



# Technology-facilitated violence against women and girls

## SHORT GUIDE TO RECOGNITION AND REPORTING



**Technology-facilitated violence against women and girls**  
**Short guide to recognition and reporting**

Author: Gorica Ivić

Design and DTP: Lejla Jamakosmanović

Publisher: UN Women Bosnia and Herzegovina

Address: UN House, Zmaja od Bosne bb, Sarajevo, BiH

Year of publication: 2025

Place of publication: Sarajevo

ISBN: 978-9926-535-02-5

CIP record available in the COBISS system of the National and University Library of BiH under

ID number: 67488006

---

Technology-facilitated violence  
against women and girls

# **SHORT GUIDE TO RECOGNITION AND REPORTING**

Gorica Ivić

---

Sarajevo, 2025



This publication was produced within the framework of the global campaign “16 Days of Activism against Gender-Based Violence” and the joint programme Gender Equality Accelerator (GEA), in partnership with the European Union (EU), Sweden, and Denmark, implemented by UN Women, UNDP, UNFPA, and UNICEF in Bosnia and Herzegovina, as part of the United Nations cooperation with institutions of Bosnia and Herzegovina, with the aim of achieving gender equality and contributing to the realization of the Sustainable Development Goals (SDGs).

The views expressed in this publication are those of the author and do not necessarily reflect the official positions of the United Nations or its member states, implementing agencies (UN Women, UNDP, UNFPA, UNICEF), or the programme partners (European Union, Sweden and Denmark).

---

# INTRODUCTION

Digital technologies and online spaces have become integral to everyday life, communication, professional activities, and social engagement. At the same time, the very tools that enable connection, visibility, learning and empowerment are increasingly being used as means of control, intimidation, and violence against women and girls. Technology-facilitated violence represents a continuation of gender-based violence in the digital environment and cannot be viewed as “less serious” or separate from other forms of violence.

Women and girls in Bosnia and Herzegovina, particularly journalists, politicians, activists, and women who speak publicly about human rights, are increasingly exposed to threats, harassment, blackmail, stalking, the non-consensual publication of intimate content, and other forms of technology-facilitated violence. These attacks are not isolated incidents – they aim to silence, discipline, and exclude women from public, political, and digital spaces.

While the legislative framework in Bosnia and Herzegovina addresses certain forms of technology-facilitated violence through the criminal codes of Republika Srpska, the Federation of Bosnia and Herzegovina, and the Brčko District of BiH, practice shows that victims often encounter obstacles in recognizing violence, documenting evidence, and achieving effective protection. Insufficient understanding of technology-facilitated violence, the complexity of collecting evidence, and the fear of stigmatization further hinder reporting and the prosecution of perpetrators.

This guide was created with the aim of providing clear, understandable, and practical information on technology-facilitated violence against women and girls. It is intended for women who have experienced or are at risk of such violence, as well as for professionals working within institutions, civil society organizations, the judiciary, the police, and social work centres, serving as a tool for better understanding, recognition, and adequate response.

The handbook presents an overview of the legislative framework in Bosnia and Herzegovina, the most common types and forms of technology-facilitated violence, their consequences for the psychological, social, economic, and physical health of women, as well as basic guidelines for documenting evidence and reporting violence to competent institutions and platforms. Particular emphasis is placed on survivor safety, the importance of timely response, and the availability of support mechanisms through civil society organizations.

# LEGISLATIVE FRAMEWORK IN BOSNIA AND HERZEGOVINA

## Republika Srpska - Criminal Code of Republika Srpska<sup>1</sup>

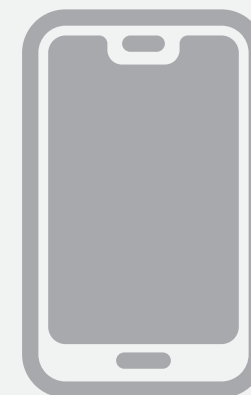
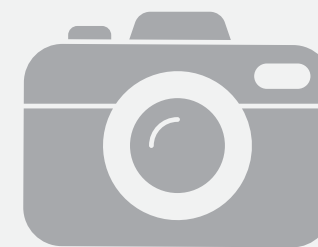


In Bosnia and Herzegovina, technology-facilitated violence is legally regulated through the criminal codes of Republika Srpska, the Federation of Bosnia and Herzegovina, and the Brčko District of Bosnia and Herzegovina.

Article	Criminal Offense	Description of the Act Constituting the Basic Offence	Aggravated Form of the Criminal Offence	Prescribed Penalty
156.	Unauthorized Photographing	(1) Taking photographs or video recordings of a person without their consent, thereby violating their privacy. (2) Disclosure or presentation of the recording to a third party, or otherwise enabling a third party to access or become acquainted with its content.	If the offence was committed by an official abusing their position.	Basic form: fine or imprisonment of up to <b>1 year</b> . Aggravated form: imprisonment from <b>6 months to 3 years</b> .
156a.	Unauthorized Publication and Display of Another Person's Document, Portrait, Photograph or Recording	Publishing/displaying content of a personal nature without consent, where such publication or display had or could have had harmful consequences to the personal life of the person concerned.	If committed against a family member or with the intent to damage reputation (Article 156a, Paragraph 2); severe consequences (serious impairment of health or death of the person whose document, portrait or recording was published- Article 156a, Paragraph 3).	Basic form: fine or imprisonment of up to <b>2 years</b> . Intent to cause harm / family member: imprisonment from <b>6 months to 3 years</b> Serious bodily harm: imprisonment from <b>1 to 5 years</b> . Resulting in death: imprisonment from <b>2 to 10 years</b> .
157	Unauthorized Use of Personal Data	Unauthorized collection, processing, disclosure or use of personal data; unauthorized access to a protected database.	If offense was committed by an official; attempt is punishable.	Basic form: fine or imprisonment of up to <b>1 year</b> . Unauthorized database access: Same prescribed penalty. By an official: imprisonment from <b>6 months to 3 years</b> .

[1] "Official Gazette of Republika Srpska", No. 64/2017, 104/2018 – Constitutional Court Decision, 15/2021, 89/2021, 73/2023; "Official Gazette of BiH", No. 9/2024 – Constitutional Court of BiH Decision; "Official Gazette of RS", No. 105/2024 – Constitutional Court Decision, 19/2025; "Official Gazette of BiH", No. 14/2025 – Constitutional Court of BiH Decision; "Official Gazette of RS", No. 31/2025 and 85/2025 – Constitutional Court Decision.

Article	Criminal Offense	Description of the Act Constituting the Basic Offence	Aggravated Form of the Criminal Offence	Prescribed Penalty
170.	Sexual Harassment	Unwanted verbal, non-verbal, or physical conduct of a sexual nature; violation of dignity; fear or a hostile environment.	Against a vulnerable person (due to subordination, illness, disability, age, pregnancy, impairments). <b>Committed via a computer network.</b>	Basic form: fine or imprisonment of up to <b>1 year</b> . Against a vulnerable person: imprisonment of up to <b>2 years</b> . Via network: imprisonment from <b>6 months to 3 years</b> .
170a.	Misuse of Sexually Explicit Photographs or Video Recordings	Abuse of a relationship of trust and making explicit recordings, originally created with consent, available to third parties without consent; creation or alteration of explicit recording and presenting it as authentic.	If committed <b>via a computer system</b> and made available to a larger number of persons.	Basic form: imprisonment of up to <b>2 years</b> . Via network: imprisonment from <b>1 to 3 years</b> . The recordings and equipment used shall be confiscated.
208a.	Defamation	Making or disseminating false statements about a person, where the person is identifiable and damage to reputation is caused.	If committed <b>through media, computer network</b> , at a public gathering or made available to a larger number of persons; if serious consequences occur.	Basic form: fine <b>BAM 1,000 – 3,000</b> Through media/network: <b>fine BAM 2,000 – 5,000</b> Serious consequences: <b>fine BAM 3,000 – 6,000</b> .
208b.	Disclosure of Personal and Family Circumstances	Disclosure of any information relating to a person's private or family life that may harm their honour or reputation, without justified public interest.	If made available to a larger number of persons; if serious consequences occur.	Basic form: <b>fine BAM 1,000 – 3,000</b> Through media/network: <b>fine BAM 2,000 – 5,000</b> Serious consequences: <b>fine BAM 3,000 – 6,000</b> .



# Criminal offenses under the Criminal Code of the Federation of Bosnia and Herzegovina<sup>2</sup> – Technology-Facilitated Violence

Article	Criminal Offense	Description of the Act Constituting the Basic Offence	Aggravated Form of the Criminal Offence	Prescribed Penalty
179a.	Stalking	Repeated following, stalking, or establishing unwanted contact directly, <b>through another person, or via ICT, thereby</b> causing distress or fear.	Against a family member, a child, a vulnerable person, or motivated by hatred.	Basic form - imprisonment of up to <b>1 year</b> ; Aggravated form – imprisonment of up to <b>3 years</b> .
181b.	Psychological Violence	Abuse or conduct that violates dignity and psychological integrity of a person.	Against a child, a vulnerable person, motivated by hatred, or <b>via ICT</b> .	Basic form - imprisonment of up to 1 year; Aggravated form - imprisonment from <b>6 months to 5 years</b> .
188.	Unauthorized Interception and Audio Recording	Unauthorized <b>interception or recording of conversations</b> , statements, or messages within a computer system, or enabling an unauthorized person to become acquainted with a conversation or statement that has been unlawfully intercepted or audio recorded.	If committed by an official in the performance of their official duties.	Basic form - fine or imprisonment of up to <b>3 years</b> ; By an official: imprisonment from <b>6 months to 5 years</b> .
189.	Unauthorized Optical Recording	<b>Recording a person without their consent</b> within their premises; showing or transmitting the recording or otherwise enabling a third party to directly access such recording.	If committed by an official.	Basic form - fine or imprisonment of up to <b>3 years</b> ; By an official: imprisonment from <b>6 months to 5 years</b> . Equipment used shall be confiscated.



[2] Criminal Code of the Federation of Bosnia and Herzegovina ("Official Gazette of the Federation of Bosnia and Herzegovina", No. 36/2003, 21/2004 – corrigendum, 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016, 75/2017, 31/2023 and 58/2025)

Article	Criminal Offense	Description of the Act Constituting the Basic Offence	Aggravated Form of the Criminal Offence	Prescribed Penalty
189a.	Misuse of Sexually Explicit Recordings	Abuse of a relationship of trust and, without the consent of the recorded person, delivering to a third party a <b>recording made with consent, or creating false/altered explicit recordings.</b>	If the recording is made available to a larger number of persons via a system.	Basic form - imprisonment of up to <b>3 years</b> ; Aggravated form - imprisonment from <b>6 months to 5 years</b> . Recordings and equipment used shall be confiscated.
203a.	Sexual Harassment	Unwanted verbal, non-verbal or physical conduct of a sexual nature that aims at or results in a violation of a person's dignity, causing fear or creating a hostile, humiliating or offensive environment.	Against a subordinate, dependent, vulnerable person, family member, close person, motivated by hatred or <b>via ICT</b> .	Basic form - imprisonment of up to <b>1 year</b> ; Aggravated form - imprisonment from <b>3 months to 3 years</b> .



# Brčko District of Bosnia and Herzegovina– Criminal Code of the Brčko District of Bosnia and Herzegovina<sup>3</sup> - Criminal Offences Related to Technology-Facilitated Violence

Article	Criminal Offense	Description of the Act Constituting the Basic Offence	Aggravated Form of the Criminal Offence	Prescribed Penalty
185.	Unauthorized Interception and Audio Recording	Any person who, by means of special devices and without authorization, intercepts or audio records a conversation or statement not intended for them, or enables an unauthorized person to become acquainted with a conversation or statement that has been unlawfully intercepted or audio recorded, or who unlawfully intercepts or records another person's messages within a computer system.	If committed by an official in the performance of their official duties.	Basic form - fine or imprisonment of up to <b>three years</b> ; Aggravated form - imprisonment from <b>6 months to 5 years</b> .
186.	Unauthorized Optical Recording	Any person who photographs, films or otherwise <b>records another person without their consent</b> within their premises, or directly transmits such recording to a third party, shows it, or otherwise enables a third party to become directly acquainted with it.	If committed by an official in the performance of their official duties.	Basic form - fine or imprisonment of up to <b>3 years</b> ; Aggravated form (official)-imprisonment from <b>6 months to 5 years</b> .
186a.	Misuse of a Recording Containing Sexually Explicit Content	Any person who abuses a relationship of trust and, <b>without consent, makes available to a third party a sexually explicit recording</b> created with consent for personal use, thereby violating the privacy of the person recorded, or creating a new recording or altering an existing sexually explicit recording, or presenting such recording as authentic, thereby violating the privacy of the person recorded.	If committed through the use of <b>ICT technology</b> or distributed to a larger number of persons.	Imprisonment of up to <b>3 years</b> (for both the basic and aggravated forms).



[3] Criminal Code of the Brčko District of Bosnia and Herzegovina ("Official Gazette of the Brčko District of BiH", No. 19/2020 – consolidated text, 3/2024 and 14/2024)

# TYPES AND FORMS OF TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN AND GIRLS



**Airdrop (cyberflashing)** enables the exchange of content between nearby Apple devices. **Example of violence:** The perpetrator sends unsolicited sexually explicit images to women in public spaces (e.g., bus, cafe). As such content can often be transmitted anonymously, victims experience fear, discomfort and insecurity in public environments.

**Algorithm** determines which content we see on social networks. **Example of violence:** Algorithms can amplify misogynistic content, insults, and threats directed at women, as they often favour content that provokes strong reactions. This encourages echo chambers, radicalization, and coordinated attacks on women, particularly targeting female journalists, politicians, and activists.

**Cloud** is a method of storing data on external servers. **Example of violence:** The perpetrator hacks the victim's account, accesses private files, and threatens to publish intimate content. Such acts result in fear, coercion and long-term psychological, professional and social consequences.

**Body shaming** involves commenting on and mocking a person's physical appearance (GREVIO, 2021). **Example of violence:** Women are subjected to insults, ridicule, and the circulation of manipulated images on social media. Consequences may include shame, anxiety, withdrawal from digital spaces and deterioration of mental health.

**Creepshots** are sexually suggestive images of women taken without their consent (GREVIO, 2021). **Example of violence:** The perpetrator secretly photographs a woman in a public space, focusing on intimate body parts, and subsequently shares the images on forums and pornographic platforms accompanied by degrading comments.

