harassment, non-consensual sharing of intimate images, doxing, impersonation on social media, and the use of threats or intimidation via messaging platforms)

2. Reporting Digital Violence:
   - Did you report the violence, threats, intimidation via information and communication technologies, and to whom?

3. Help and Protection from Institutions:
   - Did the institutions you approached provide help and protection? What were your experiences with institutions, and what measures do you consider necessary for better protection of victims of digital violence?

Questionnaire – Ministries of Internal Affairs

1. Challenges in recording and providing protection

- Do police officers encounter reports of violence against women committed using information and communication technologies (SMS, call, Facebook, Instagram, Messenger, WhatsApp, TikTok, etc.) and what are the challenges in providing protection?
- Does the Ministry of the Interior keep special records of reports of violence against women committed using information and communication technologies (SMS, call, Facebook, Instagram, Messenger, WhatsApp, TikTok, etc.)?
- What is the number of reports of violence against women committed using information and communication technologies (SMS, call, Facebook, Instagram, Messenger, WhatsApp, TikTok, etc.)?

2. Legislative changes

- Would introducing a special article of the law that would criminalise digital violence and define information and communication technologies as a means, method and procedure in the commission of criminal offences, as well as acts of violence against women, help prevent and/or influence the digital dimension of violence?
- What changes in legislation do you consider crucial for better protection of victims of digital violence?

References

International documents

- Council of Europe, (20 October 2021) *GREVIO General Recommendation No. 1 on the digital dimension of violence against women*, Council of Europe, strana 13. Dostupno online (na Engleskom jeziku) na: https://www.coe.int/en/web/istanbul-convention/general-recommendation
- Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention) (2011) (CETS No. 210).
- Council of Europe Convention on Cybercrime (Budapest Convention) (2001) (CETS No. 185).
- GREVIO, (2022) *GREVIO's (Baseline) Evaluation Report on legislative and other measures giving effect to the provisions of the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention) Bosnia and Herzegovina*, Council of Europe.

National documents

- Criminal Code of Brčko District, "Official Gazette" of Brčko District, No. 19/2020, revised text and 3/2024.
- Criminal Code of the Federation of Bosnia and Herzegovina, "Official Gazette" of the Federation of Bosnia and Herzegovina, 36/03.
- Criminal Code of Republika Srpska, "Official Gazette" of Republika Srpska, 73/23.
- High Judicial and Prosecutorial Council of Bosnia and Herzegovina, *Annual Reviews of the Structure of Crime in Bosnia and Herzegovina 2018-2023*, available online at: https://vstv.pravosudje.ba/vstvfo/B/141/kategorije-vijesti/1198/1363/114475.
- Republika Srpska, 2023, Ministry of Internal Affairs of Republika Srpska, available online https://mup.vladars.rs/index.php?vijest=66&vrsta=statistike&stat=1.

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE