



PS-CGBV

TRAINING CURRICULUM FOR VICTIM SUPPORT SERVICES AND YOUTH WORKERS



<https://ps-cgbv.eu>



Table of contents

1. Introduction	8
2. Forms of Cyber GBV	9
Objectives	9
2.1. Theoretical framework	9
2.1.1. Sexual and sexually motivated cyber violence	9
2.1.2. Cyberbullying - violence against a specific person	12
2.1.3. Limiting freedom through technology	14
2.1.4. Xenophobia, radicalism, insults on the basis of belonging to a minority group	14
2.1.5. Toxic communities	16
2.2. Best practices	17
2.2.1. Manual for experts who work with youth, research report (Slovenia)	17
2.2.2. Staying Safe Online: Gender and Safety on the Internet: Experiences of Young Women and Men in Cyprus	18
2.2.3. The Warriors against GBV project	18
2.3. Conclusion	18
2.4. Exercises	18
Activity 1: Role-Playing Scenarios	18
Activity 2: Cyber GBV Impact and Storytelling	20
3. Prevention of cyber GBV	22
Objectives	22
3.1. Theory	22
3.1.1. Principles of prevention	22
3.1.2. The role of education & educational activities in prevention	27
3.1.3. Multi- sectoral approach to preventing cyber gender-based violence	28
3.1.4. Empowering users	30
3.2. Best practices	31
3.2.1. Undefeated - best practice of campaign for universal prevention of CGBV	31
3.2.2. "I can say I won't!" - site with various material for universal prevention	32
3.2.3. "No to online violence!" - example of multisectoral approach	39
3.2.4. Common sense education - examples of ready-made workshops for promoting digital communication and preventing cyberbullying	39
3.3. Conclusion	39
3.4. Exercises	40

Activity 1: Interactive Prevention Strategy Development	40
Activity 2: Cyber GBV Awareness Campaign	41
Activity 3 : Creative Posters Against Cyber GBV and Advocacy	43
4. Consequences of online violence	45
Objectives:	45
4.1. Theory	45
4.1.1. Psychological consequences	45
4.1.2. Consequences for interpersonal and social relations	46
4.1.3. Economic consequences	46
4.1.4. Physical effects	47
4.2. Best practices	47
4.3. Conclusion	48
4.4. Exercises	48
Activity 1: "Consequence Collage" Creation and Gallery Walk	48
Activity 2: Impact Analysis and Response Planning	49
5. Counseling for perpetrators of cyber GBV	52
Objectives:	52
5.1. Theory	52
5.1.1. Foundations of rehabilitation - understanding the behavior; ethics and boundaries	52
5.1.2. Assessment and evaluation of perpetrators	53
5.1.3. Education and skill development	53
5.1.4. Intervention strategies	54
5.2. Best practices	56
5.2.1. WWP European Network - Training on Cyber Violence and Perpetrator Work	56
5.2.2. Contexto	57
5.3. Conclusion	57
5.4. Exercises	58
Activity 1: Perpetrator Rehabilitation Role-Play and Discussion	58
Activity 2: Interactive Learning Stations on Rehabilitation Approaches	59
6. Proactive strategies to protect oneself online	61
Objectives	61
6.1. Theory	61
6.1.1. Digital/Cyber hygiene	61
6.1.2. Practicing self-care and setting boundaries	63
6.1.3. Understanding the main principles of manipulation	66
6.2. Best practices	68
6.2.1. Cyber gender-based violence awareness campaigns	68

6.2.2. Education through games	69
6.2.3. Advocacy for stricter laws	70
6.3. Conclusion	71
6.4. Exercises	72
Activity 1: Recognising main principles of manipulation	72
Activity 2: Creating an awareness campaign	73
Activity 3: Cyber Hygiene and Digital Well-being Workshop	75
Activity 4: "Digital Self-Defense" Role-Playing Game	76
7. Provision of psychological support to the victim	78
Objectives	78
7.1. Introduction	78
7.2 Theory	78
7.2.1. The Psychological Impact of Cyber Violence	78
7.2.2. Psychological Support Techniques	79
	82
Best Practices	82
EU Kids Online Network	82
Overview	82
Key Activities and Contributions	82
Safer Internet Centres (SICs) across Europe	83
Overview	83
Key Activities and Contributions	83
	86
8. Legal guidance – Where and how to report online abuse	87
Introduction	87
BULGARIA	89
CYPRUS	90
CZECH REPUBLIC	91
Republic of Croatia	92
Greece	93
9. Conclusion	96
10. ANNEX	98
Chapter 2 - Activity 3 - Story Prompts	100
Chapter 3 - Activity 1 Interactive Prevention Strategy Development	101
Chapter 5 - Activity 2	102
Chapter 6 - Activity 1	104
Chapter 6 - Activity 3	105
Digital Defense Toolkit Cards	106
Game Setup	106
Chapter 7 - Activity 1	107
6.5. Sources:	120

https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4126576/	121
https://www.sciencedirect.com/science/article/pii/S2666557323000228	121
https://www.uktherapyguide.com/cyberbullying	121
https://domental.com/online-therapy/cyberbullying-therapy	121
https://www.academia.edu/79061163/Cyberbullying_and_its_impact_on_young_peoples_emotional_health_and_well_being	121
https://socialwork.buffalo.edu/social-research/institutes-centers/institute-on-trauma-and-trauma-informed-care/what-is-trauma-informed-care.html	121

1. Introduction

This project - Prevention and Support for Cyber Gender-Based Violence, is implemented within the Erasmus+ KA2 program, by a partnership, led by the Association of Ladies Union of Drama - HOH (Greece), together with The Future Now Association (Bulgaria), South-Western University "Neofit Rilski" (Bulgaria), Gender studies (Czech Republic), Osijek University (Croatia) and DOREA Educational Institute (Cyprus).

"Additional information about the project and our partners is available on our website: <https://ps-cgbv.eu/>"

The project aims to develop meaningful and useful materials for young people and professionals in the field of prevention and support, focusing on cyber gender-based violence.

"Through the project, we have developed several key resources:

1. A web hub against cyber gender-based violence (CGBV): <https://ps-cgbv.eu/>
2. An interactive map showcasing best practices at the EU level: <https://ps-cgbv.eu/#/en/resources-map>
3. A Digital Youth Handbook on CGBV: <https://ps-cgbv.eu/#/en/sp/youth>
4. This Training Curriculum for Victim Support Services and Youth Workers
5. An Interactive Quiz for Self-Assessment
6. And a comprehensive final research paper.

Additionally, we are engaged in various dissemination activities to amplify the project's impact.

This document offers an expanded training curriculum that serves as a guide for:

- Understanding and recognizing CGBV;
- Engaging in prevention work related to CGBV;
- Exploring the connection between online violence and its real-life implications, such as stalking, and the consequences for victims;
- Strategies for working with perpetrators of CGBV.

Each chapter begins with specific learning objectives, encompasses relevant theories and best practices for inspiration, and concludes with practical applications of the learned concepts. We highly recommend going through this curriculum with colleagues to facilitate discussions, gain diverse perspectives, and collaboratively tackle this challenging subject.

As a partnership, we are thrilled to have you engaged in this field and wish you success in your endeavors!

2. Forms of Cyber GBV

Objectives

- To identify the interconnections between physical and online violence, emphasizing the importance of a comprehensive perspective
- To understand the gender aspects of cyber violence.
- To learn about various forms of GBCV and their manifestations.
- To discern between acceptable and unacceptable online behaviors, including offensive activities.

2.1. Theoretical framework

Gender-based cyber violence can be categorised into the following: **sexual violence, cyberbullying, technological restrictions on freedom, xenophobic violence, and toxic communities**. This is an artificial division, and many manifestations of gender-based violence cut across multiple categories, yet it is practical to categorize the various manifestations of gender-based cyber violence if it helps to better understand the nature of the problem.

2.1.1. Sexual and sexually motivated cyber violence

Sexual and sexually motivated cyber violence can take place between people who know each other, but also between strangers. This type of violence is specific in that it involves an inappropriate desire to engage in a sexual relationship (i.e. sexual motivation) or involves sexually explicit content, or both.

It is important to understand that it is common nowadays for people to express their sexuality through online technologies. We can probably agree that, for example, adult dating on Tinder, flirting in private messages on Instagram or communication between people who are in a relationship on WhatsApp are all perfectly normal and safe activities. So where is the line that we shouldn't cross?

It is essential that all those involved in these activities do so consensually, i.e. with mutual consent. For example, if I want to flirt with someone on social media but the other person explicitly rejects me, does not respond to me or blocks me, I must stop my behavior, or I am committing violence. Similarly, there is a fundamental difference between exchanging arousing photos between people who build sexual tension with each other in this way in a consensual and mutual way, and so-called **dickpics**, i.e. unsolicited photos of penises.

The biggest problem arises when sexually motivated cyber violence is directed against minors. In this case, it often crosses the line of legality and becomes a criminal

offense - typically **the distribution of pornography to a child, the use of a child to produce pornography and the possession of child pornography are all criminal offenses**. These offenses are often committed unwittingly by adolescents themselves, for example when they exchange intimate photographs of themselves in a peer-to-peer romantic relationship.

Manifestations of sexual cyber violence

cyber grooming	Behavior where the aggressor makes contact with a (usually) minor in an online environment in an attempt to gain their trust and get them to meet in person, leading to a sexual assault. Most cases of cyber grooming are perpetrated by men against underage girls ¹ .
sexting	Sexting is a communication activity using electronic devices involving sexually explicit messages and pictures (e.g. nudes, dick pics - see below). There are various platforms where sexting can happen: not only dating apps but also widely used applications such as Instagram, Facebook, WhatsApp etc. Sexting as such can be a part of healthy and consensual sexual behavior; non-consensual sexting however is a form of sexual abuse.
dick pics	Dick pics are pictures of someone's penis taken and distributed by an electronic device such as smartphones. If not consensual, they are a form of online sexual abuse. They are disproportionately often sent to women and girls by men, sometimes using short-range wireless technology (see Cyber flashing).
cyber flashing	Cyber flashing is a form of sexual abuse using short-range wireless technology such as Bluetooth or AirDrop technology to send sexually explicit pictures or videos (e.g. dick pics - see above). The content is distributed to electronic devices of victims randomly and without their consent.
online harassment	Online harassment can be defined as using ICT to stalk, intimidate, harm, or disgrace someone. In many definitions, there is emphasis on repeated action by an individual or a group against someone. However, in broader terms online harassment can consist of many different strategies varying in intensity, frequency and online tools employed to enact them. Online harassment can affect people regardless of their gender but the strategies and content differ significantly with regard to the gender of the victim.
rape threats	Rape threat is a threat of sexual assault made against another person with varying goals of the perpetrator. On the internet, rape threats are often used to intimidate women and LGBTQ+ people; e.g.

¹ <https://www.nspcc.org.uk/about-us/news-opinion/2022/online-grooming-crimes-rise/>

	as a part of hate speech or as an intimidation tactic carried against women in positions of power and in a professional setting.
coercing	Coercion is a set of manipulative tactics used with the goal of obtaining activities of a sexual nature or consent to such activities. Coercive tactics vary in force and nature and can manifest as compliments, paying special attention to the victim, continually requesting sexual activities and can go as far as grooming, insults, threats, etc. The perpetrators often play the “nice” guys and employ various sexist, misogynistic, homophobic, racist and other myths and stereotypes. It is important to note that consent obtained by coercive methods is not freely given and cannot be considered as valid.
revenge porn	Revenge porn is a form of sexual abuse. It is a type of non-consensual pornography that involves online distribution of sexually graphic photographs or videos without the consent of the individual in the images. “The perpetrator is often an ex-partner who obtains images or videos in the course of a prior relationship, and aims to publicly shame and humiliate the victim, in retaliation for ending a relationship.” ² Revenge porn is often used as a tool of coercion, blackmail, sextortion (see below and above) etc.
upskirting, downblousing	Recording or taking pictures under someone’s skirt (upskirting) or of someone’s chest/breasts through the neckline of their clothing (downblousing), usually with the intention of publication. It happens without consent and usually even without knowledge of the person being recorded. There are even specialized internet forums and groups where this kind of images and videos are being shared.
recording and distribution of sexual assault	Recording and distribution of sexual assault is one of the most serious manifestations of sexualised violence on the internet and is in itself a criminal offence. However, it is important to note that a part of such content is overlooked or misinterpreted due to distribution of the recordings amongst other pornographic content on mainstream pornographic websites. The prevalence of rape-themed content on mainstream pornographic websites is itself a disturbing manifestation of rape culture, and in many cases, presumably consensual pornographic content can be a result of assault or coercion.
victim blaming	In the still prevalent rape culture (i.e. social environment where

rape and other forms of sexual violence are pervasive and normalized, being made light of, joked about or dismissed, due to societal attitudes towards gender (in)equality), victim blaming is a strategy to dismiss the severity of sexual abuse by shifting the blame from the perpetrator to the victim. It relies on various myths stemming from sexism, misogyny or purity culture and ignores relevant data. Social media can be an effective tool of victim blaming considering their ability to quickly and widely broadcast victim-blaming content and harass the victim.

2.1.2. Cyberbullying - violence against a specific person

A specific form of cyber violence is violence between people who know each other in the offline world. For example, this can be school bullying, which takes place online as well as in school. Bullying is a widely used term that refers to different types of injustice. However, in a narrower sense, it must be long-term and systematic violence against a particular person. In the Czech education system, bullying is a frequent and much feared phenomenon, and schools must have specific crisis plans in place to deal with it, which they follow when investigating and dealing with school bullying. However, they rarely know how to deal with bullying that takes place online. But it can have a very intense impact on classroom dynamics. A typical manifestation of this is, for example, the setting up of a WhatsApp group in which almost the entire class will be present, except for one or a few children who are ostracized in this way.

Similar acts of bullying can occur in universities or work teams. However, unlike school bullying, bullying affecting children and young people in these settings often lacks the necessary procedures to prevent, detect and address bullying.

Manifestations of cyberbullying

ostracism	Ostracization, or the exclusion of an individual from the collective, or partial or complete ignoring of the individual. In the online space, it can manifest itself as the exclusion of an individual from group communication, e.g. from a group chat room or social media groups.
blackmailing	Forcing someone to take an action, usually through the threat of disclosure of sensitive or personal information, photographs or videos (see also sextortion, revenge porn, forcible outing). This is a legally punishable act.
doxxing and sextortion	Doxxing is an abuse tactic often employed in blackmailing. It means publishing someone's information online without their permission, e.g. phone number, address but also sexual orientation or gender

	identity - see forcible outing.
sextortion	The term sextortion is a combination of the words sex + extortion and refers to extortion in which intimate materials (photos, videos) are used. Sextortion can be targeted at a specific person (e.g. singled out on social networks), but it can also take the form of email spam (i.e. it is not targeted at a specific person but is distributed en masse).
forcible outing	Disclosing or revealing someone's sexual orientation or gender identity against their will or without their permission. It threatens the psychological well-being and often physical safety of the individual and can become the subject of blackmail and lead to suicidal behaviour.
flaming	Flaming is an example of hostile online behavior used to undermine an opinion or break up a discussion through hateful, pejorative, insulting language. As opposed to trolling, flaming resigns on even a pretense of discussion - it only consists of escalating verbal aggression.
(gender-)trolling	Gender trolling is a strategy used to silence, undermine, belittle, and humiliate (usually) women online through employment of pseudo arguments, gender-based insults and threats (e.g., rape threats, death threats). It can result in women resigning on their presence in public and online spaces.
hate mail	Abusive, hateful, or threatening messages that are sent to an individual via email. Individuals sending hate mail often do so anonymously, as they are trying to avoid possible criminal prosecution arising from certain hateful content.
deepfakes	Deepfakes is a term for visual or audiovisual content edited or created by artificial intelligence that deliberately edits, distorts, or falsifies statements or recordings of specific individuals. Deepfakes are known from cases involving the falsification of statements by politicians but are most often used as a tool of cyber-violence: they can be used for blackmail, revenge porn, non-consensual creation and dissemination of pornographic or violent content. In 2018, a study by Sensity AI found that up to 95% of deepfakes are non-consensual pornographic content, 90% of whose victims are women. The potential for next-generation AI to create highly realistic and often difficult to detect deepfakes is a major threat at the moment.

2.1.3. Limiting freedom through technology

Technology can also be misused to restrict freedom. Dangerous pursuit, i.e. **stalking**, can be classified as a criminal offense. However, few people know that stalking that takes place in an online environment is also considered stalking. Behavior in which the aggressor misuses technology to track down his victim and then threaten him/her in the physical world is assessed as particularly dangerous.

But technology also amplifies **domestic or partner violence** - our phones and social networks can become tools of control and blackmail. A separate discipline is the abuse of the so-called **Internet of Things (IoT)**. Violence through IoT includes, for example, lowering the temperature in the home through remote control of the heating, spying on people in the home through home cameras, or even turning on doorbells or lights. Such behavior often includes **gaslighting**, one of the manipulation techniques. An extreme example of this phenomenon is locking victims inside or outside the home and blocking their freedom of movement through remote-controlled 'smart' locks.

Technology also allows **exaggerated and disproportionated control** over how much money someone spends and on what, who meets whom, who writes to whom, where they are, etc. This in itself can be an advantage and make partner life easier, but it is very easy to use these devices for blackmail and manipulation, especially if the respective people share all their passwords with each other.

2.1.4. Xenophobia, radicalism, insults on the basis of belonging to a minority group

The categories that often become criminal **offenses** are xenophobically motivated insults, **hate speech and hate crime** on the basis of belonging to a minority group. It is important not to turn a blind eye to the manifestations of xenophobia in the online space, because social networks in particular have a great deal of power to encourage the radicalisation of people through the validation of their opinions by means of algorithms which, in simple terms, show us what we want to see and enclose us in so-called **echo chambers** in which self-fulfilling prophecies are confirmed.

Manifestations of violence against minority groups

hate crime	Hate crime refers to criminal acts against a person, group of persons, property, or organization based on their real or perceived identity that motivates hateful behavior in the perpetrator. The degree of protection afforded to different groups of people on the basis of their identity varies slightly across the EU. Groups of
------------	--

	persons can be defined according to various factors: race, nationality and ethnicity, religion, sexual orientation, gender identity, disability (physical or mental), age, social class etc. Hate speech on the Internet may constitute a criminal offense.
hate speech	Hate speech is a specific form of hate crime that manifests itself in hateful messages, posts, comments, trolling, etc. in the online space. An important aspect is the possibility of rapid and mass dissemination and, in some cases, the difficulty of identifying the perpetrator.
sexism	Sexism is the belief in the inferiority of a gender; however, it is most often directed at women. In the online environment, it manifests itself in various forms of sexualised violence, discrimination, exclusion, persecution, hatred, etc., leading to the exclusion of women from public space.
fatshaming	Fatshaming consists of various forms of online violence with the goal of making someone feel embarrassed or ashamed about being fat by publicly criticizing or drawing attention to a person. Fatshaming can take various forms from seemingly well-meant advice behind health concerns to open insults and degrading language. This type of online violence is more prevalent towards women in many different environments and is often used to undermine public figures.
LGBTQ+ hate	Online hate and violence based on an individual's sexual orientation or gender identity. It can take a wide range of forms using social media, the common denominator (whether excuse or target) of which is orientation or gender identity. ILGA Europe has identified 2022 as the year with the strongest wave of hate against LGBTQ+ people in the last 10 years. Hatespeech and other forms of cyber-violence have been increasingly directed at trans* people, including public statements by political representatives. Manifestations of violence in cyberspace, as with intimate partner violence for example, are interconnected with the offline world - here too we have seen a recent rise in hate violence against LGBTQ+ people. All forms of violence have been on the rise, particularly around Pride events.

How to address xenophobic violence

We have several tools to deal with online xenophobia (for more detailed information on online protective tools, see Chapter 6; for country-specific legal guidance see

Chapter 9). We can choose from them based on the danger of a particular situation, but also based on our own capacities and our own safety. We can either ignore online xenophobia, hide it, report it to the company that runs the app, or we can file a criminal complaint with the police. The police should definitely be involved in dealing with cases of direct incitement to violence or killing - for example, if someone is planning an act of violence online and encouraging other people to participate. On the other hand, it is currently not possible for most people to report all acts of xenophobia to the police because there are too many of them. We can therefore use the possibility of reporting specific posts or profiles on social networks directly to their operators. The platforms are obliged to delete xenophobic and violent posts and block the profiles of those who violate the rules of the platforms in this way.

In cases where we encounter xenophobic speech online - especially if we ourselves are part of the group against which the violence is being perpetrated - we must think first and foremost about our own safety and wellbeing. It is perfectly okay and desirable to leave places where we do not feel comfortable. Does it annoy you that people write xenophobic comments on a news website? Stop following that site. You can also just block specific people whose posts and comments make you uncomfortable. Create an environment on social media that meets your needs and supports your wellbeing.

2.1.5. Toxic communities

Online communities can be a source of significant support for their membership; for example, for LGBTQ+ people they can often be one of the few places where they can authentically express their orientation or gender identity and network within the community. However, **online communities can also be highly toxic environments** in which members encourage each other to hate certain groups of people and to behave dangerously towards others or themselves. As with other forms of cyberviolence, toxic communities can escalate violence from online manifestations into the physical world.

For example, there may be sexist, misogynistic communities (typically **Red Pill**³, **incels**⁴), whose members support each other in hateful behavior towards women (and often LGBTQ+ people), which can extend to the offline space in the form of verbal

³ Red Pill or Redpillers refer to the red pill from The Matrix movie, which made the main character see the world as it really is. The so-called Redpillers consider themselves to have seen through the system and discovered the true nature of the world, which they believe is dominated by women.

⁴ Incel (= involuntary celibate) is a person (usually a man) who regards himself or herself as being involuntarily celibate and typically expresses extreme resentment and hostility toward those who are sexually active. Source: <https://www.merriam-webster.com/dictionary/incel>

or physical violence, stalking, and in extreme cases, extremist acts. Members of these communities are overwhelmingly male, emphasising stereotypical and heteronormative gender roles, considering sexual intercourse a male right and thus promoting rape culture.

Pro-ana groups (before the proliferation of social networking, it was mostly pro-ana blogs), on the other hand, are an example of groups that are dangerous to their own membership. Pro-ana groups glorify anorexia and other eating disorders as a way to be as thin as possible, regardless of the health and psychological consequences. The members counsel each other not only on how to most effectively lose weight and starve themselves, but also on how best to hide it. These groups are predominantly girls and women - this is consistent with the gender composition of eating disorders sufferers (globally⁵ 5,5–17,9 % of young women and 0,6–2,4 % men; people with a minority gender identity or sexual orientation were more at risk of eating disorders).

How to recognize a toxic community?

Toxic online communities are often indistinguishable at first sight from supportive communities. They are also supportive in nature, but unfortunately, they encourage their members to engage in risky behavior. But there are a few signals that should tell us that all may not be well with the community, and we should beware.

Toxic communities are very **closed**, and it is difficult and often almost impossible to leave them. For example, if someone decides to leave a whatsapp group that supports unhealthy weight loss, they may be rejoined by another person after a while. Toxic communities are often shrouded in **secrecy** - they make their members feel that they are not allowed to tell anyone about what is going on in the community. Toxic communities are **isolated** and encourage **refusal** of professional help. Examples include communities that promote self-harming, where the perception is that psychological care will only harm the person, etc.

2.2. Best practices

2.2.1. Manual for experts who work with youth, research report (Slovenia)

This manual explains different types of violence focusing on gender-based cyber-violence. It explains the phenomena and roles of those included in that type of

⁵ <https://pubmed.ncbi.nlm.nih.gov/36125216/>

violence and gives advice on how to provide support to youth that experience gender-based cyber-violence. Research reports the collected data. <https://www.gov.si/assets/ministrstva/MDDSZ/Enake-moznosti/OdklikniPrirocnikMladina.pdf> and https://odklikni.enakostspolov.si/wp-content/uploads/2020/02/Odklikni_POROCILO_A4_12_2020web.pdf

2.2.2. Staying Safe Online: Gender and Safety on the Internet: Experiences of Young Women and Men in Cyprus

The overall project aim is the collection of gender-related data, involving both quantitative and qualitative analysis, and awareness raising about the role of gender in cyber-related-abuse (sexual harassment, stalking, cyber-bullying among other) associated to the use of the internet and new communication technologies by young people, particularly social networking websites. Available at: https://medinstgenderstudies.org/wp-content/uploads/INTERNET-SAFETY-RESEARCH-Full-Report_Combined-FINAL.pdf

2.2.3. The Warriors against GBV project

The project was created to train and empower youth workers by providing them with innovative methods of working with young people who are victims of gender-based violence. You can find inside options for creating safe spaces, a methodology for holding safe spaces online and offline, as well as stories of survivors – warriors – of GBV. See <https://warriors-gbv.eu/#/en>

2.3. Conclusion

Gender-based cyber violence can take many forms and manifestations. It is important to learn how to recognise them so that we can address and, more importantly, prevent them. It is crucial not to underestimate the impact of violence that happens in the online space. It is no less real than the violence that takes place in the offline world, and although it often does not hurt physically, it does not diminish the mental pain it causes. Society is only just learning to seek out and punish online violence. But the fact that it sometimes fails to do so quickly and consistently enough should not be a reason to neglect our vigilance against cyber violence. On the contrary. It is important to build empathy in the online world, to name acts of cyber violence and to learn mutual respect.

2.4. Exercises

Activity 1: Role-Playing Scenarios

Objective: To understand different forms of gender-based cyber violence through interactive role-playing.

Target Group: Youth and young adults aged 12-30.

Group Size: Up to 10 participants per session.

Duration: Approximately 60 minutes.

Materials Needed:

- Scenario cards for the youth worker (provided at the [annex](#) below). These can be printed once and re-used
- Timer. A phone would suffice
- Note-taking materials (optional).

Process:

1. **Introduction (10 minutes):**
 - Begin by explaining the purpose of the activity: to understand and recognize various forms of cyber GBV.
 - Emphasize the importance of a respectful and sensitive approach to the scenarios, acknowledging the potential emotional impact of the topics.
 - Briefly explain what cyber GBV is and its different forms.
2. **Formation of Groups (5 minutes):**
 - Divide participants into small groups of 2-3 people.
 - Ensure each group feels comfortable with their team members.
3. **Distribution of Scenarios (5 minutes):**
 - Hand out a different scenario card to each group.
 - Explain that each scenario represents a form of cyber GBV: cyber grooming, sexting, online harassment, and a fourth type which will be revealed through the scenario.
4. **Role-Playing and Discussion (30 minutes):**
 - Instruct each group to read their scenario and decide how they want to role-play it. One or two members should enact the scenario, while the others observe.
 - After the role-play, the observing members will initiate a discussion within their group, guided by the following questions:
 - What form of cyber GBV was depicted?
 - How might the victim feel in this situation?

- What could be the short-term and long-term impacts of such an incident?
 - How could the victim seek help or support?
 - What preventive measures could be taken to avoid such situations?
 - Allow each group 10 minutes for the role-play and discussion.
- 5. Group Sharing and Debriefing (10 minutes):**
- Invite each group to share their scenario and the insights from their discussion with the entire group.
 - Facilitate a group discussion, focusing on the different perspectives and solutions offered.
 - Conclude with a debriefing, emphasizing key learnings and reminding everyone of the resources available for those who might be affected by cyber GBV.

Activity 2: Cyber GBV Impact and Storytelling

Objective: To explore the impacts of cyber GBV and develop empathetic and effective response strategies.

Target Group: Youth and young adults aged 15-30.

Group Size: Up to 10 participants per session.

Duration: Approximately 90 minutes.

Materials Needed:

- Story prompts describing different cyber GBV scenarios (ensuring sensitivity and appropriateness). - Prompts provided in the [Annex](#)
- Flip chart or whiteboard and markers.
- Note cards and pens for participants.
- Comfortable seating arrangement for open discussion.

Procedure:

- 1. Introduction to Cyber GBV Impacts (15 minutes):**
 - Begin with a brief overview of the various forms of cyber GBV and their potential emotional, psychological, and social impacts. If possible, try to address also the physical aspects that Gender Based Violence can sometimes have on a person because of the trauma produced and endured.

- Emphasize the importance of understanding these impacts to respond effectively and empathetically.
- 2. Story Prompt Discussion (20 minutes):**
 - Distribute different story prompts to small groups (2-3 participants per group). Each story should describe a scenario involving a form of cyber GBV.
 - Ask groups to read their stories and discuss the potential impacts on the victim, their friends, family, and broader community. *Note for facilitator, draw 4 circles each one increasing in size starting with the victim in the middle and the expanding to the friends and then to community members.*
- 3. Developing Response Strategies (30 minutes):**
 - Instruct each group to brainstorm and note down possible response strategies for the victim and their support network. These strategies should focus on both immediate and long-term support. *Note for facilitator, draw a table with two columns. One for immediate and the other one for long-term support.*
 - Encourage creative and empathetic thinking, considering emotional support, practical advice, and referral to professional services.
- 4. Forum Discussion (20 minutes):**
 - Bring the groups together in a circle for an open forum discussion.
 - Each group presents their story and proposed response strategies, followed by a broader discussion, allowing others to add insights or alternative strategies.
- 5. Reflection and Personal Commitment (15 minutes):**
 - Conclude with a reflective session where participants consider how they can apply what they've learned in their own lives or communities.
 - Encourage participants to write a personal commitment on a note card regarding how they will contribute to addressing cyber GBV.

Debriefing and Conclusion:

- Summarize the key takeaways, emphasizing the role of empathy and informed response in addressing cyber GBV.
- Remind participants of the importance of seeking professional help when needed and the availability of resources for support. It would be great to provide or promote some local organizations that work on this topic.

Safety and Sensitivity Measures:

- Monitor the discussions to ensure they remain respectful and supportive.
- Be prepared to intervene if the discussion becomes distressing for any participant.

- Provide a safe space for participants to express their feelings and thoughts without judgment.

3. Prevention of cyber GBV

Objectives

- To understand the foundational principles of prevention and their application in the digital context.
- To highlight the impact of educational initiatives on preventing cyber GBV.
- To explore the roles of different sectors in a collaborative prevention effort.
- To understand how to empower users with the knowledge and tools to protect themselves and others online.

3.1. Theory

3.1.1. Principles of prevention

Prevention encompasses actions aimed at **eliminating or reducing** risks and threats to well-being. In the area of violence prevention, the emphasis is on reducing the risks related to violence, postponing the occurrence of violence or completely eliminating it. There are several approaches to the classification of preventive activities (Porta, 2018). It is classically divided into **primary, secondary and tertiary levels** of prevention while Gordon's (1983) classification of prevention levels distinguishes between **universal, selective and indicated prevention**.

Primary prevention includes interventions that are undertaken before any cyber gender-based occurrence violence (CGBV), thus reducing the overall prevalence of CGBV. At this level of prevention, it is necessary to determine which characteristics of the individual and their environment lead to the appearance of violence, and to act on them in order to prevent violent behavior from manifesting itself (Harvey et al., 2007). For example Wirawan et al. (2022) found that anxiety and prior experiencing CGBV predicted committing CGBV in young adults. Taking this into account, primary prevention would be focused specifically on reducing anxiety and reducing effects of experiencing CGBV to eliminate the likelihood that the participants of these preventive activities will later commit GBVV. The Association for Progressive Communication indicates that three groups of people most often experienced CGBV - people in intimate relationships, the public figures, and those who have prior experience of gender-based violence and CGBV. Being female is also an important risk for experiencing CGBV - although men report that they experience more online violence, it is women who experience more online harassment based on their gender (Vogels, 2021). Thus, primary prevention activities would be directed precisely at these groups of people. However, today there are a lot of primary prevention approaches that include raising awareness of young men because it is recognized that

CGBV is a problem based on gender inequality and therefore it is important that, in addition to girls and others who are more likely to experience CGBV, like members of LGBTIQ+ community, preventive activities are directed at young men, as a group more likely to commit CGBV. The idea is that by encouraging attitudes that are supportive of gender equality, the occurrence of violent behavior will be prevented, that is, that supporting a gender-respecting way of thinking will be transferred to behavior as well.

Secondary prevention refers to interventions that are undertaken after the occurrence of violence, but before it becomes chronic. The main purpose is to reduce the long-term consequences of violence (Graffunder et al., 2004). Secondary prevention in terms of its function and implementation overlaps with early detection and recognition of CGBV. Therefore, it is crucial that everyone, not only those who are involved in CGBV either by committing it or experiencing it, know how to recognize the signs of CGBV. Familiarizing bystanders and all stakeholders with behaviors that are typical for CGBV (see the second chapter) or knowing the psychological reactions of people who experience CGBV (e.g. emotional distress, anxiety, or fear, withdrawal from the use of digital technologies) can make it easier for bystanders to recognize whom they need to support. In addition, it is important to teach both those who experienced CGBV and the bystanders how to respond appropriately (eg report CGBV or provide or request support).

Tertiary prevention refers to the reduction of the long-term consequences of CGBV or to the treatment activities undertaken for perpetrators of CGBV. Tertiary prevention activities include crisis care, advocacy and counseling aimed at victims, but also legal reactions and involvement in the treatment of perpetrators. It is crucial that these activities are coordinated in order to prevent further CGBV and revictimization (Crooks et al., 2007).

Gordon's (1983) classification of prevention activities is based on the filter principle, that is, on the level of coverage of the population to which the activities are directed. The broadest level of prevention is **universal**. It includes activities offered to the entire population. Unlike primary prevention, there is no need to identify risk factors, but activities are offered to everyone. There is a risk that the activities are not adapted to people who already have experience with CGBV and that they are demotivated to participate in further preventive activities. Targeting those who are at high risk of involvement in CGBV is a feature of **selective prevention**, and it is important for us to know the risk and protective factors (as in primary prevention). **Indicated prevention** focuses on those who are already committed or who have experienced CGBV and thus is aligned with the features of secondary prevention. In the context of Gordon's classification, the level of tertiary prevention is observed through treatment rather than interventional preventive procedures.

Comparison of classification of prevention activities

Public health classification		Gordon's classification	
Levels	Definition - amount of risk	Levels	Amount of population covered
Primordial prevention	Prevention of development of risk factors	Universal prevention	Prevention activities aimed at the whole population
Primary prevention	Prevention of occurrence of CGBV when risk factors are present	Selective prevention	Prevention activities aimed at selected subgroups with higher risk for CGBV
Secondary prevention	Prevention of aggravation of CGBV after first incidents	Indicated prevention	Preventive activities aimed at those included in some CGBV incidents
Tertiary prevention	Activities after multiple CGBV incidents to prevent further occurrences, minimize the consequences and impact of previous CGBV incidents	Treatment	Activities aimed on those victimized by CGBV or chronic perpetrators of CGBV

Kafonek & Richards (2017) have, for the area of gender-based violence (GBV), highlighted the key features of successful preventive strategies at the university level. They indicate that these programs should be comprehensive in order to prevent different forms of GBV, should be based on a clearly defined theory (often the Bronfenbrenner's socioecological model or some adaptation of that model is used) and encourage positive interpersonal relationships (e.g., programs based on inclusion bystander in providing support to peers experiencing violence). They also point out that they should be socio-culturally relevant (for example, consider that Roma women will be more exposed to CGBV than other women living in Europe). They recommend that a variety of methods should be used in the program, i.e. that different experts, such as youth workers or lawyers who work with victims should be special guests, but also other approaches such as psychodrama should be included. They indicate the need to determine the optimal duration of the program, emphasizing the importance of booster sessions (booster session that will be organized after the end of the continuous program - for example after six months, in order to preserve the skills and knowledge acquired in the program), as well as the so-called ongoing programs that use passive methods such as posters or flyers that are constantly

available. For the success of the program, it is important that they have well-trained implementers, as well as a good evaluation.

The principles of universal and primary prevention, which raise the awareness of those not yet involved in CGBV, clearly indicate the importance of a **proactive approach**. If the involvement of an individual in CGBV is prevented, all undesirable consequences are completely prevented (e.g., the withdrawal of women from the digital world, which increases the digital gap, the appearance of unpleasant emotions, and even impairment of the mental health of people who experience CGBV). This reduces not only the suffering of the individual, but also the costs for society that arise from the consequences of involvement in CGBV, which exist in a reactive approach. For proactivity, it is crucial that all stakeholders think clearly in advance about their options for action and foresee possible challenges. For example, at work or at school/university, co-workers may notice that a young person is a victim of CGBV, but if there is no clear guideline, and even an obligation, to provide support, they may consider that it is the victim's private matter, that it is not theirs to mix. In Croatia, Ministry of Family, Veterans and Intergenerational Solidarity (2004) has declared a Protocol on procedure in the case violence among children and young people. In that document is clearly described what school, police and centers for social care are obligated to do (step by step) if violence occurs, including sexual harassment and online violence. Everyone working in school, police and social welfare are obligated to follow that protocol, and some employees who did not obey, have faced dismissal due to violation of work duties. Governmental Office for Gender Equality of the Republic of Croatia declared Protocol on procedure in the case of sexual violence (<https://ravnopravnost.gov.hr/UserDocsImages/dokumenti/Protokol%20final.pdf>). That protocol includes sexual violence conducted via digital technology as a form of sexual violence and describes steps that various institutions are obligated to follow in cases of sexual violence.

The proactive approach is based on setting clear norms on how to react before violence occurs, while the **reactive approach** implies that stakeholders only react, that is, even when signs of violence are observed, a formal report is awaited from the person who experienced the violence. With GBV, including CGBV, a big challenge is that it is not reported or is very rarely reported (Violence, WIGB, 1999). Therefore, only with a proactive approach can we ensure that even those victims who are not ready or are not aware of how to take legal steps receive appropriate help. The importance of a proactive approach is recognized at Victim's rights directive (Directive 2012/29/EU) in which it is emphasized that victims of gender-based violence are more often women and that they are in a particularly difficult position if they experience violence within intimate relationships and from the perpetrator on whom they are materially dependent. Therefore, in this directive, while considering the diversity of the legislation of EU member states, it emphasizes the importance of **providing the victim with all information in an understandable way**, and

checking whether the victim has fully understood all aspects of the legal actions taken. Brody (2020) points to another type of reactivity in the activities that take place in the class, and within the framework of LGBTIQ+ topics, while looking at the selection of preventive activities that are often directed according to the current situation in the class - for example, if a student has gay parents, the topic of life with gay parents will be discussed, while if in the class is transgender student, activities such as hosting a transgender person will be chosen. Although both types of activities are chosen with the aim of prevention, at the same time they focus all attention on a particular student. The same type of reactivity is also found in situations when it is known that someone experienced CGBV in the class, so only then do universal CGBV prevention activities begin. If the case is known in the class, it can lead to additional victimization of the student who experienced violence through working through similar examples in universal prevention activities. Therefore, it is important that preventive activities are truly proactively included according to the principles of primary and universal prevention for all young people, systematically and before young people become involved in CGBV. Brody (2020) indicates that teachers often find themselves in a situation where they do not have adequate materials, i.e. lack of evaluated programs, and thus emphasizes the importance of a systematic and comprehensive approach to the topic as well as the education of teachers.

The previously mentioned examples of preventive activities that focus the attention of all participants in a potentially negative way on one student indicate the importance of ethical behavior. Namely, as CGBV refers to the behavior that takes place on SNS and in the digital world, part of that behavior takes place within the framework of direct communication (e.g., via direct messages on Instagram) which are not readily available to others. Although it is important to prevent CGBV, the optimal level of respect for privacy should be considered. It may seem like a good idea to directly monitor the communication that young people have in order to protect them from cyber- violence, including CGBV, by doing so we are doing multiple damage. We violate the privacy of young people, but, at the same time, we don't show them trust and thereby reduce the development of taking responsibility for their own behavior in the digital world. Also, young people often say that they avoid confiding in their parents when they experience cyber- violence, because parents often react by demanding that their children refrain from using digital technologies. As a result, these children and youth are punished multiple times, while not doing anything wrong - they are prevented from participating in various activities in which their peers participate, and after experiencing violence and thus emotional injury, they are additionally punished, and a sense of guilt is implied for them because they experienced violence. Since, in addition to girls, young people who are members of the LGBTIQ+ community are disproportionately more exposed to CGBV, an additional ethical challenge in respecting privacy is present. Members of the LGBTIQ+ community, particularly in under-inclusive societies, may be particularly

affected by such invasions of privacy, especially if they are unwilling to share their LGBTIQA+ identity with others. Such interventions, instead of being preventive in nature, can be frightening for them.

3.1.2. The role of education & educational activities in prevention

In the context of sexual violence on campuses, Flanery (2023) points to an important shift from a reactive secondary prevention approach where activities are focused on providing support to those who have experienced sexual violence to primary and universal prevention activities such as awareness campaigns and interventions based on bystanders

The goal of awareness campaigns is to **spread awareness of the existence of CGBV**, its characteristics and forms, and by increasing knowledge and promoting attitudes against CGBV, ensure that individuals do not commit behaviors that are CGBV, that society as a whole becomes sensitized and acts on potential perpetrators so that they do not engage in CGBV as well as ensuring a sufficient amount of knowledge to all those who encounter violence as persons who experience it or as bystanders to know how to recognize and react to it. Campaigns rely on **key messages** that are transmitted through different channels to the target audience. Some common forms of awareness campaigns are public service campaigns, social media awareness drives, or educational workshops. AIContentfy team (2023) describing key strategies begin with key audiences. They recommend that stakeholders should be identified in such a way as to analyze who can have a direct or indirect influence on the program itself - their inclusion can increase the impact of the campaign, and taking their perspective can be crucial when tailoring the messages addressed to them. It is important to know their socio-demographic characteristics such as sex, gender, age, but also their attitudes, behaviors and interests.

AIContentfy team (2023) indicates that for the success of the campaign we need to set **clear goals** that are specific and measurable, such as increasing knowledge or changing behavior⁶. In order to be able to evaluate the success of the campaign, it is necessary to clearly define this goal in advance through fully measurable outcomes (e.g., if our goal is to increase awareness of a topic, the outcome will be, for example, 5,000 reactions - views, downloads, likes - on the campaign's SNS). One of the important recommendations is the use of different media, both traditional (print media, television and radio) that suggest a dose of seriousness, especially when the message needs to be conveyed to different generations, including those we call digital immigrants (e.g. teachers who belong to generation X who need to be made aware about the challenges of CGBV experienced by their Z generation students), as well as

⁶ How to make SMART goals could be find on <https://www.mindtools.com/a4wo118/smart-goals>

SNS and influencers that will be more acceptable to young people. For a successful campaign, it is also important to cooperate with partners who will contribute different expertise, but also increase resources and ensure that the campaign reaches as wide an audience as possible. Already during campaign planning, by setting measurable goals and outcomes, it is defined how the campaign will be evaluated. Namely, the evaluation should logically follow from the set outcome - if we expect to increase the knowledge about the features of CGBV by 20% among the target group, we will apply some form of knowledge test before and after the implementation of the campaign and monitor whether the goal has been achieved. If we expect that after the campaign, 50% more high school students will know that CGBV exists through this campaign, we will check how many young people knew about this phenomenon before the campaign, and how many heard about it through the campaign and compare the numbers. When designing campaigns, it is useful to learn from examples of successful campaigns (for example, to see how important it is to use attractive visuals), but also from examples of unsuccessful campaigns (so that we know what to avoid - such as overly complex language).

Fisher et al. (2010) in their manual provide clear instructions on how to **plan workshops and programs** aimed at preventing gender-based violence. Firstly, it is important to determine the **needs and problems** on which we want to focus the training , and to know the **goals and short-term, medium-term and long-term outcomes**, which should include five elements (who is the target group, what we want to change about them, how much change we expect and in what time frame, and how the change will be measured). Also, program authors should identify **possible participants** of the program, and ask several potential participants to participate in the planning of activities in order to **get their perspective**, determine **the main topics** that the program will deal with, take into account the **organizational possibilities and individual readiness** to participate, plan the necessary **resources** and choose **trainers**. After the planning phase, it is important to **adapt the program** considering the characteristics of the participants (e.g., young people will benefit more from programs in which they are active and create something through projects, for example, a TikTok video that will instruct bystanders how to react when they notice someone experiencing CGBV). It is also necessary to plan how to conduct **process and outcome evaluation**. In process evaluation, we can use adapted questions recommended by Fisher et al . (2010, p. 41):

"What organizational characteristics, identified in your initial assessments, were addressed in your training? What characteristics of the individual participants, identified in your initial assessments, were addressed in your training? What was the participants' satisfaction with the training? What was the staff's perception of the training? What amount of content (i.e., dosage) did the participants receive? Did the training follow the basic plan for delivery?"

For early recognition of CGBV it is important to rely on technology companies and social media platforms, as well as turning to institutions that provide legal support in CGBV cases, and their role will be considered below.

3.1.3. Multi- sectoral approach to preventing cyber gender-based violence

Although technology companies and social media platforms are crucial because without them CGBV can hardly take place, there are challenges in their more active involvement in preventing such behaviors. Namely, as Suzor et al. (2019) emphasize, despite offering their services all over the world, most of these companies have their headquarters in the USA. American legislation does not sufficiently regulate the obligation of these companies to act in cases of CGBV. An additional challenge is the emphasis on freedom of speech, which, as Suzor et al. (2019) correctly conclude, is an excuse for inaction. These authors indicate that it would be important to communicate with these companies, but also the general public and legislators in order to encourage everyone that CGBV should be viewed in the context of gender inequality. Namely, the lack of reaction under the pretext of freedom of speech can encourage victims of CGBV (who are more often women) not to use the services of these companies to protect themselves from experiencing CGBV on them, and as a result, to expand the digital gap. As digital inclusion is today a prerequisite for the realization of educational and work potentials, as well as the overall quality of life, such an avoidance strategy will consequently lead to increasing general inequalities to the detriment of victims of CGBV. Ceia et al. (2021) indicate that data management is particularly important for women who are more often exposed to CGBV, which includes doxing and revenge porn, but also stalking because the posts often include information about the daily routines of users. Although these aspects can be acted upon by raising the user's awareness of the ways of use and ensuring privacy, the responsibility of technology companies is also manifested in the fact that they participate in the development of applications that enable, for example, locating women in the vicinity without the knowledge of these women. Nevertheless, the public calling out of one such application (Girls around me) some ten years ago led to the fact that the company that developed that application withdrew it from the offer through the app stores. Therefore, it is extremely important to stimulate a public debate, and in that way, to stimulate technology companies and social media platforms to develop and actively and timely use different mechanisms for the prevention of CGBV.

Fernandes et al. (2021) indicated in the report of the European Parliament that numerous technology companies and social media platforms rely on AI and moderators, but that this is often not enough for a quick and efficient reaction. In their

report, they monitor the legal regulation of CGBV in EU countries and identify six basic challenges:

- Lack of a harmonized legal definition of gender-based cyber violence
- Lack of awareness of gender-based cyber violence across all stakeholders' groups
- Under-reporting of gender-based cyber violence
- Victim support and safeguarding challenges
- Limited research and knowledge on various aspects of the phenomenon
- Investigative challenges , including difficulties accessing records and working cross-border.

Despite the inconsistency of legal reactions in EU countries in cases of CGBV, legal experts and police officers are stakeholders with whom it is crucial to cooperate in order to provide adequate legal support to persons who experience CGBV. At the same time, it is important to raise the awareness of these legal experts about the nature of CGBV and the need to harmonize legal procedures in order to provide adequate support to victims. Fernandes et al. (2021) report describes when one blogger tried to report the case of CGBV experienced in 2014 to the police, she found out that the data from her report, including her personal data, would be publicly available. When it is known that doxing is one of the forms of CGBV, it is understandable that such exposure of the victim's data to the public does not contribute to her protection, but on the contrary makes it easier for the perpetrators to continue attacking her. Adding to her mistrust was the fact that the police officers were digitally illiterate and did not even know how to examine the evidence of CGBV that she had brought to them on a USB. This example shows how important it is to provide training for police officers and legal professionals in order to make them more sensitive to all CGBV challenges, but also to motivate them to actively advocate and demand changes in legal procedures to ensure the preservation of privacy and anonymity of victims and develop the necessary digital skills not only for a few specialized police officers, but also for those police officers who will be the first to respond. Awareness of the extent of under-reporting of CGBV indicates how crucial sensitive and educated legal experts and police officers are. For victims experiencing CGBV, it is important that NGOs proactively collaborate with legal professionals.

3.1.4. Empowering users

When we talk about empowering users in the prevention of CGBV, we focus on developing their digital literacy and digital skills, clarifying issues of consent and boundaries online and safe communication practices.

Digital literacy is understood as knowledge, while digital skills enable the appropriate use of technology in order to find, critically evaluate and/or use and transmit the

necessary information. However, they are not limited to the technical use of information, but also to the responsible use of digital technologies. Stauffer (2020) indicates that any curriculum that teaches digital skills should include areas of information literacy, ethical use of digital resources , understanding digital footprints , protecting yourself online, handling digital communication and cyberbullying .

Increasing information literacy starts with its clear definition, then it is recommended to use examples of trustworthy and non- trustworthy information to ensure recognition of the differences between them. This distinction should then be clearly stated in the guidelines that indicate the credibility of the information (it is stated who the author is, they have good credibility, the information is current and the very domain on which we find the information is credible, the page is well designed, the information is written grammatically and linguistically correctly). It is important to encourage critical thinking (teaching young people to value information by answering the questions: " Does someone or an organization benefit from this information? Does this information sound biased towards one side or another? Can you tell if the author has an opinion? Does the heading or headline match the information in the body? Does the information conflict with something the student knows to be true?", Hummel, 2022). Responsible use of information, which includes citing information found in paper as well as online editions, as a form of copyright compliance is a way to increase not only the responsibility of young people but also their digital skills.

It is important to develop the idea of digital footprints, that is, all the information about us that we passively leave or actively share. Young people will easily accept that personal information such as providing information about their education, residence or age is part of digital footprints , but they should be directed that the information found, for example, in a photo published by them or someone else about them, as well as technical data about the photo itself (time and place of its creation) are part of such a digital footprint and can be misused for CGBV. The awareness that everything is being shared, even based on the favorite browser we use or the data with which mobile phone we took a photo, is part of our digital footprint.

Basic digital skills include Internet safety - creating strong passwords, using privacy settings, and knowing what not to share on social media.

By using available examples of good practice, adapting these examples to your own cultural context as well as to the young people you work with, taking into account their perspective, you can empower them not only in the use of digital technologies, but also in self-protection and prevention of experiencing GBV.

3.2. Best practices

3.2.1. Undeclared - best practice of campaign for universal prevention of CGBV

In the PS CGBV project as an example of good practice is the campaign from Poland Undeclared (<https://www.youtube.com/watch?v=uZpiZ-e7E8c>) in which the video shows a young woman who resembles the scientific icon from Poland Marie Curie who posts on SNS about her work on experiments in the laboratory. Soon, she receives a lot of misogynistic comments that, for example, recommend that she return to the kitchen.

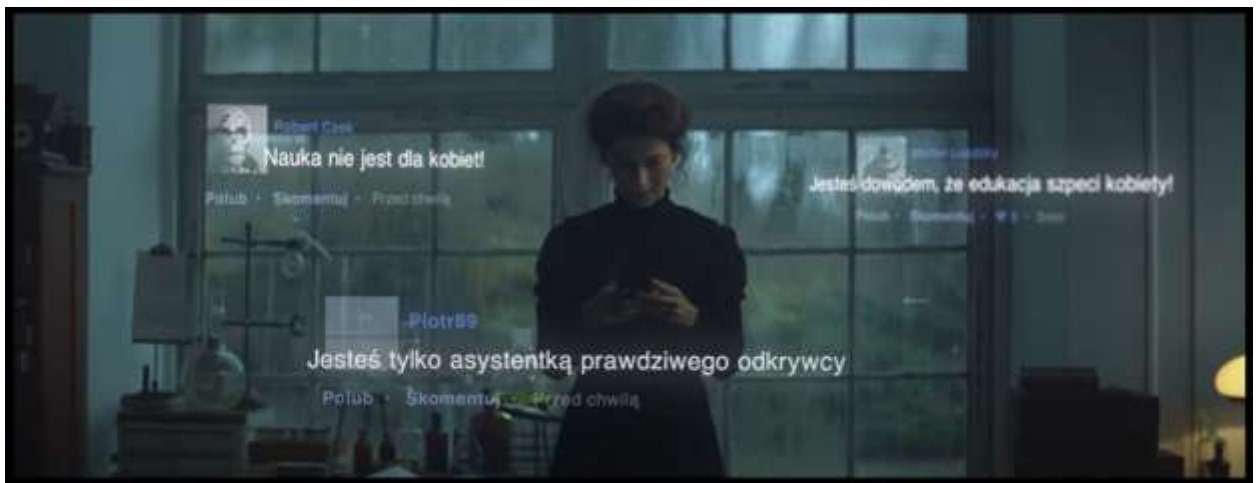


Image from video Undeclared - source <https://www.youtube.com/watch?v=uZpiZ-e7E8c>

Despite the discomfort she feels, she returns to her laboratory and announces that she is back in it on the same SNS. Now the laudatory comments follow, and the video ends with the moment when she is awarded the award and everyone applauds her. The viewer's attention will certainly be attracted by the discrepancy between the appearance of the laboratory, the environment and the clothes of the actress, which correspond to the beginning of the twentieth century on the one hand, and the publication on SNS on the other. The video is also very culturally sensitive because it uses a reminder of a globally popular scientist who changed gender stereotypes with her scientific work, and her background supports the viewers' national pride and facilitates identification. It shows her as a young woman who does not give up despite the obstacles and achieves the goal she set for herself, and in the end she experiences recognition for the same and is thus an inspiration. The model is how to ignore comments that are CGBV, continue your activities, but also use SNS, and show that you should focus on those comments that are supportive. This is an example of how to tailor a campaign to the specifics of your audience and communicate.

3.2.2. "I can say I won't!" - site with various material for universal prevention

Another example of a good campaign is the Croatian campaign "I can say I won't!" (<https://nechupedia.sezamweb.net/>) that has a comprehensive site with different text, video clips, game, magazine, and infographics for youth about CGBV and other important topics (quality in relationships, social support ...).



Image from site of "I can say I won't!" - source <https://nechupedia.sezamweb.net/>

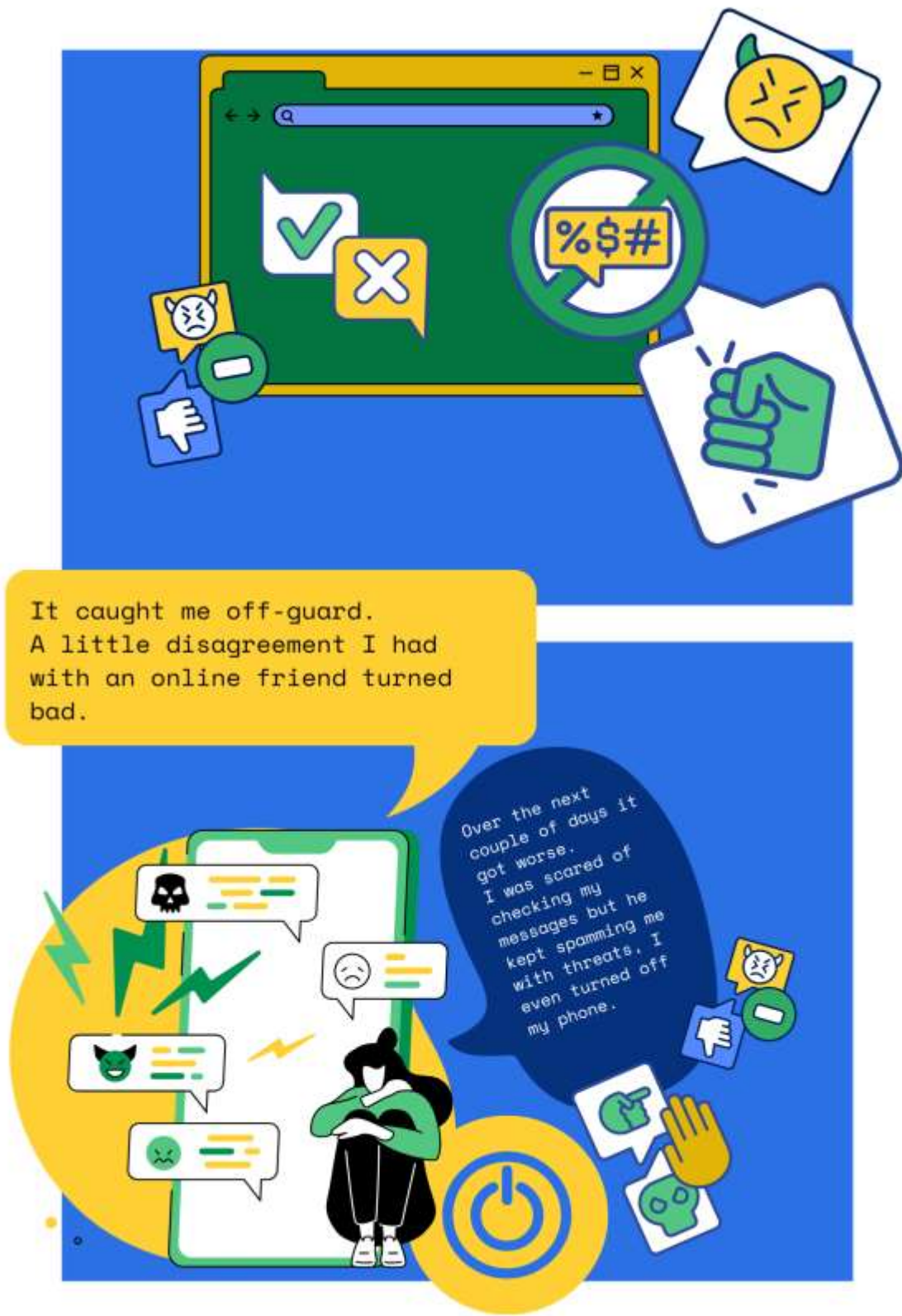
The mentioned campaign is part of a wider project that also includes a manual for teachers with four elaborated workshops (<https://api.ps-cgbv.eu/media/file/637d151844d4c.pdf>) that teachers can download and implement in their original form or adapt to their own style. It is commendable that for each workshop the goal, outcomes, expected duration, which is harmonized with the school hours, all instructions, and materials for each workshop are shown. In addition to the workshops themselves, the manual provides clear instructions on how to react when a teacher notices that a student has experienced CGBV (Cesar (Ed. 2021, p. 60):

- *"don't suggest to the victim to "turn off" the Internet and get away from social networks, because this does not stop the violence, and the victim could become even more isolated,*
- *ignore messages that are not important, that do not threaten and do not affect the reputation of the other person (most perpetrators expect a reaction and are ready to continue and increase the abuse and violence when they realize that they have achieved it) - instead*

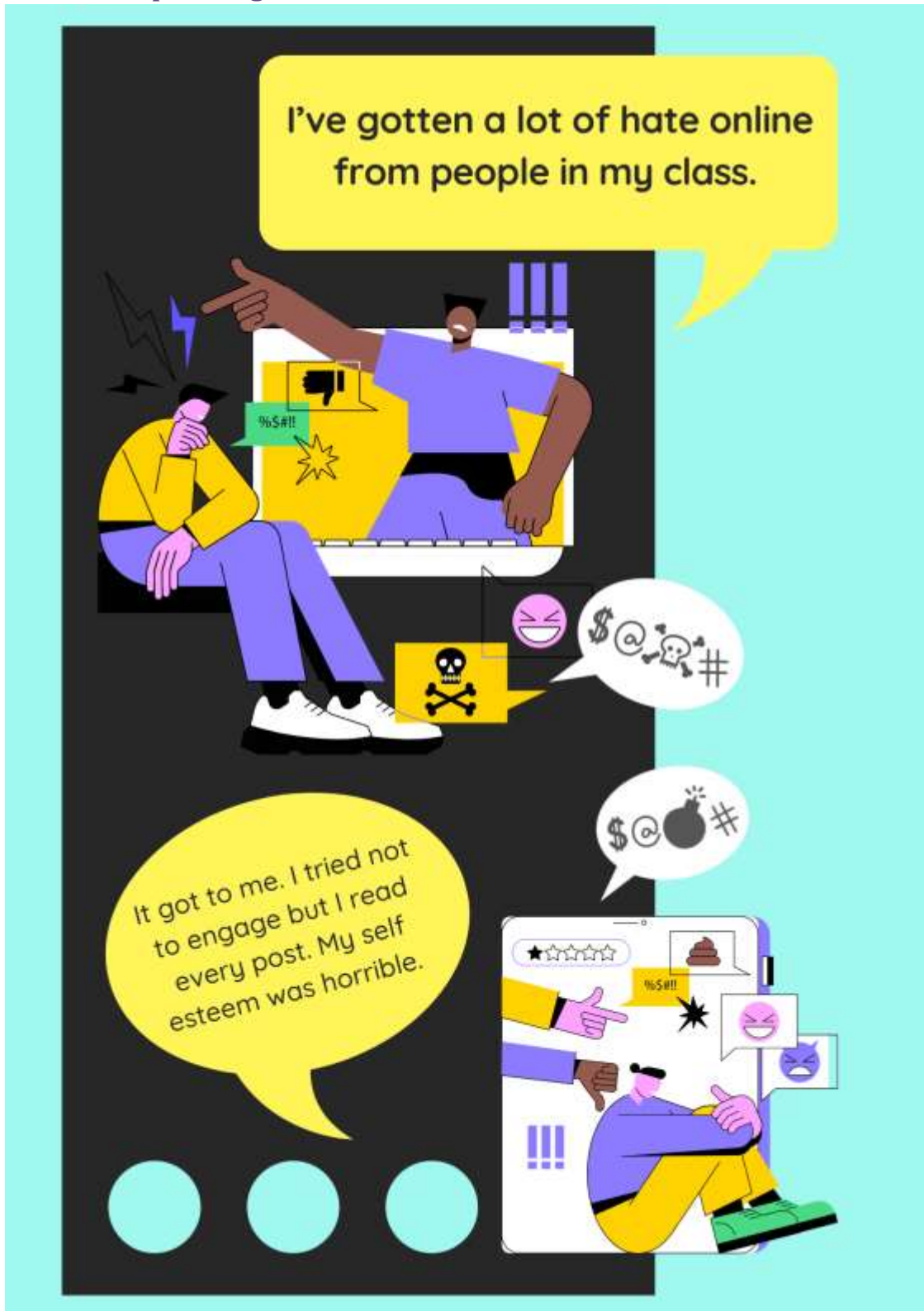
- *use the option to block individuals who send abusive messages (on various platforms such as Facebook, Instagram and Twitter),*
- *unfollow and distance yourself from problematic posts (Facebook) or photos (Facebook and Instagram), remove people with whom you do not feel safe and comfortable sharing content from your friends list,*
- *report content (Facebook and Instagram) that violates the rules and community guidelines (provide a clear description of where you found such content),*
- *collect evidence with screenshots and saved messages (it is important to have evidence of abuse to initiate legal proceedings),*
- *contact specialized organizations and associations dealing with digital rights and organizations for the protection of children's and women's rights for the purpose of information and support,*
- *report to responsible institutions - agencies in charge of combating high-tech crime in the police or special departments of the state attorney's office,*
- *remind children and young people not to share their passwords with anyone and that it is important to ask for help - if it is not possible to prevent violence, it is important to stop it as soon as possible. "*

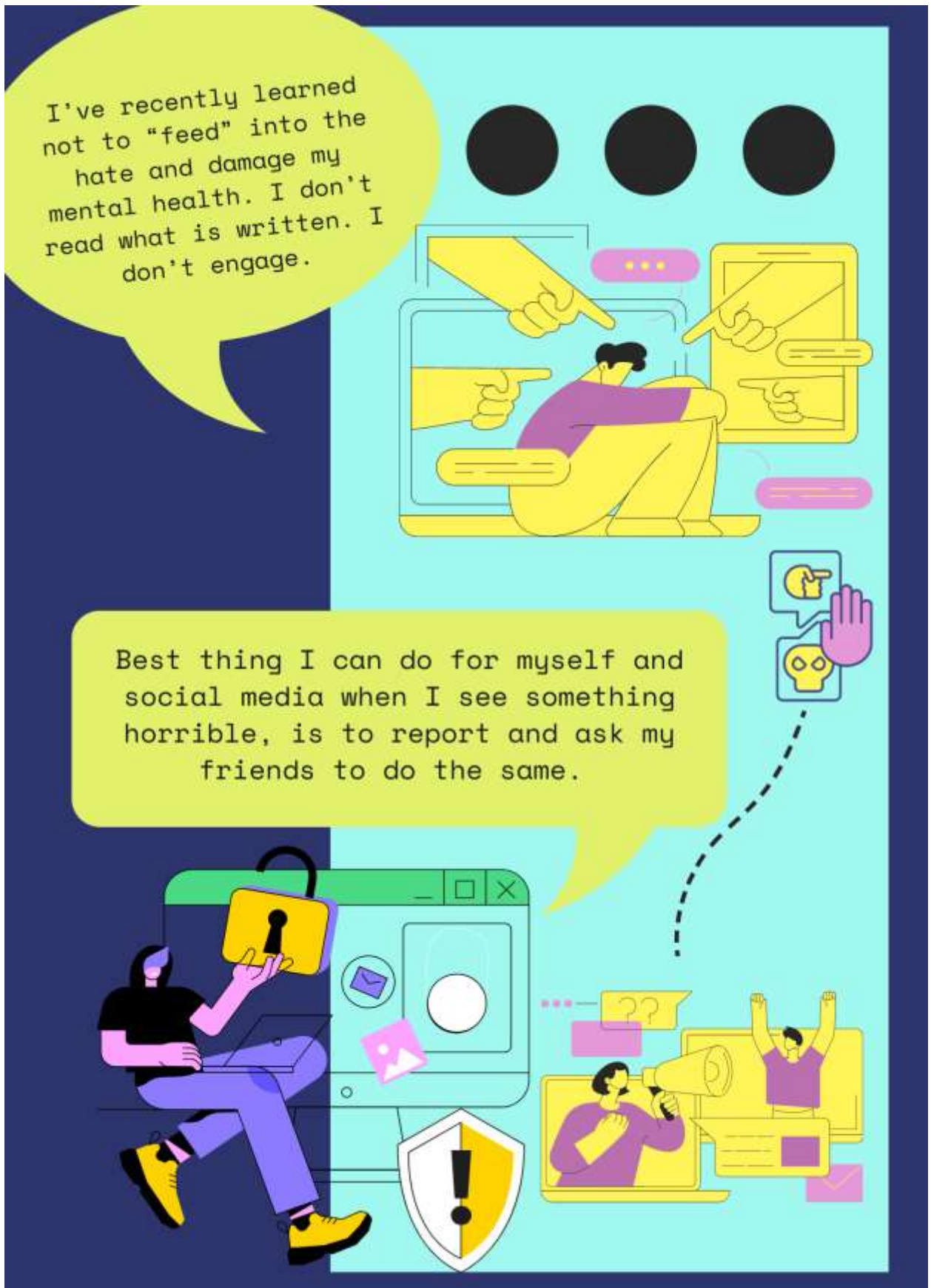
Below, our team has created two comics to demonstrate some of the situations listed above.

Comic 1: Just words on a screen



Comic 2: Stop feeding the beast





3.2.3. "No to online violence!" - example of multisectoral approach

An example of good practice is "No to online violence!" (<https://babe.hr/en/online-nasilju/>) designed by the Croatian association BaBe! with partners, which also contains the CGBV application form, with explanations of the most common forms of CGBV and the form for requesting support. At the end of the form for reporting violence, there is an important note: "Your contact information is handled with particular care and serves only so that our experts can get back in touch with you. The data is not forwarded to third parties and is used exclusively to provide support." It is aligned with both a proactive approach and the ethical principles of respecting the rights of a person who has experienced CGBV. On the link related to the provision of support, information is provided about a trusted person who can be a support when reporting a CGBV to the police or when filing a criminal report, it is recommended who can and who cannot be that person and the right to have them present is indicated during all legal proceedings is stated. Information is given about free psychological and free legal counseling, which includes counseling in situations of online violence (via SOS phone, website, e-mail and personal contact - coming to the counseling center), information about the possibilities of obtaining legal, health and psychological help (in and outside within the framework of the social welfare system), legal advice and placement in a safe house for the most vulnerable persons.

3.2.4. Common sense education - examples of ready-made workshops for promoting digital communication and preventing cyberbullying

On the pages of *common sense education* (<https://www.commonsense.org/education>) teachers can find well designed workshops for children and young people that promote appropriate forms of digital communication and cyberbullying. The duration of the workshops is adapted to the school lesson, and the topics are covered separately for each age group. Thus, for young people aged 15, the workshop on digital communication focuses on red flags that can help young people recognize that a certain chat is risky.

3.3. Conclusion

Although CGBV is a serious problem that disproportionately affects women and gender minorities, preventive activities can reduce the consequences, completely eliminate or at least delay the occurrence of this form of violence or prevent the continuation of CGBV. It is important to know which levels of preventive activities are appropriate for which target group. It is equally important to carefully plan and

evaluate and refine preventive programs. In the prevention of CGBV, we achieve the best results with a proactive and multi-sectoral approach.

3.4. Exercises

Activity 1: Interactive Prevention Strategy Development

Objective: To collaboratively develop and present comprehensive strategies for the primary, secondary, and tertiary prevention of cyber GBV.

Target Group: Youth workers and young adults aged 15-30.

Group Size: Up to 10 participants per session.

Duration: Approximately 120 minutes.

Materials Needed:

- Flip chart or whiteboard with markers.
- Reference materials on prevention principles (handouts or digital access - Provided in the [Annex](#))
- Case studies or real-life examples of cyber GBV (sensitive information redacted).
- Notepads and pens for participants.

Procedure:

1. **Introduction to Prevention Principles (20 minutes):**
 - Start with a presentation on the principles of cyber GBV prevention, covering primary, secondary, and tertiary prevention levels.
 - Explain the difference between these levels, using examples to illustrate each.
 - Distribute handouts or provide digital access to detailed information on each prevention level for reference.
2. **Formation of Groups (10 minutes):**
 - Divide participants into three groups, assigning each group a level of prevention: primary, secondary, or tertiary.
 - Each group will focus on developing a strategy related to their assigned prevention level.
3. **Strategy Development (40 minutes):**

- Groups work on creating a detailed prevention strategy, considering factors such as target audience, methods, challenges, and potential impact.
 - Encourage groups to think creatively and use the reference materials to inform their strategies.
 - Facilitators move between groups to provide guidance and ensure the strategies are comprehensive and relevant.
4. **Group Presentations (30 minutes):**
- Each group presents their strategy to the other participants.
 - Encourage questions and discussions after each presentation to refine and expand upon the strategies.
5. **Collaborative Discussion (20 minutes):**
- Engage all participants in a discussion on how these strategies can complement each other and work together in a comprehensive approach to prevent cyber GBV.
 - Discuss the roles of various stakeholders (individuals, communities, organizations) in implementing these strategies.

Debriefing:

- Summarize the key points from each strategy and the importance of a multi-layered approach to prevention.
- Highlight how understanding and applying these principles can contribute to reducing the prevalence and impact of cyber GBV.

Activity 2: Cyber GBV Awareness Campaign

Objective: To raise awareness about cyber GBV through the creation of an educational campaign.

Target Group: Youth and young adults aged 15-30.

Group Size: Up to 10 participants per session.

Duration: Approximately 90 minutes.

Materials Needed:

- Art supplies (paper, markers, colored pencils, etc.).
- Digital tools for video or graphic creation - Canva or Powtoon can be used to create most materials

- Information pamphlets or resources on cyber GBV - Preferably material from PSCGBV
- Projector or screen for presentations (optional).

Procedure:

1. Introduction and Education (15 minutes):

- Start by discussing what cyber GBV is, including its forms and impacts.
- Provide brief educational input using pamphlets or resources to ensure everyone has a foundational understanding of the issue.

2. Formation of Groups and Campaign Conceptualization (20 minutes):

- Divide participants into small groups of 2-5 people.
- Each group will brainstorm ideas for an awareness campaign that could include posters, social media posts, short videos, etc., focusing on different aspects of cyber GBV.
- Encourage creativity and the use of compelling messages to raise awareness and educate their peers.

3. Campaign Development (40 minutes):

- Groups will use the materials provided to create their campaign elements.
- If digital tools are used, ensure that participants have the necessary skills or provide a brief tutorial.
- Facilitators should move between groups, offering guidance and encouragement.

4. Presenting the Campaigns (10 minutes per group):

- Each group will present their campaign to the other participants.
- Encourage them to explain the thought process behind their campaign, the specific aspect of cyber GBV they are addressing, and the impact they hope to achieve.

5. Group Discussion and Feedback (15 minutes):

- After all presentations, facilitate a group discussion.
- Encourage participants to provide constructive feedback on each campaign, focusing on the message, creativity, and potential impact.
- Discuss how these campaigns could be implemented in real-life settings to raise awareness.

Safety and Sensitivity Measures:

- Remind participants to be sensitive in their representations of cyber GBV.
- Avoid graphic or triggering content in campaign materials.
- Ensure that the campaigns focus on education, prevention, and support rather than sensationalism.

Debriefing:

- Conclude the activity by highlighting the importance of awareness and prevention of cyber GBV.
- Discuss how participants can use their campaigns in their communities or online to make a real impact.
- Provide information about resources and support for anyone affected by cyber GBV.

This activity is designed to empower participants to take an active role in addressing cyber GBV, using their creativity and understanding to develop impactful awareness campaigns. It also aims to enhance their understanding of the issue and its various forms while fostering a sense of community and shared responsibility in preventing cyber GBV.

Activity 3 : Creative Posters Against Cyber GBV and Advocacy

Objective: To engage youth in creating artistic posters that raise awareness and call for action against cyber GBV.

Target Group: Youth and young adults aged 15-30.

Group Size:

Up to 15 participants per session.

Duration:

Approximately 90 minutes.

Materials Needed:

- Poster boards or large sheets of paper.
- Markers, colored pencils, paints, and brushes.
- Magazines, newspapers, and other materials for collage (optional).
- Scissors and glue.
- Examples of impactful advocacy posters (for inspiration).

Procedure:

1. Introduction to Cyber GBV (10 minutes):
 - Briefly explain what cyber GBV is and its impacts.

- Discuss the importance of public awareness and advocacy.
- 2. Inspiration and Ideas (10 minutes):
 - Show examples of advocacy posters related to social issues.
 - Encourage participants to think about key messages they want to convey in their posters.
- 3. Brainstorming Session (20 minutes):
 - Participants brainstorm ideas for their posters.
 - Themes can include the impact of cyber GBV, support for victims, and calling for stronger laws or societal change.
- 4. Poster Creation (40 minutes):
 - Participants use the provided materials to create their posters.
 - Encourage creativity and personal expression.
- 5. Poster Presentation and Discussion (10 minutes):
 - Each participant presents their poster to the group.
 - Discuss the messages conveyed and the artistic choices made.
- 6. Reflection and Closing (10 minutes):
 - Reflect on what was learned through this activity.
 - Discuss how these posters could be used in real-life advocacy efforts (e.g., in schools, community centers, online).

Safety and Sensitivity Measures:

4. Ensure the activity is conducted in a safe and supportive environment.
5. Monitor the content to ensure it is respectful and appropriate.
6. Encourage positive and constructive feedback during presentations.

Additional Activities (Optional):

- Planning a Visit or Meeting:
 - Guide participants on how to request and prepare for a meeting with their council member.
 - Discuss key points to bring up, how to present their case, and how to follow up after the meeting.
- Using Posters as Advocacy Tools:
 - Encourage participants to use their posters as visual aids in their lobbying efforts, whether in meetings, community events, or as part of a larger campaign.

Tips for Effective Lobbying:

7. **Be Informed:** Understand the issue thoroughly and have facts to support your stance.
8. **Be Clear and Concise:** Clearly articulate what you are asking for and why.
9. **Be Respectful:** Even if you disagree, maintaining a respectful tone is crucial.

10. **Follow Up:** After your initial contact or meeting, follow up with a thank-you message and reiterate your key points.

4. Consequences of online violence

Objectives:

- To understand the connection between cyber violence and the consequences in the real life of the victim
- To comprehend the different effects in the lives of the victims
- To be able to acknowledge the changes in the behavior of the victims

4.1. Theory

Cyber violence is a relatively new form of gender-based violence that has emerged with globalization and spread of the internet. Like any form of violence, cyberviolence is not limited to any age or social context, gender or nationality.

The anonymity of the perpetrator helps the most violent and remorse-free attack on the victim as their real life is not affected. The victim's experience in this case is not the same. The effects of this form of violence have real consequences in their lives at different levels, depending on the case and degree of violence. Based on various studies related to sexual violence on the Internet, it has been found that women and people who are part of the LGBTQ+ community are more likely to be victims of online violence because of their gender or sexual preference than men. (Fatem - Zahra, 2018)

The consequences can be psychological, interpersonal, social, physical, and economic. In this section we will examine the influence of gender-based online violence on the victim's daily life and how this experience can give new direction to their life. (Dunn, 2020)

4.1.1. Psychological consequences

The most common and widespread consequences are psychological. The manifestation of these effects can be through anxiety, depression, PTSD, and victims may even engage in acts of self-harm (Adikari, 2016). Many times, a combination of these effects has been shown and the psychology of the individual gets worse as time passes and this violence is inflicted on them. To better examine the psychological effects of cyber violence we can give an example. In a study conducted at the

University of Georgia in the United States of America in 2017, 7 women who experienced online violence because of a romantic partner were asked how they dealt with this experience. The form of online violence that these women experienced was the publication of explicit and personal photos of themselves online without their consent (revenge porn; see also chapter 2). The survey was conducted using an open semi-structured interview so that they could express their experiences in more detail. The findings of this research concerning the psychological impact showed that all of these women were terrified that a person they trusted so much had exposed them to others/strangers in such a way. Many of them lived in a constant state of anxiety and dread about who might find out, who already knew, and what impact this would have on their lives in general. Some of these women have attempted suicide, and very few of them have spoken to their loved ones or an expert out of fear and shame. (Thacker, 2017)

4.1.2. Consequences for interpersonal and social relations

Taking again the example of revenge porn, it is observed that many women isolated themselves and did not talk to acquaintances or friends, so that they had to face this difficult period of their lives alone. The fear and shame of such an act, the paranoia that can be created by constant surveillance and the violation of their privacy in such a way, leads these individuals to cut themselves off from their familiar and social environment and by extension their support network. Often the psychological consequences of such violence lead to the collapse of the rest of their lives, as they are overwhelmed by the thought of this experience, do not associate with friends, family and people and often neglect their academic or professional obligations. This leads to a distortion of the person's self-image, which makes them even more vulnerable to the circumstances surrounding them. (Dunn, 2020)

4.1.3. Economic consequences

Economic impacts are effects of cyber violence that we do not think about as often, but they are existent. This economic burden can be caused intentionally or unintentionally by the perpetrator. Their goal may be to hurt the victim financially and use any means to fulfill that goal. (Dunn, 2020)

Otherwise, the actions of the abuser lead the victim to circumstances that put them under financial strain, for example if they have to pay a psychologist, a lawyer or a company that will ensure their safety in the online space and in the physical world. In the example of revenge porn many women have lost their jobs due to the leakage of

such photos and videos. Many girls have been expelled from schools and universities, forcing them to change their professional orientation without having chosen it themselves, with the result that their income and financial movements are affected directly or in the future. (Dunn, 2020) (see also more on victim blaming in chapter 2)

4.1.4. Physical effects

When cyber violence goes beyond the boundaries of the internet, not only from the victim's point of view (psychological, social, economic consequences) but also from the perpetrator's point of view, violence, usually physical violence, is observed. We are no longer referring to distanced threats but to direct contact with the victim in the real world, through stalking, beatings, rapes or even murders. This transition brings a new wave of impact on the victim. Violence goes from symbolic to real, without a safety net and inhibitions. (Dunn, 2020)

All these impacts experienced by the victim just through the use of the internet lead the victim to a more distant and formal approach with the internet, they will not move freely in the online spaces when they know that their every move is being monitored by someone. Even if this unpleasant experience is over, the online participation of these individuals is generally reduced for fear of experiencing something similar. (Dunn, 2020)

4.2. Best practices

<https://saferinternet4kids.gr/>

<https://timetotalk.gr/>

<https://www.stoponlineviolence.eu/>

These good practices are essentially aimed at addressing the lack of awareness about cyber and gender-based violence, while there are also hotlines that can help the victim, making it easier for them to deal with all the possible consequences that can arise after a cyber attack. Another aim of these good practices is for victims to claim their vindication, while at the same time encouraging their mental resilience.

Finally, good practices aim to:

- Create the ability to recognise (signs of) online violence against girls.
- understand the emotional impact and other possible consequences of online violence against girls for anyone involved.

- know how to prevent online violence against girls.
- know how to act in an adequate, supportive and positive way if they themselves or someone else experiences online violence.

4.3. Conclusion

When one refers to online gender-based violence there is a disconnection from the consequences in real life, believing that the effects are limited in cyberspace. It has been proven that this form of gender violence has the same devastating effects on a person's life as any other. Some consequences are more subtle, such as stress, the costs of managing such an incident, but others are more obvious, such as signs of depression, isolation and physical abuse in the most extreme cases. Victims feel that they are dealing with this situation alone and that no one can help them. In most cases, due to fear and shame, they do not communicate their problem and as a result the issue is magnified. A very small percentage communicates it to official bodies and an even smaller percentage communicates it to family or friends.

4.4. Exercises

Activity 1: "Consequence Collage" Creation and Gallery Walk

Objective: To use visual arts as a means to explore and express the various consequences of cyber violence, followed by a gallery walk for reflection and discussion.

Target Group: Youth and young adults aged 15-30.

Group Size: Up to 10 participants per session.

Duration: Approximately 120 minutes.

Materials Needed:

- Collage materials: magazines, newspapers, colored paper, scissors, glue, markers, and other art supplies.
- Large poster boards or canvas for each group.
- Space to display the collages for a gallery walk.

- Information sheets on the consequences of cyber violence (psychological, interpersonal, social, economic, physical) for reference.

Procedure:

- 1. Introduction to the Activity and Consequences (20 minutes):**
 - Provide a brief overview of the different consequences of cyber violence.
 - Introduce the concept of a collage as a way to visually represent complex ideas and emotions.
- 2. Collage Creation (60 minutes):**
 - Divide participants into small groups.
 - Each group is tasked with creating a collage that represents one or more of the consequences of cyber violence. Encourage them to think abstractly and use symbolism, colors, and imagery to convey their message.
 - Provide collage materials and space for groups to work.
- 3. Gallery Walk and Presentation (30 minutes):**
 - Set up the completed collages around the room like an art gallery.
 - Participants walk around the room to view each collage. The creators of each collage briefly explain their work and the ideas behind it.
 - Encourage participants to reflect on how each collage made them feel and what they learned about the consequences of cyber violence.
- 4. Group Discussion (10 minutes):**
 - Gather the participants for a group discussion.
 - Discuss the different interpretations and perspectives showcased in the collages.
 - Reflect on the power of art to convey complex and emotional subjects.

Debriefing:

- Summarize the key themes and insights that emerged from the collages and discussions.
- Highlight the importance of understanding and acknowledging the diverse impacts of cyber violence.
- Provide information about resources and support for those impacted by cyber violence.

Activity 2: Impact Analysis and Response Planning

Objective: To analyze the various impacts of cyber violence and develop comprehensive response plans to mitigate these consequences.

Target Group: Youth workers and young adults aged 15-30.

Group Size: Up to 10 participants per session.

Duration: Approximately 120 minutes.

Materials Needed:

- Handouts detailing the different consequences of cyber violence (psychological, interpersonal, social, economic, physical).
- Case studies or hypothetical scenarios depicting instances of cyber violence.
- Flip chart or whiteboard and markers.
- Note-taking materials for participants.

Procedure:

1. Educational Overview of Cyber Violence Consequences (20 minutes):

- Begin with a presentation on the various consequences of cyber violence: psychological, interpersonal, social, economic, and physical.
 1. **Psychological Consequences:** Anxiety, depression, self-harm, long-term emotional trauma.
 2. **Interpersonal and Social Consequences:** Isolation, difficulty maintaining relationships, social withdrawal.
 3. **Economic Consequences:** Job loss, educational setbacks, financial burdens from seeking legal or psychological help.
 4. **Physical Consequences:** In extreme cases, stalking and physical harm resulting from online threats materializing in the real world.
- Discuss the short-term and long-term impacts on victims and their surroundings.

2. Case Study Analysis (30 minutes):

- Provide each group with a different case study or hypothetical scenario that illustrates an instance of cyber violence.
- *Examples:*
 - i. *A case of revenge porn leading to psychological distress and social withdrawal.*
 - ii. *An instance of severe cyberbullying causing economic hardship, such as losing a job due to reputational damage.*

- iii. *A situation where online harassment escalates into real-world stalking, leading to physical safety concerns.*
 - Ask groups to identify and discuss the specific consequences presented in their case study.
- 3. **Response Plan Development (40 minutes):**
 - Instruct groups to develop a comprehensive response plan for the victim in their scenario. This plan should address how to mitigate each identified consequence based on their available resources
 - Encourage groups to think about various support mechanisms, such as psychological counseling, legal aid, social support networks, and financial assistance. *Note to the facilitator: be prepared to offer some examples from their local context.*
- 4. **Group Presentations and Collective Feedback (20 minutes):**
 - Each group presents their case study and the response plan they developed.
 - Facilitate a group discussion after each presentation, focusing on the feasibility and comprehensiveness of the response plans.
- 5. **General Discussion and Key Takeaways (10 minutes):**
 - Engage in a discussion about the importance of a holistic approach in responding to the consequences of cyber violence.
 - Highlight the roles that different individuals and organizations can play in supporting victims.

Debriefing:

- Summarize the main strategies discussed for mitigating the impacts of cyber violence.
- Emphasize the need for awareness and preparedness in addressing these consequences.
- Provide information on resources and organizations that offer support for cyber violence victims.

5. Counseling for perpetrators of cyber GBV

Objectives:

- To establish the basic principles that guide the rehabilitation of perpetrators.
- To develop skills in assessing the risk and needs of perpetrators.
- To provide education on gender norms, consent, and healthy relationships.
- To discuss therapeutic approaches and their implementation in counseling.

5.1. Theory

Perpetrator programmes can be provided by state-run agencies and/or NGOs (community-based programmes). In many countries there are a variety of service providers combining state-run programmes and NGOs.

5.1.1. Foundations of rehabilitation - understanding the behavior; ethics and boundaries

In recent years there has been growing recognition of the need to engage both victims and perpetrators of family violence, to both prevent future violence and to encourage engaging and assisting perpetrators or non-perpetrators who are at risk of carrying out domestic violence. The thinking is that a proactive approach is needed, one which goes to the source of the problem – the perpetrators of abuse.

A range of different approaches and methodologies are employed in perpetrator programs, including goal setting, solution focused approaches, counseling, behavior change, narrative therapy, and anger management. One of the mostly widely replicated models is the Duluth model, which focuses heavily on gender equity issues and teaching behaviors to control violence

Despite the widespread pessimism about the effectiveness of perpetrator programs and the plethora of limitations which have been identified, it does seem that some small successes have been achieved, and can continue to be achieved, if the correct conditions are met. Some of these conditions will be outside of the control of program facilitators. For example, there is evidence that programs are more likely to succeed where couples want to stay together. Other factors influencing effectiveness will be the reasons that perpetrators have for attending programs. They may be legally mandated to attend or they may be socially mandated, responding to expectations from family and friends. Their motives may include achieving a reduced penalty in court, avoiding jail, stopping their partner from leaving, or gaining access to their

children. Their attendance may have little to do with taking responsibility for their violence.

5.1.2. Assessment and evaluation of perpetrators

The first step in working with domestic violence perpetrators is to assess their risk of reoffending and their motivation to change. This can help you tailor your intervention to their needs and goals, as well as monitor their progress and safety. You can use various tools and methods to assess risk and motivation, such as standardized scales, interviews, observations, and feedback from victims and other sources. You should also consider the context and factors that may influence their behavior, such as culture, gender, substance use, mental health, and social support.

5.1.3. Education and skill development

1) Communication Skills Development

Effective communication is crucial for addressing the underlying causes of aggressive behavior in online contexts. Enhancing these skills involves:

- **Active Listening:** Teaching perpetrators to fully concentrate on others' words, fostering empathy and understanding. For example, in a counseling session, a perpetrator may be asked to listen to a victim's account of how cyber harassment affected them and then reflect back the emotions and impacts they heard.
- **Assertive Expression:** Training in expressing needs and feelings assertively, yet respectfully, to replace aggressive or passive-aggressive online interactions. For instance, role-playing exercises can be used where the perpetrator practices expressing disagreement online without resorting to derogatory or threatening language.
- **Conflict Resolution:** Techniques for managing disputes peacefully, emphasizing problem-solving and negotiation, such as guided exercises on resolving online arguments constructively, avoiding escalation into cyberbullying or harassment.

2) Emotional Regulation

Managing emotions is essential to prevent impulsive and harmful actions online. Key aspects include:

- **Self-awareness:** Helping perpetrators recognize their emotions, triggers, and impacts, such as identifying feelings of anger or inadequacy that lead to abusive online behavior.
- **Stress Management:** Techniques like mindfulness, relaxation exercises, and physical activities to mitigate stress, which can be a precursor to online aggression. For example, introducing breathing techniques to use when feeling the urge to post harmful comments.
- **Response Modification:** Learning to pause and consider reactions, opting for non-harmful responses. This might involve practicing a 'time-out' before responding to online provocations.

3) Examples of Educational and Skill Development Activities

These activities are designed to reinforce key skills:

- **Role-Playing Sessions:** Simulating online scenarios to practice healthier communication and emotional responses. For example, role-playing how to respond to a heated discussion in an online forum without resorting to cyber aggression.
- **Group Discussions:** Facilitated sessions for sharing experiences and learning from others, such as discussing the consequences of cyberbullying on victims.
- **Workshops on Emotional Literacy:** Focusing on identifying and managing emotions, particularly those that might trigger harmful online behavior.

4) Lifestyle Change Promotion: Promoting Healthy Habits and Constructive Use of Time

Adopting a healthier lifestyle can significantly influence behavior modification:

- **Routine Building:** Encouraging a structured daily routine with healthy habits. For example, integrating specific times for online activity and ensuring it is balanced with offline activities.
- **Engagement in Positive Activities:** Promoting participation in activities like sports or hobbies that can offer positive outlets for emotions and reduce time spent in potentially harmful online environments.
- **Social Connections:** Building and maintaining positive social relationships, both online and offline, to foster a support network that discourages negative online behavior.

5.1.4. Intervention strategies

The next step is to choose an intervention model that suits the perpetrator's risk and motivation level, as well as your own skills and resources. There are different types of intervention models for working with domestic violence perpetrators, such as cognitive-behavioral therapy, motivational interviewing, trauma-informed care, and restorative justice. Each model has its own strengths and limitations, and may work better for some perpetrators than others. You should also be aware of the evidence and outcomes of each model, and adapt them to the specific needs and circumstances of each case.

- a. Cognitive Behavioural Therapy is one of the most actively researched psychotherapies and has received consistent empirical support for a host of mental health problems and conditions. In the treatment of aggressive behavior, CBT interventions are now a commonly used approach to help different populations to regulate anger and aggressive behavior. The main techniques used in CBT focus on establishing a therapeutic relationship, behavioural change strategies, cognitive restructuring, modification of core beliefs and schemas, and the prevention of relapse and recurrence. Cognitive theory suggests that psychopathology is characterized by the activation of a conglomerate of related or contiguous dysfunctional beliefs, meanings, and memories that operate in coordination with affect, motivation, behavior, and physiological responses. Different psychopathological conditions are associated with specific biases that influence how an individual incorporates and responds to new information.
- b. Motivational Interviewing is often delivered as a brief intervention based on client-centered principles. Guided by these principles, MI emphasizes strategic use of common counseling skills, such as reflective listening, summarizing, and paraphrasing. Advice is typically only given on request, and with patient permission. MI is also sometimes combined with other types of interventions (e.g., Cognitive Behavioral Therapy) in order to enhance treatment retention and engagement. The aim of the combined Motivational Interviewing and Motivational Enhancement Therapy is to increase client motivation and commitment to reduce or quit bad behavior – usually over the course of 3 to 4 sessions. With this increased commitment to change, the patient is believed to be able to mobilize their own internal and external resources to facilitate change.
- c. Restorative justice is an approach oriented towards repairing, as far as possible, the harm caused by crime, conflict or other transgressions. A core element of restorative justice is the participation of the victim, the offender and possibly other parties, such as the community, to voluntarily come

- together with the help of a facilitator to address the harm and its consequences. The most common processes are victim-offender mediation or conferencing, which take place as direct face-to-face encounters (after a well-developed preparation) or indirect encounters (e.g. via video calls or messages). What's unique about restorative justice is that it creates a safe space where the parties are empowered and responsible for the consequences of the act that brought them together.
- d. To effectively combat Cyber Gender-Based Violence (CGBV), a range of targeted strategies is implemented. **Digital Safety Planning**, crucial for victims' protection, involves steps like password changes and privacy enhancements; a victim of cyberstalking, for instance, successfully secured their online presence with the help of a digital safety expert, thwarting the stalker's efforts. **Trauma-Informed Cyber Support** addresses the psychological fallout of digital abuse, exemplified by a support group that aids revenge porn victims through counseling, aiding in coping with public exposure and shaming. **Legal and Policy Advocacy** plays a pivotal role, as seen in the use of anti-cyberbullying laws to prosecute online harassers, setting legal precedents that strengthen CGBV mitigation efforts. **Educational Workshops on Digital Literacy and Ethics** contribute significantly, with initiatives like a university's program on digital consent leading to reduced online harassment. **Cognitive-Behavioral Therapy**, tailored for CGBV perpetrators, has shown effectiveness in a rehabilitation program that significantly cut recidivism among convicted online harassers. Lastly, **Building Online Support Networks** provides invaluable emotional support; a dedicated online forum for cyber harassment victims exemplifies a platform for sharing and healing, underscoring the importance of these diverse yet interconnected strategies in addressing the multifaceted challenge of CGBV.