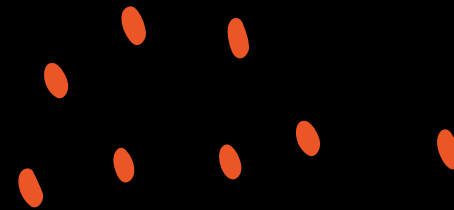
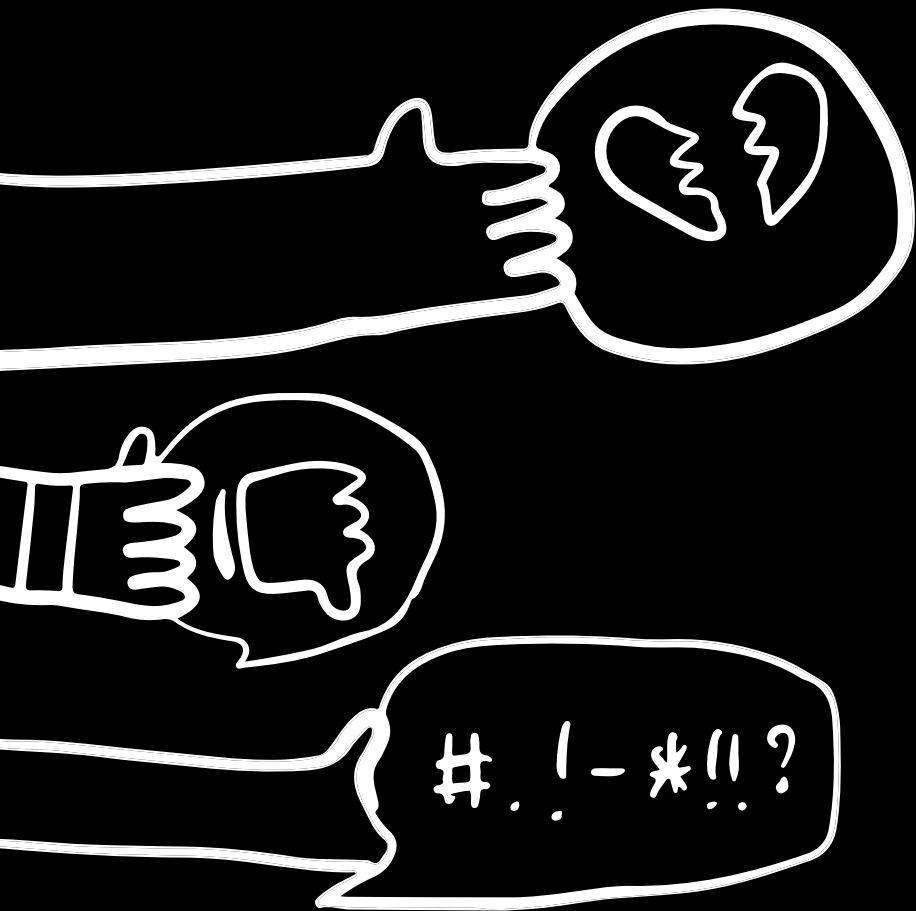
**Cyberbullying** refers to abuse carried out through digital tools and platforms, most commonly targeting minors (GREVIO, 2021). **Example of violence:** Perpetrators use networks to share insults, mock victim's appearance, publish private information, or create fake profiles in order to humiliate her.

**Cyberflashing or cyber exhibitionism** involves sending unsolicited sexually explicit content via dating apps, messages, or technologies such as AirDrop (GREVIO, 2021). **Example of violence:** A woman in a public space receives an explicit image from an unknown person via AirDrop or direct message, without consent.

**DDoS attack** is an attempt to overload a website or server by sending excessive traffic, thereby preventing normal functioning. **Example of violence:** Women's rights activists or organizations become targets of an attack that crashes their websites and disables communication.

**Deepfakes and media manipulation** are videos in which one person's face is digitally replaced with another's using algorithms and artificial intelligence, often combined with altered audio to create the illusion that another person's actions are staged. (GREVIO, 2021). **Example of violence:** The perpetrator uses deepfake technology to replace a female politician's face onto the body of a person in an explicit pornographic video. The fabricated content is then shared on social media and websites, alongside degrading comments and insinuations.





**Doxing (revealing private data)** refers to the online publication of a victim's personal information without consent (GREVIO, 2021). **Example of violence:** Following a public appearance, a human rights activist's personal data, such as home address, phone number, email, or business contacts are deliberately published on social media, forums, or websites to intimidate her or incite others to harass her, which can result in death threats and continuous harassment.

**Silencing** denotes the exclusion from online discussions due to fear of violence or harassment (GREVIO, 2021). **Example of violence:** A journalist becomes the target of coordinated online attacks including death threats, sexual harassment, and the publication of personal data. Due to the intensity of the attacks, the journalist deactivates her accounts to protect herself and her family, thereby losing access to professional communication channels and effectively being silenced as a public voice.

**Geolocation** is a digital function that enables the determination of a device's geographic position via GPS signals. **Example of use in the context of violence:** The perpetrator secretly installs a tracking application or uses an already enabled GPS function on the victim's device to track her movements in real time. Information regarding locations such as home or workplace may be used for control, intimidation, or planning physical attack

**Hacking** refers to unauthorized access to digital accounts, devices, or networks. **Example of violence:** The perpetrator uses stolen passwords or specialized tools to access the victim's email or social media accounts. After gaining access, the perpetrator retrieves private messages and content, and publishes them to publicly shame, manipulate or intimidate the victim.

**“Happy slapping” (Filmed Assault)** refers to the recording of a physical or sexual assault and the subsequent distribution of the footage online. **Example of violence:** A group of perpetrators physically attacks a woman while one of them records the assault. The video is then shared on social media, triggering further insults, harassment and a renewed cycle of humiliation for the victim. The recording often encourages perpetrators to make the violence more "dramatic" in order to attract attention.

**Image-based sexual abuse or non-consensual sharing of intimate content** involves distribution of sexually explicit images or videos without the victim's consent (GREVIO, 2021). **Example of violence:** A partner or former partner publishes intimate photos, that were originally taken with the victim's consent, on pornographic websites or forums without the victim's permission.



**Sexual Extortion**, commonly referred to as “sextortion,” refers to an act in which a perpetrator uses the threat of publishing sexual content – such as images, videos, deepfake material, or sexual rumours – to intimidate, coerce, or blackmail a victim. Perpetrators typically demand additional sexual content, money or both, exercising manipulation and control over the victim (GREVIO, 2021). **Example of violence:** The perpetrator threatens to release explicit images unless the victim provides additional sexual content. In other cases, the perpetrator may hack the victim's phone or social media accounts to obtain intimate content, and uses threats of publishing that material for financial extortion.

**Spyware/Stalkerware** refers to software that monitors the activities of a victim's device without their knowledge (GREVIO, 2021). **Example of violence:** The perpetrator secretly installs a tracking application, known as spyware or stalkerware, on the victim's phone. This application enables monitoring of messages, calls, emails, and real-time location. Additionally, spyware can enable access to the device's camera and microphone, meaning the perpetrator can listen to private conversations and see where or what the victim is doing.

**Trolling** – organized mobbing and online harassment which involves intentionally posting offensive comments to provoke a reaction (GREVIO, 2021). **Example of violence:** A group of social media users coordinates to post offensive, misogynistic, and threatening comments on the profile of a women's rights activist. The comments include humiliation, ridicule, and threats of violence. These attacks often escalate into a coordinated campaign involving false accusations, sharing disinformation, and encouraging other individuals to participate in the harassment.



# CONSEQUENCES OF TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN



## Psychological Consequences

Violence perpetrated through technology leaves deep emotional wounds. Constant exposure to threats, humiliation, and surveillance leads to anxiety, depression, sleep disturbances and feelings of isolation. Many women often experience the feeling of being "trapped," as the violence does not stop with physical distancing - the perpetrator may remain present at all times through digital channels. Fear is further intensified when the victim knows or suspects that the perpetrator has access to sensitive information (location, messages, photos). Due to social stigmatization and fear of judgment, many women do not report the harassment, which increases their emotional exhaustion.

## Social Consequences

Victims often withdraw from social media platforms to avoid attacks, threats, and humiliation, thereby losing important opportunities for communication, education, and professional development. The non-consensual publication of intimate content causes permanent stigmatization - once content is online, it becomes an indelible part of a woman's life. This limits her freedom, undermines her self-confidence, and can lead to withdrawal from social and public life, especially among female journalists, politicians, and activists.

### **Economic Consequences**

Digital violence can seriously jeopardize a victim's professional reputation. The publication of private information or sexualized content may result in job loss, career stagnation, or withdrawal from the profession due to stigma and reputational damage. The costs of legal assistance, content removal, and other technical support are often high, and financial blackmail further exacerbates the situation. Many victims are left without stable incomes, facing long-term economic consequences.

### **Legal Consequences**

Due to insufficiently developed legal frameworks and the complexity of collecting and preserving digital evidence, victims often encounter difficulties in reporting and prosecuting perpetrators. Online anonymity, the use of VPNs and other technical tools make it difficult to identify perpetrators. Institutions sometimes lack the technical expertise and capacity to respond effectively, which further discourages reporting and contributes to a culture of impunity.

### **Permanence of Digital Content**

Once published, content can remain accessible for months or years. Every time it reappears, it causes retraumatization and a renewed sense of loss of control. Content removal processes are often long, complex, and incomplete. Digital violence knows no borders - it can appear at any time, across multiple platforms, creating a constant sense of danger.