5.2. Best practices

5.2.1. WWP European Network - Training on Cyber Violence and Perpetrator Work

<https://www.work-with-perpetrators.eu/training/cyberviolence-and-perpetrator-programmes>

https://www.work-with-perpetrators.eu/fileadmin/WWP_Network/redakteure/Campaign/WWP_flyer_EN_FINAL.pdf

This program emphasizes understanding cyberviolence and its nuanced connection with offline violence, offering insights on how to assess and intervene with

perpetrators effectively. The training agenda covers different forms of cyberviolence, including cyberharassment and cyberstalking, and explores the legal aspects of cyberviolence within the European context .It also delves into the psychological aspects of cyberviolence, examining the link between coercive control and cyberviolence, and the impact on victims .The program integrates assessments of cyberviolence in everyday work with perpetrators, utilizing modern tools developed within the Destalk project.

The training includes tackling cyberviolence in both individual interviews and group work settings, providing key elements of cyberviolence assessment on real-life case studies. It also focuses on protecting survivors from cyberviolence, including risk assessment and safety planning.

5.2.2. Contexto

The Contexto Programme is a hands-on program aimed at helping those who have committed intimate partner violence. It's run by the University of Valencia in Spain and follows a well-thought-out approach called the ecological model (first introduced by Heise in 1998 and endorsed by the World Health Organization). This program's main goal is to tackle the causes of violence in close relationships and boost factors that prevent it. It does this by looking at four key areas: the person's own characteristics, their relationships, their immediate environment, and wider societal influences (as described by Lila and others in 2010). The programme is conducted in three phases: assessment, intervention and follow-up. A comprehensive study analyses the results of the application programme and you can read more about it here: https://scielo.isciii.es/scielo.php?script=sci_arttext&pid=S1889-18612013000100004

5.3. Conclusion

As we conclude Chapter 5, it's imperative to reflect on the significance and complexity of counseling perpetrators of cyber gender-based violence (CGBV). This chapter has underscored the critical need for comprehensive rehabilitation programs that go beyond mere punitive measures, aiming instead to address the root causes of such behaviors and foster lasting behavioral change.

The interventions and strategies discussed in this chapter, including communication skills development, emotional regulation, and lifestyle change promotion, are integral to reshaping the behaviors and attitudes of CGBV perpetrators. These approaches, rooted in empathy, understanding, and behavioral psychology, are designed not only

to prevent recidivism but also to contribute positively to the broader societal challenge of eradicating cyber GBV.

As we move forward, it's crucial to continue developing and refining these approaches, ensuring they are adaptable to the ever-evolving digital landscape. Collaboration among mental health professionals, legal experts, educators, and policymakers is essential to create a holistic and effective response to cyber GBV. Ultimately, the goal is to foster a digital environment characterized by respect, empathy, and responsibility, where individuals are both aware of the consequences of their actions and equipped to make positive choices in their online interactions.

5.4. Exercises

Activity 1: Perpetrator Rehabilitation Role-Play and Discussion

Objective: To simulate and understand various rehabilitation approaches for perpetrators of cyber GBV, emphasizing the need for behavior change, ethics, and boundary setting.

Target Group: Youth and young adults aged 15-30.

Group Size: Up to 10 participants per session.

Duration: Approximately 120 minutes.

Materials Needed:

- Role-play scripts depicting scenarios involving perpetrators of cyber GBV.
- Information sheets on different rehabilitation approaches (such as the Duluth model, CBT, motivational interviewing, etc.).
- Flip chart or whiteboard and markers for group discussions.
- Evaluation forms or checklists to assess the perpetrator's risk and motivation for change.

Procedure:

1. Introduction to Perpetrator Rehabilitation (20 minutes):

- Begin with an overview of the importance of engaging perpetrators in rehabilitation to prevent future violence
- Introduce various rehabilitation approaches and methodologies, including goal setting, counseling, and behavior change strategies

Role-Play Preparation (20 minutes):

- Divide participants into small groups, assigning each group a role-play script that illustrates a scenario with a cyber GBV perpetrator.
- Provide groups with information sheets on different rehabilitation approaches to guide their role-play.

Role-Play Execution (30 minutes):

- Each group performs their role-play, depicting an interaction between a perpetrator and a counselor/therapist.
- Encourage the portrayal of various intervention strategies, focusing on behavior change and ethical considerations.

Group Discussion and Evaluation (30 minutes):

- After each role-play, lead a group discussion on the effectiveness of the portrayed rehabilitation approach.
- Use evaluation forms or checklists to assess factors like risk of reoffending and motivation to change, as depicted in the role-play
- .

Education and Skill Development (20 minutes):

- Discuss the importance of education and skill development in rehabilitation, including communication skills and emotional regulation
 - .
 - Encourage participants to brainstorm additional educational and skill development activities that could aid in rehabilitation.

Debriefing:

- Summarize key insights from the role-plays and discussions.
- Emphasize the complexity of perpetrator rehabilitation and the need for tailored interventions.
- Discuss how understanding these approaches can contribute to broader efforts in preventing cyber GBV.

Activity 2: Interactive Learning Stations on Rehabilitation Approaches

Objective: To provide an engaging and educational experience on different rehabilitation approaches for cyber GBV perpetrators, using interactive learning stations.

Target Group: Youth and young adults aged 15-30.

Group Size: Up to 10 participants per session.

Duration: Approximately 120 minutes.

Materials Needed:

- Station setup materials: Posters, infographics, and interactive elements (like quizzes or simple activities) related to different rehabilitation models (e.g., Cognitive Behavioral Therapy, motivational interviewing, the Duluth model).
- Information sheets or handouts about the basics of each rehabilitation approach. *View more in the chapter and in the [Annex](#)*
- Small tokens or stickers for participants to collect at each station as part of an incentive system.
- A reflection sheet or journal for each participant.

Procedure:

1. **Introduction to Rehabilitation Approaches (15 minutes):**
 - Begin with a brief overview of why rehabilitation is important for perpetrators of cyber GBV.
 - Introduce the concept of different rehabilitation approaches in simple terms.
2. **Learning Station Rotation (60 minutes):**
 - Set up different stations around the room, each dedicated to a specific rehabilitation approach.
 - Participants rotate through the stations in small groups, spending about 10-15 minutes at each.
 - At each station, participants engage with the materials, complete a simple interactive activity, and collect a token or sticker.
3. **Group Reflection and Discussion (30 minutes):**
 - Once all participants have visited each station, gather them for a group discussion.
 - Ask participants to share what they learned at each station and their thoughts on the different approaches.

- Encourage them to reflect on how these approaches can help prevent future cyber GBV.

4. Personal Reflection Activity (15 minutes):

- Provide each participant with a reflection sheet or journal.
- Ask them to write down one key takeaway from each station and how they think this knowledge can contribute to positive change.

Debriefing:

- Collect the reflection sheets (if participants are comfortable sharing) and summarize common themes and insights.
- Highlight the importance of understanding and addressing the causes of cyber GBV for effective prevention.
- Discuss the role of education and awareness in transforming attitudes and behaviors.

6. Proactive strategies to protect oneself online

Objectives

The specific objectives of this chapter are:

- Offer practical strategies and tips for preventing cyber violence, focusing on proactive measures individuals can take to safeguard themselves and others online.
- Emphasize the importance of digital literacy in navigating online spaces safely, including understanding the need for privacy settings, strong passwords, and practicing responsible online behavior, in general..
- Provide guidance on maintaining online well-being, emphasizing the importance of self-care, setting boundaries, and seeking support when faced with online negativity.
- Provide the awareness of social engineering techniques and how they can be used to manipulate people.

6.1. Theory

Protecting oneself against the possible dangers of cyber violence has become crucial in a time when the digital world is permeating every aspect of our life. Cyber violence, which includes cyberbullying, cyberharassment, and other forms of digital abuse, can have a significant negative impact on people's mental health and general online experience. However, there are ways to protect oneself from it. Adopting preventive measures such as digital hygiene (also known as cyber hygiene) habits, understanding principles of persuasion and knowing how to set boundaries can be vital to successfully navigating the dynamic internet ecosystem.

In this chapter, we present a set of practical tips and strategies to empower people in protecting themselves from cyber violence, while also fostering a digital space characterized by respect, empathy, and responsible online behavior.

6.1.1. Digital/Cyber hygiene

We are all aware of the term “personal hygiene”, but have you ever heard of the term “digital hygiene”? Digital hygiene, also known as cyber hygiene or online hygiene, refers to the practice of keeping your gadgets - such as your computer, tablet, and phone - organized and up to date with the newest software to guard against online dangers. To put it simply, maintaining good digital hygiene is all about how one uses

a single device and the safety measures one takes to keep data and private information safe and organised. While personal hygiene helps one to stay safe and healthy, digital hygiene helps one to achieve the same goals, just in digital life.

Here are some tips and practices how to implement digital or cyber hygiene:

- **Understanding that personal data is important.** There is a popular misconception among internet users that their data or access to their data is not important. The online data gives one control over their identity and personal image/presence in the digital world. Without this control, people with malicious intentions such as hackers can manipulate their identity to serve their goals, whether it is selling them a more expensive vacation, stealing their savings or impersonating them to reach their malicious goals.
- **Strengthening the passwords.** It is essential to use strong and unique passwords for online accounts. The strongest passwords usually are a combination of letters, numbers, and symbols. Avoid using easily guessable information, such as your pet's name or the name of your highschool/university. Furthermore, different passwords should be used for different accounts. Ideally, passwords should be something one can easily remember, but difficult to guess for others, e.g. "3MonkeysRDancing^^". While it is hard to remember all the passwords, there are useful online tools such as password managers that make management of passwords easier - usually they will automatically update stored passwords, keep them encrypted, and require multi-factor authentication for access. Finally, it is essential not to share passwords, even with your friends and loved ones.
- **Enabling two factor (2FA) Multi-Factor Authentication.** It is important to enable two factor or multi factor authentication whenever possible, as it adds an extra layer of security. Two-factor authentication (2FA) requires users to present two types of authentication, while MFA requires users to present at least two, if not more types of authentication. Thus, while passwords can sometimes get leaked, it is more difficult to hack a person when two factor or multifactor authentication is enabled.
- **Keeping software updated.** It is important to keep operating systems, antivirus software, and other applications up to date as updates often include security patches that protect against known vulnerabilities. It is especially important not to download and install any games or software from doubtful sources, for example, torrent downloads, "cracked" software downloads, etc. On the other hand, any unused software should be uninstalled and removed.
- **Regularly backing up the important data.** By backing up important files and data regularly, either to an external hard drive or a secure cloud service, a person can ensure that in the event of sudden data loss due to a security

- incident (e.g., hacking, cyber violence from the partner), the data can be restored.
- **Using secure wifi networks.** Secure wifi networks prevent unauthorized users from accessing WIFI and stealing any data - this could include passwords, banking information, or personal data that can be used for identity theft. Public wifi networks can often be unsecured and vulnerable for attack, thus, this is why it is highly recommended not to use public wifi, especially for important transactions such as internet banking, etc.
 - **Limiting digital and social footprint.** Sharing every part of one's life with others to strengthen social connections has never been easier thanks to social media and other technological developments. The result of that is oversharing, which frequently goes unreported since so many people engage in it. Unfortunately, oversharing can give malicious onlookers more information about a person than that person would ever want to divulge. Based on the information posted and available online, people with malicious intentions can create a clearer picture of one's life, habits, key relationships, and possessions. This can significantly increase the risk of become a victim to cyber violence. Thus, it is essential to regularly review and update one's privacy settings on social media platforms as well as be mindful of what can be and should be shared online, especially to strangers on the internet. Keep in mind one good rule of “digital permanence” - anything that is uploaded and published once on internet, most likely to stay there forever.
 - **Keeping oneself updated.** Developing a proactive “security first” mindset is a key to reducing the chances of becoming a victim of cyber violence. It is essential to keep up with new cybersecurity developments, new scam threats as well as new tools and techniques to protect oneself.

Overall, there are many tips and strategies to keep up with digital hygiene. To stay safe online it is important to understand the general principles and make them a part of daily routine. Furthermore, considering that the digital landscape is always evolving with new threats emerging every day, it is paramount to keep oneself updated with the latest policies, tools and protection measures. Finally, it is essential to acknowledge that digital threats and cyber violence do not only come from strangers, the perpetrator could be anyone, even a person from a family or social circles. As such, protecting personal data, particularly passwords and other personal sensitive data, requires a strict commitment to privacy, ensuring that sensitive information remains inaccessible even to trusted people.

6.1.2. Practicing self-care and setting boundaries

In an era where communication is easily accessible through the touch of a button on our phones, individuals find themselves increasingly immersed in the online realm - constantly refreshing news feeds, engaging in social media, seeking information, reading news, checking emails beyond work hours, shopping, and chatting. While being able to easily access various types of information can be invaluable, the online world also harbors dark aspects, particularly in terms of cyber violence. Therefore, it is crucial, especially for the younger generation that spend a lot of their time online, to develop awareness and implement self-care practices and online boundaries. This proactive approach is essential for safeguarding against cyber violence in the digital space.

Here are a few tips and practices how to implement self-care and boundaries online:

- **Considering one's purpose:** Before starting to interact online, especially using social media, it is wise to think about one's purpose of using it and adjust one's own profile settings accordingly in order to only reveal as much of oneself as one wishes and not overshare on private information.
- **Being selective about who one connects online:** There is no need to accept all friend requests received on social media, especially from strangers or people one only knows in passing. Even if these people don't necessarily pose a danger, everyone decides on their own who they surround themselves with. It is also advised to regularly review one's friends' or followers' lists and remove or block individuals who engage in harmful behavior.
- **Taking things slow:** People often get to know others faster online, as they tend to express their emotions in a more unfiltered way or reveal personal details earlier than they might have done in a face-to-face interaction. It takes time to get to know a person in real life and at first, one mostly gets to know the side of a person that the other person wants them to see. As it is even more difficult to uncover a person's true intentions online, one should take more time to get to know somebody until the person can be trusted.
- **Utilizing available platform features.** Many platforms, especially social media ones, have many features available to the user that can help them to stay away from certain topics, comments, etc. as well as certain users that evoke negative emotions and can lead to stress and anxiety. For example, many platforms have a feature to filter comments (blocking certain keywords from comment section), blocking people or sharing content only to close friends, choosing who can comment on one's posts, etc. to maintain a positive online environment.
- **Practicing digital detox.** To avoid being permanently exposed to neither the addictive dopamine rush of being online nor negative emotions triggered by hateful messages and comments, one should set boundaries by limiting the

- time spent online. In this respect, each individual has to decide for themselves whether it helps to not be on the phone directly before going to bed or getting up, install timers for certain apps, or delete those apps completely for a while.
- **Prioritizing mental health.** Constant exposure to social media, online interactions, and digital stressors can significantly impact one's mental health. Thus, it is paramount to learn how to recognize the signs of digital fatigue, anxiety, or burnout and take proactive steps to address them. This may involve setting limits on screen time as mentioned above, practicing mindfulness, and engaging in offline activities that bring joy and relaxation. Regularly checking in with one's emotions and being mindful can help to form and maintain a healthier relationship with the digital world.
 - **Seeking help.** Cyber violence can have severe implications on one's mental health. If one feels unable to manage the situation and their mental wellbeing on their own, it is essential to reach out and seek help - either from friends and family or professionals. By talking about the difficulties encountered in the virtual realm, such as cyberbullying or harassment, one can acquire understanding, adaptive mechanisms, and psychological assistance. Asking for assistance is a proactive step that promotes mental well-being and gives people the tools they need to navigate the digital realm more resiliently.
 - **Being thoughtful with one's communication:** In addition to establishing one's boundaries, it is also essential to respect the boundaries of others and to regularly reflect on one's behavior. In doing so, one can always imagine oneself in the role of the other conversational partner and think about how one perceives one's message. Reflecting does not only prevent misunderstandings but also ensures that one does not become a culprit who harms others with their behavior online.

In case one is confronted directly with cyber violence, the following steps can serve as a guide how to deal with it:

- **Ignoring:** In the case of hateful comments and messages online, it is recommended not to respond, especially if the author is a stranger. Haters and trolls feel encouraged to continue bullying by the response of the recipient, while they might lose interest over time if they do not receive an answer.
- **Recording:** In case of cyber bullying and especially cyber violence, it is important to keep a record of the occurrences. By collecting proof it's easier to verify what has happened and identify the culprit. Not only does keeping a record help the victim with analyzing the situation, but also does it help to reach out for support.
- **Reaching out:** As soon as the victim has reflected on the situation and realized that he or she is being exposed to cyber violence, he or she should confide in other people in their immediate personal environment. With the support of

- friends and family, solutions can be sought together and ways can be found to free the person concerned from the victim role.
- **Cutting off the bully:** If the bullying continues although the hateful comments or messages are being ignored, the aggressor can be blocked on social media, for instance. If the harassing via the phone doesn't stop and even the blocking of the number doesn't help, the victim might consider changing his or her phone number.
 - **Reporting the bullying:** If the aggressor leaves visible traces of harassment on a website like Facebook, Instagram, YouTube or any other social platform, the culprit violates the website's terms of use. Hence, the victim can report the culprit and ensure that the negative messages and comments get deleted and the person responsible gets kicked off the social media platform. It might even be possible to uncover an anonymous aggressor in that way and hold this person responsible for his or her actions.
 - **Turning to the local authorities** If none of the previously listed actions were successful in stopping cyberviolence, local authorities must be notified. It is essential to keep records of harassing messages, comments, or actions as evidence when reporting. Even though a lot of online bullies are "anonymous", police have the tools to be able to track them down and take action. Please keep in mind that, there are different laws and legislation in place in each country related to cyber harassment, and cyber violence in general. In the EU, while there is no EU-wide anti-online bullying law so far, only European directives, many countries have developed their own national laws and have their own cyber crime police units.