### **Physical Consequences**

Digital violence is frequently interconnected with physical and sexual violence. Threats transmitted online may escalate into physical attacks, particularly when the perpetrator uses geolocation, spyware, or other tools to track the victim. Such forms of control increase the risk of physical violence, restrict the victim's movement, and hinder access to help. Digital technologies thus become an extension of the perpetrator's power and control over the victim.

# DOCUMENTING TECHNOLOGY-FACILITATED VIOLENCE AND ABUSE



## Why is it important to document violence and preserve evidence?

If you decide to report violence to an online service or platform, the police, or another competent institution, you will likely be required to provide evidence of the abuse/violence you have experienced. Evidence can also be used **in court, in criminal proceedings, if you are seeking a protective order, or in proceedings related to domestic violence and/or child custody.**

Even if you do not currently feel ready to report the violence, documenting incidents and collecting evidence can provide you with important options in the future. This is particularly important if you believe the perpetrator might delete traces of the abuse or remove content testifying to the violence you have been exposed to, evidence which you might need later.

Experiencing violence can be very difficult, and some actions may seem too stressful and challenging – including documenting and collecting evidence, which may upset you further, especially if you encounter unexpected information. Do not pressure yourself to document everything perfectly; rather, collect evidence only when it is safe to do so. Do as much as you can, and seek support if you need it.



## What types of evidence should be documented and preserved?

It is important that you try to preserve all information that may help identify person responsible for technology-facilitated violence.

### Record details such as:

- Harmful or abusive content: messages, comments, images, or videos sent to you or shared about you
- The platform or service through which the content was sent or shared
- Source data, such as HTML code and the URL address of the website where the content appeared. URL (Uniform Resource Locator) represents the unique address of a website, e.g., <https://www.facebook.com>. It is visible in the browser, and should be copied directly rather than typed manually to avoid errors
- Usernames and profile URLs used to send or share content
- Dates and times when the content was published
- Records of financial transactions, if any
- SMS messages, including the perpetrator's phone number and the full message history
- Voice messages, save or record copies of all threatening or offensive voice messages
- Number and time of calls and messages received
- Fake profiles created in your name
- Tracking or surveillance devices found in your home, vehicle, bag, etc.
- Evidence of installed tracking applications
- Unauthorized logins to your devices or online accounts
- Any use of children as part of the abusive conduct
- Medical findings and documentation, if you have visited a healthcare institution due to the consequences of violence
- Any other evidence demonstrating a pattern of abusive behaviour

## Search for your data online

If you believe your private information has been published without permission (doxing):

- search for your name on the internet
- check if your number, address, or photos have been published
- use "reverse image search" (a method of searching the internet using an image instead of text)
- check websites that provide phone number lookup services

## Document recurring behaviours

Technology-facilitated violence often includes: repeated contacts, persistent harassment, surveillance, tracking. Keep notes on every incident, even if it seems insignificant. Combined with photos, screenshots, and records, this can help demonstrate a pattern of abusive behaviour. For the criminal prosecution of these acts, it is often necessary to prove continuity and repetition of the behaviour.

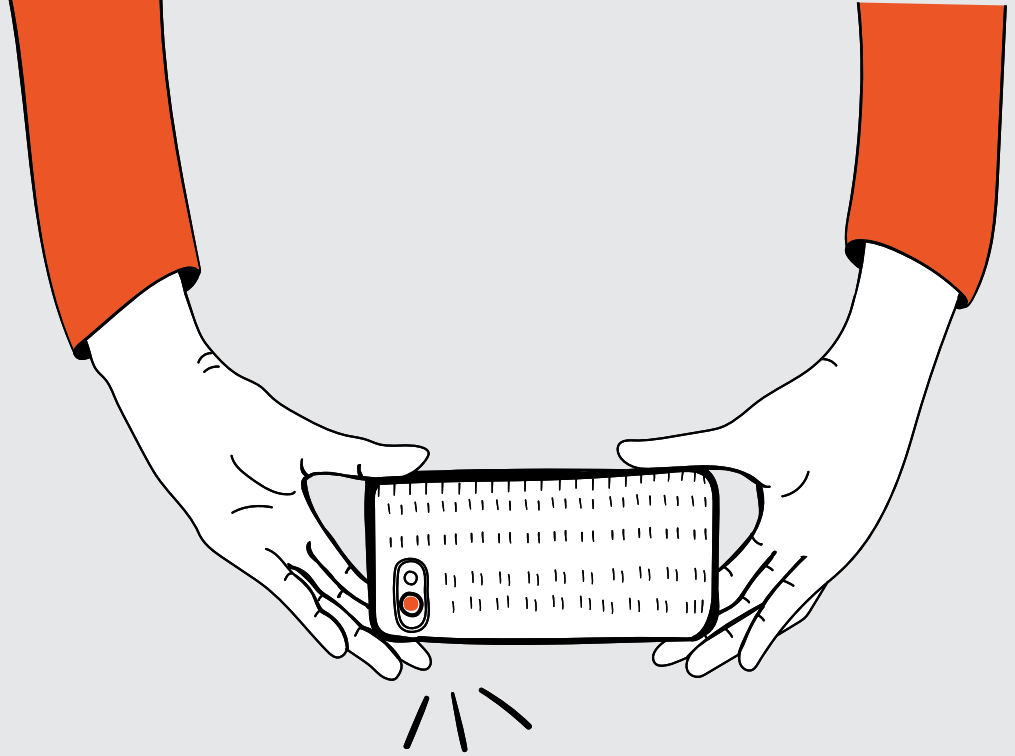
## Take screenshots, photos and recordings

Screenshots, photos, and screen recordings are the most effective ways to document: abusive messages, social media posts, live chats, and perpetrator profile data. When taking a screenshot, ensure that profile name and profile photo of the perpetrator are clearly visible.

*Save original content without editing – do not highlight text, do not crop images.*



*If the message is part of a longer communication, capture the entire conversation, including dates, times, and usernames. Some apps notify users when a screenshot is taken. In such cases, it may be safer to photograph the screen using another device.*



## Document surveillance and tracking

If you suspect you are being tracked via: tracking devices, spyware apps, smart home devices, and/or cameras, document:

- where and when the tracking appears to occur
- patterns of behaviour
- suspicious devices or device packaging/boxes (take a photo of them)

If you discover a device (e.g., AirTag), **take a photo of it and leave it in place until you notify the police** – removing the device may alert the perpetrator.

## How to safely document violence and preserve evidence

There are several ways to collect evidence – some may be safer than others, depending on your situation. Always use a **secure device** to collect evidence, especially if you suspect you are being tracked or monitored. **A secure device is one that you can use without the perpetrator's knowledge.**

### This can be:

- your own device (if the perpetrator does not have access to it)
- device belonging to a trusted person – a friend or family member
- computer at work

Avoid using a secure device to log into accounts that the perpetrator knows about or may control. If you must use a potentially compromised device, delete traces as soon as you send the evidence to a trusted person.

## To protect the evidence:

- verify who has access to your devices and cloud services
- use strong passwords and enable multi-factor authentication
- make sure that your cloud service does not automatically delete content after a certain period of time

Create a separate folder, give it a name recognizable only to you, and, where possible, make multiple copies stored separately.

## ADVICE

- **Do not communicate with the perpetrator(s)! Do not respond and do not delete messages!**
- **Do not agree to blackmail (if the perpetrator demands it, do not give money, do not send photos or videos, do not agree to favours/concessions, etc.).**
- **Do not alter, delete, or edit the evidence. Any alteration diminishes its value as evidence.**
- **Preserve original files whenever possible and make copies. Original files containing metadata (EXIF data, email headers) carry greater evidentiary value than just screenshots.**
- **If the violence was committed via email, save the sender's original message, including the full header and content.**
- **Document all incidents of violence: who sent or published what, and when.**
- **If the threat/blackmail is serious REPORT IT TO THE POLICE IMMEDIATELY!**



## Reporting technology-facilitated violence

Timely reaction by competent authorities is crucial for protection. There are several ways to report technology-facilitated violence:

### Reporting violence on social media platforms

#### Using platform reporting tools:

Most social media platforms like Facebook, Instagram, TikTok, and X (Twitter) have built-in options for reporting inappropriate content. You can report offensive comments, threats, fake profiles, or harassing messages directly through the platform.

#### Blocking and reporting users:

If you are experiencing harassment, you can block the user and report their account so the platform can initiate the process of removing content or restricting access. However, if you intend to report the violence to competent institutions and fear that the abuse may continue through alternative or newly created profiles, it may be advisable not to block the user immediately but instead to report the matter to the police.

### Reporting to competent institutions

#### Police:

You can report technology-facilitated violence by:

- calling **122** (police emergency number),
- visiting the nearest police station/administration,
- contacting official police departments in your entity or canton.



The police are obliged to receive every report, implement protective measures, and initiate an investigation.

Upon receiving a report, the police will communicate with internet service providers to preserve evidence necessary for further investigative proceedings, obtain relevant data upon formal request, and, if necessary, remove unwanted content from online spaces.

Within the police framework at the entity and cantonal levels, Departments for Combating Computer and High-Tech Crime / High-Tech Crime Units have been established, which you may contact directly via email.

**When reporting to the police, you will typically be required to provide:**

- your personal information
- information about protective measures, if they have already been imposed
- the identity of the perpetrator (if known)
- any known criminal history of the perpetrator
- all available information and evidence related to the violence

You may be required to hand over the device containing evidence of violence to the police for an extended period (e.g., your personal mobile phone). It is important to clearly explain how the technology-facilitated violence has affected you, what consequences it left, whether you are frightened,

upset, or if you are experiencing psychological disturbances as a result. Also, state if the violence has led to changes in your daily life, such as, you no longer use social networks, you have changed your place of residence, you do not go out to the same places, you avoid appearing at public gatherings, you have changed jobs, etc. This is important for processing the violence and for the formal evidentiary procedure before the competent institutions.