6.1.3. Understanding the main principles of manipulation

One of the most powerful tools used to manipulate people is called social engineering. Social engineering can be defined as the act of manipulating human beings, most often with the use of psychological persuasion, to gain access to systems containing data, documents, and information that the social engineer should not have access to obtain. In simple words, Social engineering is the art of exploiting human psychology, rather than technical hacking techniques, to gain access to buildings, systems or data.

In the digital landscape, perpetrators often exploit human psychology to deceive them into disclosing sensitive information or engaging in harmful actions. Thus, by familiarizing oneself with social engineering methods, individuals can improve their awareness of potential threats, such as phishing attempts or impersonation schemes. This awareness can empower individuals to critically assess online interactions,

identify red flags, and make informed decisions to protect their personal information and digital well-being.

Cyber-criminals have learned and become experts in social engineering, appealing to human nature to reach their malicious intentions and goals. Their most common manipulation methods usually rely on immediate human responses and emotions such as fear, intimidation, sense of urgency, greed, curiosity, trusting nature and empathy. Cybercriminals are aware that a well-crafted and personalized text message, voice message, or email can trick recipients into sending money, disclosing personal information or intimate pictures, or downloading a malicious file.

To understand better the concept of social engineering and how to recognise manipulations, it is essential to take a look at 6 principles of persuasion explained by Dr Robert B. Cialdini in his book “Influence: The Psychology of Persuasion”. While initially, these principles were used in marketing, to manipulate people to spend money and buy products/services, they were easily adopted and are used in social engineering nowadays as well.



Let's take a closer look at such principles and how they could be implemented in real life situations:

1) **Reciprocation** – “give and take”, wanting to repay what the other person has provided. Classic examples of it are - an email offering a discount or coupon on some purchases in exchange for sharing information or signing up for an account; exchanging sexual content (“I show you mine, you show me yours”), an email promising to give access to confidential information if a specific attachment is downloaded, etc.

2) **Scarcity** – it is in human nature to want what is difficult to get. People are more likely to give their personal information, for example, to sign up for a waiting list of some product/service they desire and it is exclusive and hard to get.

3) **Authority** – people tend to follow authority and credible experts in general. Therefore, people with malicious intents often try to impersonate a known person with some authority, e.g. a colleague, boss, any public authority figure, or famous person/expert. Consider a scenario of an ad in social media where a renowned expert invites individuals to invest in what appears to be an extraordinary investment opportunity. Those who perceive the expert as an authoritative figure are more susceptible to this invitation, even in instances where the advertised opportunity is, in fact, a fraudulent scheme. Another example could be a woman, receiving explicit emails, messages or any other unwanted advancements from a boss or any person in power position - often in these cases, stopping her from reporting it.

4) **Consistency** – people are, in one way or another, creatures of habit. Any form of communication that looks like official communication exploits this fact, hoping the recipient overlooks the unusual request that is included. For example, an email with the Amazon logo saying a shipment is held up and asking the recipient to confirm their home address may not raise red flags even if no shipment is expected - that is the power of a widely recognised brand. Other examples could be deepfake pictures and videos. We are used to a person's look, thus images and videos that copy the look, the manners or sometimes even the speech of that person can easily fool us as it is familiar to us.

5) **Consensus or social validation** – people tend to follow other people, especially when they are not certain about something. This principle can explain online bullying better - people tend to do what they see the others are doing.

6) **Liking** – this is a quite simple principle – if people like you or conversely they want to be liked, they are most likely to say “yes”. For example, if we like a person, whether a friend or a love interest, we are more likely to do what they are asking.

7) **Unity** – this principle was not initially in the book and was added later. The idea is that the more people identify themselves with other people, the more they are influenced by them. For example, a person is more likely to reveal sensitive information in a casual chat on a Facebook group dedicated to his hobby and gathering other hobby enthusiasts. The same goes to revealing sensitive information to family and friends based on trust.

6.2. Best practices

The key to reducing cyber violence is awareness, education and advocacy. However, with the digital landscape, and information overload, it is becoming increasingly difficult to educate people, attract supporters and motivate them to get involved. Here are some of the best practises aiming to raise awareness, reduce the stigma and educate communities.

6.2.1. Cyber gender-based violence awareness campaigns

This is where well-designed and impactful awareness campaigns can play a crucial role. Awareness campaigns represent one of the most widely embraced, efficient, and adaptable methods for generating public interest and educating communities on significant matters - such as the escalating issue of cyber gender-based violence.

An awareness campaign is any time-bound, strategic campaign primarily focused on enhancing public visibility and understanding of a particular cause. Typically, these campaigns are designed to spread word about an important issue, why it matters, how to tackle a given issue, and why a person needs to support proposed solutions.

A good example of such awareness campaigns is the “#SafeSpaces” campaign developed by European Institute for Gender Equality (EIGE). The campaign created and used artworks portraying three forms of cyber violence against women and girls (CVAWG): cyber stalking, cyber bullying and online gender-based hate speech related to three physical spaces: home, school and public. The campaign invites the community to reflect and answer simple questions: Are we as safe as we think we are? Is the women or girl next to us safe? More information about the campaign can be found [here](#).



The example of #safespaces campaign in Lithuania. Source: <https://eige.europa.eu/>

Another good example is “Orange the World, 16 Days of Activism against Gender-Based Violence” annual campaign. The campaign begins on 25 November, the International Day for the Elimination of Violence against Women and runs through International Human Rights Day on 10 December. It calls for an end to violence against women and girls. In 2023, the campaign theme is “Invest to prevent violence against women & girls”. More information about the campaign can be found [here](#).

6.2.2. Education through games

Engaging and motivating the youth in the learning process can be quite difficult task, especially when it comes to conventional learning approaches. Often, the desired learning goals can be more effectively achieved through educational games as opposed to traditional methods. Educational games offer an interactive and dynamic approach, turning the learning experience into an enjoyable and immersive activity for youth. Thus, the integration of educational games into the learning process not only can make education more appealing to the younger generation but also can encourage a positive and enthusiastic attitude towards acquiring knowledge.

A good example of an educational game is the Play safe game/app. Through a series of interactive games, the app provides children and youth with the knowledge of how to recognise gender-based violence, whether it is happening to them or to someone close to them. It also explains appropriate responses and actions to take when encountering digital violence. The game also is suitable for parents and teachers as it enables them to refresh their knowledge on different forms of gender-based violence. More information about the game can be found [here](#).



Images from the app. Source:

<https://play.google.com/store/apps/details?id=diotima.unicef.play.safe&hl=en&gl=US>

Another example of an educational game is “Digital safe tea”. The game aims to give Digital women the “tea” on online safety. Players can choose one of three characters based on different “archetypes” of African women: Aisha, Goitse and Dami. Each character has a unique profile that represents a variety of occupations, regions, hobbies, and online activities. The idea of the game is to allow the player to step into the world of these women - facing a variety of scenarios that pose digital threats such as harassing messages, non consensual sharing of intimate images, cyber flashing and others. Players have to choose the most suitable response to such threats to get to the next stages of the game - teaching them how to navigate such threats in real life. More information about the game can be found [here](#).

6.2.3. Advocacy for stricter laws

Whether a person is advocating for greater road safety in the community or the protection of women's rights, there is no doubt that advocacy plays a significant role in achieving meaningful change. Through advocacy efforts, individuals, organizations or groups of people can use their voices to raise awareness on important issues, such as cyber gender-based violence and its impact on individuals and society. Advocacy can serve as a catalyst for public discussion, fostering a deeper understanding of the issue's significance, gathering more support and resulting in stricter laws and new legal frameworks. Furthermore, it serves as a tool for victims to share their stories and encourage others to take a stand as well. Overall, advocacy can be a driving force for legislative changes, shaping public opinion, raising awareness and, in general, creating safer communities whether online or offline.

A good example of advocacy, is the mother from Ireland Jackie Fox, who lost her daughter Nicole (Coco) to suicide due to years of online and offline bullying. Advocating in her daughter's name she was a driving force behind the campaign to criminalize cyberbullying and introduce a new law titled Coco's Law to commemorate her daughter. She has succeeded and Coco's Law created two new offenses which criminalize the non-consensual distribution of intimate images. The first offense deals with the distribution or publication of intimate images without consent and with intent to cause harm. The penalties applicable can be an unlimited fine and/or 7 years imprisonment. The second one, a less serious offense, deals with the taking, distribution or publication of intimate images without consent even if there is no specific intent to cause harm. This offense will carry a maximum penalty of a €5,000 fine and/or 12 months imprisonment. Find out more about this story [here](#).

6.3. Conclusion

In conclusion, preventing cyber violence is a shared responsibility that requires proactive measures and informed decision-making. By incorporating the practical tips and strategies outlined in this chapter, individuals can protect themselves against the potential dangers of cyberviolence and contribute to creating a safer digital environment. Digital hygiene practices, an understanding of persuasive techniques, the skill to set boundaries and take care of one's mental wellbeing are integral strategies in this endeavor. As we work towards a digital space characterized by respect, empathy, and responsible online conduct, each person's commitment to promoting a culture of digital well-being becomes instrumental in fostering a healthier and more supportive online community.

6.4. Exercises

Activity 1: Recognising main principles of manipulation

Objective: The main aim of this workshop is to introduce 7 principles of influence and show how they can be used in cyber crime and cyber violence. Through comprehensive practical activities students will develop their critical thinking skills, learn how to identify these manipulation strategies and resist them in the future.

Target Group: Youth and young adults aged 15-30.

Group Size: Up to 15 participants per session.

Duration: Approximately 1.5 hours.

Materials Needed:

- Printed case studies to be handed out for the participants
- Printed description of 7 principles of persuasion
- Flipchart and markers or whiteboard/smartboard

Procedure:

1. Introduction to influence (20 minutes):

- Begin with a brief presentation on the concept of influences.
- Continue with an introduction to 7 principles of persuasion by Caldini.
- Show several examples of these principles implemented in practise.

2. Applying Principles to Cyber Gender-Based Violence (40 minutes):

- Divide participants into small groups (3-4 people per group).
- Hand out each group 2 case studies of cyber violence (make sure that each case represents different principal of persuasion). Participants can also use example from their own experience if they wish.
- Ask participants reflect on the case study and discuss which principle or several principles they represent as well as what the best course of action would be in that specific situation.

3. Group Discussion and Evaluation (40 minutes):

- Each group presents their case studies - identify principle(s) of persuasion and the best course of action in that specific case.

- Feedback and constructive discussion on each case study presented, the principles and how best to act in these situations.

Debriefing:

- Summarize key insights
- Ask questions:
 - o How did understanding the 7 Principles of Influence deepen your awareness of cyber gender-based violence?
 - o Were there specific scenarios or case studies that stood out to you?
 - o In what ways do you think the principles can be applied to prevent or respond to cyber gender-based violence?

Activity 2: Creating an awareness campaign

Objective: The main aim of the workshop is to introduce participants to the concepts of advocacy and self-advocacy. Through comprehensive discussions and practical activities, the workshop also aims to emphasize the significance and potential of building awareness campaigns as effective tools for both advocacy and self-advocacy. Participants will delve into the nuances of creating effective campaigns, realizing how these initiatives can be effective means of promoting causes, increasing public awareness, and giving people the confidence to speak up for others as well as themselves.

Target Group: Youth and young adults aged 15-30.

Group Size: Up to 15 participants per session.

Duration: Approximately 3 hours.

Materials Needed:

- Flipchart and colourful markers
- Magazines with pictures and scissors
- Laptops, tablets or phones

Procedure:

1. Introduction to social awareness campaigns (30 minutes):

- Begin with an introduction to advocacy and self-advocacy terms.

- Continue with an introduction to social awareness campaigns and an overview of the importance of social awareness campaigns - highlight their impact on awareness raising, education and social change within the society.
- Show several examples of social awareness campaigns dedicated to cyber violence against women and ask participants to share the awareness campaigns they know of. Try to show campaigns involving different tools used.

2. Creating a social awareness campaign: preparation (30 minutes):

- Divide participants into small groups (3-4 people per group). Ask each group to choose a specific topic for a social media campaign focused on cyber gender-based violence. You can also provide them with several suggestions.
- Ask each group to formulate goal (s) for their awareness campaign and target group/future supporters (young people, elderly, general society, men or women, etc).
- Ask each group to think of a specific approach to the awareness campaign – whether it is going to be digital (online poster, video, social media posts, videos, etc.) or traditional media (e.g. poster, poem, song, billboard etc.). Emphasize on considering what type of awareness campaign approach would be most effective in engaging their target group/future supporters.

3. Creating a social awareness campaign: implementation (1 hour):

- Based on the considerations done in the preparation stage, each group works on developing their social awareness campaign. They can use online platforms to develop their campaigns, such as CANVA, or can create the campaign using the flipchart, colourful markers and magazines available.
- It is important not to limit participants' creativity – they can also choose to create a video, poem, song, mini theatre play, etc.

4. Group Discussion and Evaluation (40 minutes):

- Each group presents their awareness campaign.
- Feedback and constructive discussion on campaign effectiveness and potential improvements.

Debriefing:

- Summarize key insights
- Ask questions:
 - o What insights did you gain about advocacy and self-advocacy during the workshop?
 - o How do you envision using awareness campaigns for advocacy in your context?

- o What challenges do you anticipate in implementing awareness campaigns, and how might you overcome them?
- For anyone interested to learn more about awareness campaigns building, you can share the link to the manual [here](#) or any other material that you find useful.

Activity 3: Cyber Hygiene and Digital Well-being Workshop

Objective: To educate participants on digital hygiene practices and the importance of maintaining online well-being, empowering them to safeguard themselves and others from cyber violence.

Target Group: Youth and young adults aged 15-30.

Group Size: Up to 10 participants per session.

Duration: Approximately 120 minutes.

Materials Needed:

- Handouts or digital presentations on digital hygiene principles and online safety tips.
- Scenarios or case studies illustrating common digital threats (e.g., phishing, oversharing, insecure Wi-Fi usage).
- Interactive quizzes or activities related to digital hygiene practices.
- Materials for creating personal digital safety plans (notepads, pens, templates).
- Resources on self-care and setting online boundaries.

Procedure:

1. Introduction to Digital Hygiene (20 minutes):

- Start with an overview of what digital hygiene means and its importance in protecting against cyber violence
- .
- Discuss key aspects of digital hygiene such as strong passwords, two-factor authentication, software updates, data backup, and secure Wi-Fi usage.

2. Interactive Case Studies (30 minutes):

- Present participants with scenarios that depict common digital threats and risky behaviors.

- Facilitate group discussions on how these situations could be better handled using digital hygiene principles.
- 3. **Digital Hygiene Quiz or Activity (20 minutes):**
 - Conduct an interactive quiz or activity to reinforce the concepts of digital hygiene.
 - Include questions or tasks on identifying weak passwords, spotting phishing attempts, and best practices for online security.
- 4. **Creating Personal Digital Safety Plans (30 minutes):**
 - Guide participants in creating their own digital safety plans.
 - Include elements like setting strong passwords, regularly reviewing privacy settings, and establishing personal rules for online sharing and interactions.
- 5. **Discussion on Online Well-being (20 minutes):**
 - Discuss the importance of self-care and setting boundaries in the digital space to maintain mental and emotional health.
 - Share tips and strategies for dealing with online negativity, including when to disengage and seek support.

Debriefing:

- Summarize key learning points about digital hygiene and online well-being.
- Emphasize the role of personal responsibility in maintaining a safe and healthy digital presence.
- Provide information on resources for further learning and support in cases of cyber violence.

Activity 4: "Digital Self-Defense" Role-Playing Game

Objective: To engage participants in a role-playing game that simulates various online scenarios, teaching them how to apply digital self-defense strategies effectively.

Target Group: Youth and young adults aged 15-30.

Group Size: Up to 10 participants per session.

Duration: Approximately 120 minutes.

Materials Needed:

- Scenario cards depicting different online situations that could lead to cyber violence (e.g., receiving a phishing email, encountering a cyberbully, being asked for personal information online).
- "Digital Defense Toolkit" cards, each representing a specific digital safety practice or response strategy (e.g., using strong passwords, enabling two-factor authentication, not sharing personal info, reporting abuse).
- Rules and guidelines for the role-playing game.
- A scoreboard or tracking system to keep score during the game.

Procedure:

- 1. Game Setup and Rules Explanation (15 minutes):**
 - Briefly explain the concept of the game, which involves navigating various online scenarios and employing digital defense strategies. *Available in the ANNEX*
 - Distribute the scenario and toolkit cards to the participants and explain how to use them during the game.
- 2. Role-Playing Game Rounds (60 minutes):**
 - Participants draw scenario cards and role-play the situation described.
 - Other participants use toolkit cards to suggest practical strategies to handle the scenario.
 - Points are awarded based on the effectiveness and creativity of the strategies employed.
- 3. Discussion and Learning Points (30 minutes):**
 - After each round, discuss the scenario and the strategies used.
 - Highlight key learning points and best practices for each situation.
- 4. Wrap-Up and Reflection (15 minutes):**
 - Conclude the game and tally the scores.
 - Reflect on the importance of being prepared and proactive in digital self-defense.

Debriefing:

- Summarize the key digital self-defense strategies learned through the game.
- Emphasize the importance of being vigilant and knowledgeable about online safety.
- Provide resources for further learning and support in digital safety and cybersecurity.

7. Provision of psychological support to the victim

Objectives

- To understand the role of psychological support
- To discuss psychological impacts
- To introduce psychological strategies

7.1. Introduction

In an era increasingly dominated by digital interactions, the phenomenon of cyber violence has emerged as a significant societal issue. This chapter delves into the psychological support necessary for individuals affected by such violence. Cyber violence, encompassing a range of harmful online behaviors like cyberbullying, harassment, and digital abuse, can leave profound psychological scars. The importance of understanding, addressing, and mitigating these impacts cannot be overstated. This chapter aims to provide a comprehensive overview of psychological support mechanisms and strategies, highlighting their critical role in the recovery and empowerment of victims.

7.2 Theory

7.2.1. The Psychological Impact of Cyber Violence

Before delving into mechanisms and strategies for support of victims, it's important to have a full understanding of what impact cyber violence has on victims. A vast array of studies over the past decade has delved deeply into the consequences of cyber violence on its various participants: the perpetrators (often referred to as bullies), the victims, and those who find themselves in the dual role of both bully and victim. These studies cumulatively offer a nuanced understanding of the long-term adverse effects, with a particular focus on children and young people.

The comprehensive set of studies gathered over the past decade has probed the impact of cyber violence on perpetrators/bullies, victims, and those occupying the dual role of bully/victims. The synthesized findings offer a clear depiction of the long-term negative effects on children and young people.

The **psychological and emotional consequences** of cyber violence, as elucidated by Dredge et al. (2014) and Jang et al. (2014), represent a significant challenge, with manifestations including depressive symptomology, suicidal ideation, low self-esteem, anxiety, and loneliness. The study by Bauman et al. (2013) underscores the

link between cyber violence exposure and severe psychological outcomes, including suicidal thoughts and self-harming behavior.