If the violence occurs within a domestic context, you may request the imposition of emergency or protective measures against the perpetrator, which are implemented regardless of criminal proceedings, and their purpose is to protect victims from the recurrence of violence. If the police fail to initiate such measures, you may submit a request directly to the competent court (according to the place where the act occurred).

### **Centers for Social Work:**

If technology-facilitated violence occurs in the context of domestic violence (partner, former partner, family member), you may also contact the competent Center for Social Work.

### **The Center is obliged to:**

- immediately notify the police,
- provide support and refer you to other relevant services.

### **Prosecutor's Office:**

In any case, and particularly in more serious cases (death threats, blackmail, unauthorized recording, publication of intimate content), you may file a criminal report directly with the competent prosecutor's office.



## Civil Society Organizations:

In Bosnia and Herzegovina, there are several organizations that provide counselling, legal assistance, and psychological support to women survivors of various forms of violence, and you can turn to them for help and support.

### Some of them are:

- Center of Women's Rights Zenica - <https://cenppz.org.ba/>
- Foundation "Lara" Bijeljina - <https://www.fondacijalara.com/>
- Foundation of Local Democracy Sarajevo - <https://fld.ba/>
- Foundation United Women Banja Luka - <https://udruzene-zene.org/>
- Medica Zenica - <https://medicazenica.org/>
- Association "Novi put" Mostar - <https://www.newroadbih.org/>
- Association of Citizens "Budućnost" Modriča - <https://buducnost-md.org/>
- Association of Citizens "Vive žene" Tuzla - <https://vivezene.ba/>
- Association "Women from Una" Bihać - <https://www.zenesaune.org/>
- Women's Center Trebinje - <https://zenskicentar.org/>



## References:

European Women's Lobby. (2024). *Full report on cyber violence against women and girls*. Brussels.  
<https://www.womenlobby.org/full-report-cvawg>

GREVIO. (2021). *General Recommendation No. 1 on the digital dimension of violence against women*. Council of Europe.  
<https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147>

United Nations. (2022). *Technology-facilitated violence against women: Towards a common definition*. Report of the Expert Group Meeting, 15–16 November 2022, New York: UN Women.  
<https://www.unwomen.org/en/resources/tfvaw-common-definition-report>

Criminal Code of the Federation of Bosnia and Herzegovina. *Official Gazette of the FBiH*, No. 36/2003, 21/2004 (corr.), 69/2004, 18/2005, 42/2010, 42/2011, 59/2014, 76/2014, 46/2016, 75/2017, 31/2023 and 58/2025.

Criminal Code of the Brčko District of Bosnia and Herzegovina. *Official Gazette of the Brčko District of BiH*, No. 19/2020 (consolidated text), 3/2024 and 14/2024.

Criminal Code of Republika Srpska. *Official Gazette of Republika Srpska*, No. 64/2017, 104/2018 (Constitutional Court decision), 15/2021, 89/2021, 73/2023, *Official Gazette of BiH*, No. 9/2024 (BiH Constitutional Court decision), *Official Gazette of the RS*, No. 105/2024 (Constitutional Court decision), 19/2025, *Official Gazette of BiH*, No. 14/2025 (BiH Constitutional Court decision), *Official Gazette of the RS*, No. 31/2025 and 85/2025 (Constitutional Court decision).

Council of Europe. (2011). *Convention on preventing and combating violence against women and domestic violence (Istanbul Convention)*. Istanbul.  
<https://rm.coe.int/1680462540>

Council of Europe. (2022). *EDVAW Platform: Thematic paper on the digital dimension of violence against women*. Strasbourg.  
<https://www.coe.int/en/web/edvaw/digital-dimension-vaw>

General Protocol on Procedure in Cases of Domestic Violence in Republika Srpska, (2022). *Official Gazette of Republika Srpska*, No. 38/2022.  
[https://www.vladars.net/sr-SP/Cyrl/Vlada/Ministarstva/mpos/Documents/Opsti%20protokol%20o%20postupanju%20u%20slucajevima%20nasilja%20u%20porodici%20u%20Republici%20Srpskoj\\_342565218.pdf](https://www.vladars.net/sr-SP/Cyrl/Vlada/Ministarstva/mpos/Documents/Opsti%20protokol%20o%20postupanju%20u%20slucajevima%20nasilja%20u%20porodici%20u%20Republici%20Srpskoj_342565218.pdf)

Law on Protection from Domestic Violence and Violence against Women in the Federation of Bosnia and Herzegovina. *Official Gazette of the Federation of BiH*, No. 19/2025 of 14 March 2025.  
<https://advokat-prnjavorac.com/Zakon-o-zastiti-od-nasilja-u-porodici-i-nasilja-prema-zenama-FBiH.html>



**ONLINE  
VIOLENCE  
=  
REAL  
VIOLENCE**