Physical effects of cyber violence, such as weight fluctuations, substance abuse, headaches, abdominal pain, and sleeping problems, as highlighted by Gámez-Guadix et al. (2013) and Jang et al. (2014), underscore the broad-reaching impact on victims. Furthermore, increased school difficulties, reported by Cassidy et al. (2013) and Mishna et al. (2012), encompass school aggression, truancy, lower academic achievement, and a sense of unsafety.

The type, nature, and planning of cyberviolence incidents, as expounded by Menesini et al. (2011), influence the **psychological impact** on victims. Notably, incidents involving embarrassing pictures or videos are identified as particularly detrimental. Some findings from Wong et al. (2014) and Fletcher et al. (2014) suggest that **cyberbullies** experience more psychological difficulties and a poorer quality of life, despite their interactions with peers. The study by Bauman et al. (2013) highlights a direct relationship between cyberbullying perpetration and suicide attempts, particularly in males.

7.2.2. Psychological Support Techniques

Providing psychological support to victims of gender-based cyber violence demands an approach that is both sensitive and tailored, addressing the unique challenges and experiences associated with this specific form of online harassment.

Trauma-Informed Care

This approach to care is particularly relevant in the context of cyber violence, as it is predicated on the understanding and response to the widespread impact of trauma.

Key Components:

- **Safety:** This involves the creation of an environment where physical and emotional safety is paramount, fostering a sense of trust and minimizing the risk of re-traumatization. Ensuring secure and confidential spaces for individuals affected by cyber violence is crucial.
- **Trustworthiness and Transparency:** Building trust is achieved through clear and consistent communication. This includes providing comprehensive information about the support process, available resources, and any potential interventions.
- **Empowerment and Choice:** Central to this approach is the empowerment of individuals, allowing them to have a say and control over their recovery process. This involves actively involving them in decision-making processes and respecting their autonomy and choices.

- **Collaboration and Mutuality:** This principle emphasizes the importance of collaborative relationships between service providers and victims. It involves recognizing the expertise and experiences of the victim and working together to develop a supportive and effective plan.
- **Voice and Choice:** Prioritizing the voices and choices of survivors is key. Encouraging them to express their needs, preferences, and concerns is part of this process, involving active listening and a deep respect for their perspectives.
- **Cultural, Historical, and Gender Sensitivity:** This component involves adapting support strategies to respect the diverse cultural, historical, and gender-specific experiences and backgrounds of victims. It underscores the importance of a culturally sensitive approach in providing effective psychological support.

7.3.2 Counseling and Therapy

Counseling and therapy play a pivotal role in addressing the psychological effects of cyber violence. This can include various therapeutic modalities such as Cognitive Behavioral Therapy (CBT), which helps individuals reframe negative thought patterns, and Dialectical Behavior Therapy (DBT), which focuses on emotional regulation and interpersonal effectiveness.

- **Individual Counseling:** Tailored to address personal experiences of cyber violence, helping victims process their emotions and develop coping strategies.
- **Group Therapy:** Facilitates a shared healing experience, allowing individuals to connect with others who have faced similar challenges, fostering a sense of community and mutual support.

7.3.3 Support Groups and Peer Support

Support groups provide a safe space where victims can share their experiences and learn from others who have undergone similar challenges. Peer support, in particular, can be empowering, as it allows victims to see tangible examples of coping and resilience.

- **Moderated Groups:** These groups, led by mental health professionals, ensure a structured and safe environment for sharing and support.
- **Peer-led Groups:** Offers a more informal support setting, often led by individuals who have navigated their own journey through cyber violence.

7.3.4 Online Helplines and Chat Support

Digital support mechanisms, such as online helplines and chat services, provide accessible and immediate assistance. These platforms can be particularly effective for individuals seeking anonymous or immediate support.

- **24/7 Helplines:** Offer round-the-clock support, crucial for addressing urgent needs and crises.
- **Chat Services:** Provide a text-based support option, often preferred by those who are more comfortable expressing themselves in writing.

7.3.5 Education and Empowerment

Educational workshops and resources are crucial in empowering individuals to understand the nature of cyber violence and how to protect themselves online. This includes information on digital safety, privacy settings, and recognizing early signs of cyber abuse.

- **Workshops and Seminars:** Cover topics like digital literacy, online safety, and legal avenues for victims of cyber violence.
- **Resource Distribution:** Providing easy-to-access online resources, guides, and toolkits for self-help and awareness.

7.3.6 Crisis Intervention

In cases of acute cyber violence, immediate crisis intervention can be critical. This involves providing urgent psychological support, legal guidance, and ensuring the personal safety of the victim.

- **Emergency Counseling:** For immediate psychological stabilization in crisis situations.
- **Safety Planning:** Assisting victims in developing a plan to ensure their immediate and ongoing safety.

7.3.7 Cultural Sensitivity in Support

Acknowledging and respecting cultural nuances in the experience of cyber violence is vital. Psychological support should be culturally sensitive, recognizing how cultural background influences the experience and expression of trauma.

- **Culturally Tailored Counseling:** Adapting counseling techniques to align with the victim's cultural background and beliefs.
- **Training for Support Providers:** Ensuring that those providing support are educated about cultural competence and sensitivity.

7.3.8 Self-Care Techniques

Teaching and encouraging self-care techniques is crucial for helping victims manage the emotional toll of cyber violence. This includes strategies for stress management, mindfulness exercises, and relaxation techniques.

- **Mindfulness and Relaxation:** Techniques like meditation, breathing exercises, and mindfulness can help reduce stress and anxiety.
- **Stress Management Workshops:** Offering practical tips and strategies for managing stress in daily life.

7.3.9 Legal Support and Advocacy

Collaboration with legal professionals to inform and support victims regarding their legal options is crucial. Advocacy efforts can assist victims in navigating the legal system and seeking justice.

- **Legal Counseling:** Providing information about legal rights and options available to victims of cyber violence.
- **Advocacy Programs:** Assisting victims in advocating for their rights and seeking legal recourse.

7.3.10 Media Literacy and Digital Resilience Training

Workshops on media literacy and digital resilience are important for empowering individuals to navigate online spaces safely and confidently.

- **Digital Resilience Training:** Helping individuals develop skills to withstand and recover from cyber violence.
- **Media Literacy Education:** Teaching critical thinking skills related to digital media consumption and online interactions.

Best Practices

EU Kids Online Network

Overview

The EU Kids Online Network is a pan-European research network. It conducts extensive, multidisciplinary research focused on understanding children's online activities, the risks they encounter, and the safety measures that can protect them. This initiative has been pivotal in shaping policies and educational strategies across Europe.

Key Activities and Contributions

- **Comprehensive Research:** Conducts detailed studies on various aspects of children's online experiences, including exposure to cyber violence. This research provides insights into the prevalence, nature, and impact of online risks.
- **Policy Recommendations:** Based on research findings, the network offers tailored recommendations for policymakers. These suggestions aim to improve online safety legislation and practices, ensuring they are relevant and effective for protecting young internet users.
- **Educational Material Development:** The network collaborates with educators and stakeholders to develop educational materials and guidelines. These resources are designed to teach children about safe internet use and how to deal with cyber violence.
- **Parental Guidance:** Provides advice and resources for parents and guardians, helping them understand the digital environment and how they can support their children in navigating it safely.
- **International Collaboration:** Works with researchers across Europe, facilitating an exchange of knowledge and best practices. This collaborative approach enhances the understanding of cyber violence on a broader scale.

Safer Internet Centres (SICs) across Europe

Overview

Safer Internet Centres (SICs) are established across EU member states with the goal of making the internet a safer and better place for children and young people. These centers play a crucial role in both prevention and intervention regarding online safety issues, including cyber violence.

Key Activities and Contributions

- **Awareness Campaigns:** SICs conduct awareness campaigns targeted at children, parents, and educators. These campaigns focus on promoting safe internet use and understanding the risks associated with cyber violence.
- **Educational Resources:** Develop and distribute a wide range of educational materials. These resources are tailored to different age groups and address various aspects of online safety.
- **Helpline Services:** Offer helplines where children and teenagers can seek help and advice regarding online safety concerns, including experiences of cyber violence. These helplines provide a confidential and accessible support system.

- **Reporting Tools:** Provide tools and platforms for reporting illegal or harmful online content and behavior. This empowers users to take action against cyber violence and contributes to safer online environments.
- **Training for Professionals:** Conduct training sessions for teachers, social workers, and other professionals who work with children. These sessions equip them with the knowledge and skills to support young people in dealing with cyber violence.

In conclusion, this chapter provides an insightful exploration into the psychological impacts of cyber violence, highlighting its profound emotional, physical, and academic effects on victims, especially children and young people. It emphasizes the necessity of comprehensive psychological support mechanisms, including trauma-informed care, counseling, and culturally sensitive approaches. The chapter also sheds light on the challenges faced by perpetrators, advocating for a holistic view of cyber violence. Additionally, it underscores the importance of legal support, media literacy, and digital resilience training in empowering victims and preventing future incidents. Organizations like the EU Kids Online Network and Safer Internet Centres play pivotal roles in research, policy formation, and providing support, exemplifying collaborative efforts to combat cyber violence and enhance online safety.

Exercises

Activity 1: Empathy Building and Active Listening Workshop

Objective: To develop empathy and active listening skills among participants, enhancing their ability to provide psychological support to victims of cyber violence.

Target Group: Youth and young adults aged 15-30.

Group Size: Up to 10 participants per session.

Duration: Approximately 120 minutes.

Materials Needed:

- Scenario cards depicting various experiences of victims of cyber violence.
- Guidelines on active listening and empathy-building techniques.
- Role-play instructions and examples.
- Feedback forms for participants to evaluate their listening and empathy skills.
- Quiet and comfortable space conducive to open discussion and role-playing.

Procedure:

1. **Introduction to Psychological Support (20 minutes):**
 - Start with a brief overview of the importance of psychological support for victims of cyber violence.
 - Discuss key concepts of empathy and active listening, explaining how these skills are essential in supporting victims.
2. **Active Listening and Empathy Techniques (20 minutes):**
 - Present and demonstrate effective active listening techniques, such as maintaining eye contact, nodding, summarizing, and asking open-ended questions.
 - Discuss ways to show empathy, including understanding the victim's perspective and showing genuine concern and care.
3. **Role-Playing Activity (40 minutes):**
 - Divide participants into pairs and provide each pair with a scenario card.
 - Each pair engages in a role-play exercise where one person plays the role of the victim and the other the supporter.
 - The supporter practices active listening and empathy in response to the victim's experience.

4. Feedback and Discussion (30 minutes):

- After each role-play, partners provide feedback to each other using the feedback forms.
- Facilitate a group discussion, allowing participants to share their experiences and learnings from the role-plays.

5. Reflection and Application (10 minutes):

- Encourage participants to reflect on how they can apply these skills in real-life situations.
- Discuss the importance of providing psychological support in their communities or peer groups.

Debriefing:

- Summarize the key skills practiced during the workshop.
- Emphasize the value of empathy and active listening in supporting victims of cyber violence.
- Provide information on resources and support services for further training or for victims seeking help.

8. Legal guidance – Where and how to report online abuse

1 DIRECT ACTION

2 NATIONAL LEGISLATION OF EACH COUNTRY

Objectives

- To inform individuals and victim management bodies about the existing legislation at European Union level.
- Clarify the legislation in force in each of the Member States of the consortium on cyber violence
- Clarify how cyber violence is to be included in state legislation.
- Understand how much pressure is needed to recognise cyber violence as a separate form of violence in existing legislation.

Introduction

Certainly the intensive use of the internet creates new conditions for the manifestation of sexual harassment behaviour, as the internet is offered as a safer field for the perpetrator, in the sense that the lack of direct contact with the victim facilitates in many cases the commission of the offence (e.g. sending messages via facebook inviting the victim to intercourse or fornication). However, it is very important for each of us to know how much legislation at both state and European level protects the victim and in what way.

In general, a brief overview and reference to the legislation of the 28 EU accession countries shows the general absence of a defined legislative framework on gender-based violence online. Nevertheless, there are currently various ways of addressing cyber violence at EU level. This includes soft law and legislation applicable to online media and platforms as well as to crimes. Examples of relevant regulations include the General Data Protection Regulation (GDPR), the e-commerce regulation E-Commerce Directive, the Audiovisual Media Services Directive and the Code of Conduct on tackling illegal hate speech online (non-binding).

In the relevant literature, there is no separate definition of cyber violence, which makes it difficult to analyse the measures taken by Member States. Nevertheless, it is clear that Member States differ in their legislative approaches to combating gender-based cyber violence.

The result of the analysis of the Member States shows that criminal law provisions are used to address cyber-violence, although they are not specifically designed for this purpose. Four different types of legislation to address gender-based cyber violence were identified. Some Member States use a combination of the four approaches.

- Some Member States criminalise gender-based violence in cyberspace, e.g. Romania and France.
- Others criminalise specific types of cyber violence without addressing cyber gender violence. e.g. Belgium, the Czech Republic, Spain and France. (Exception: all Member States all Member States criminalise child pornography).
- On cyberbullying, Italy 37 deals with the protection of minors and some provisions of the Criminal Code can be used to combat cyber violence.
- On cyberbullying, Austria is in the lead.
- Hate speech without a gender-specific element is criminalised in Spain, The Netherlands, Bulgaria, Bulgaria, Greece, Croatia, Czech Republic, Portugal, Malta and the Netherlands.
- In a third category are Member States that use existing provisions that do not specifically address internet crimes. These countries include Germany, Spain, Finland, Finland and the Netherlands.
- Last, but not least, are those Member States working on the basis of non-criminal provisions. Germany, Lithuania and Ireland aim to prevent gender-based online cyber violence using this approach.

It is also particularly important to note that the 2020 motion for a resolution in the European Parliament on criminalising cyber violence took into account recommendations such as:

1. Recommendation on the objective of the directive to be adopted
2. Recommendation on the scope and definitions
3. Recommendation on prevention measures
4. Recommendation on the protection, support and compensation of victims
5. Recommendation on the prosecution and criminalisation of gender-based violence on the Internet
6. Recommendation on data collection and reporting

The recommendations contained in the annex to the resolution include the following elements: the objective of the directive; the scope and definitions; preventive measures; protection and support for victims and redress for them; prosecution and criminalisation of gender-based violence online; and data collection and reporting.

The aim of the Directive is to establish minimum rules on the definition of the crime of gender-based violence on the internet and the related sanctions, to establish measures to promote and support Member States' action in the field of prevention of this crime, as well as measures to protect and support victims and to ensure redress for them. The co-sponsors of this initiative consider that the EU lacks a legal framework for combating gender-based violence and, more specifically, gender-based violence on the Internet, as well as for the protection and support of victims.

As stated in the resolution, there are various definitions of gender-based violence online, but there is no internationally agreed legal definition. For this reason, the recommendation on scope and definitions leaves it to the Commission to propose a specific definition covering all forms of gender-based violence committed, facilitated or exacerbated in part or in full by the use of ICTs, against women because they are women, or disproportionately affecting women. This proposal is based on the definition used by the UN Special Rapporteur on violence against women in her 2018 report on cyber violence.

In order to protect and support victims of gender-based violence online, the proposal first indicates which categories of victims should be taken into account. The aim is to be as comprehensive as possible, taking into account the intersectionality and specific needs of victims. The proposal then includes various actions to implement protection and support for victims. Particular emphasis is placed on the need to improve and facilitate reporting, and to avoid secondary victimization. Training for legal practitioners and professionals who will come into contact with victims is crucial to achieving this objective.

The text discusses different behaviors that should be considered as offenses in the context of gender-based violence on the internet. It suggests adding cyberbullying, persistent internet stalking, ICT-related privacy violations, remote manipulation or surveillance, threats, sexist hate speech, inducing suicidal or anorexic behavior and trauma behaviors, computer damage, and illegal access to mobile phones and electronic devices to the list of offenses. The proposed offenses include various actions such as downloading explicit content without consent, accessing and sharing personal data or images without consent, manipulating personal data or images, remotely spying on individuals through mobile devices, making direct threats or threats of violence or coercion, engaging in sexist hate speech and violent content, inducing harmful behaviors, causing damage to files and programs, attacking websites, and illegally accessing electronic devices. These behaviors are considered as forms of gender-based violence on the internet.

BULGARIA

Bulgaria accepted a Cybersecurity law in 2018, which addresses various aspects of cybersecurity, including the organization, management, and control of cybersecurity activities, countermeasures against cybercrime, and the establishment of high levels of network and information security. The law also defines the powers and functions of competent authorities in the field of cybersecurity. It covers measures for network and information security, the scope of application including administrative bodies and operators of essential services, and exclusions from the law's application. The law emphasizes the creation and maintenance of a cybersecurity system as part of national security, the establishment of a Cybersecurity Council, and roles and responsibilities of various ministries and agencies in ensuring cybersecurity.

You can read the law (in Bulgarian) over [here](#).

This law does not specifically address cyber gender-based violence, nor cyberbullying, however - the structure responsible for these and other cyber crimes is the Cybercrime division of the Ministry of the Interior's [General Directive for fighting organized crime](#).

On the topic of gender-based violence, the [Bulgarian Protection Against Domestic Violence Act](#), adopted in 2005, acknowledges domestic violence as a public concern rather than a private matter. It introduces a unique civil procedure for domestic violence cases, incorporating elements of criminal procedure while remaining within civil law, making the burden of proof more favorable to the victim. In 2016, Bulgaria adopted the Law on Equality between Women and Men, which sets out the principle of equality as a coordinated state policy. This law aims to ensure gender equality in all spheres of life and includes measures to combat violence against women.

Additionally, specifically in the context of youth, the National Programme for Prevention of Violence and Abuse of Children 2017-2020 and the Action Plan for its implementation (2017-2018) set the prevention of all forms of violence against children (physical, emotional, sexual) in all settings (homes, schools, alternative care institutions, digital environment, penal institutions) as a priority for the government. The action plan lays out the different structures and procedures, as well as resources – both human, facilities and financial for its implementation.

CYPRUS

The main laws in the field of cybercrime in Cyprus are:

1. The Law ratifying the Convention on Cybercrime (Budapest Convention), L.22(III)/2004. This legislation covers hacking, child pornography and fraud committed via electronic communication and the Internet.

2. The Law that revises the legal framework on the prevention and combating the sexual abuse and sexual exploitation of children and child pornography, L 91(I)/2014. This legislation ratifies the EU Directive 2011/93/EE and covers child pornography, grooming and notice and takedown.
3. The Law ratifying the Additional Protocol to the Convention on Cybercrime, concerning the Criminalization of Racist and Xenophobic acts, L.26(III)/2004. This legislation covers racism and xenophobia via computer systems and the Internet.
4. The Law on the Processing of Personal Data, L.138(I)/2001.
5. The Law on the Retention of Telecommunication data for the investigation of serious offences, L. 183(I)/2007. This legislation transposed Directive 2006/24/JHA. Although the Directive was invalidated by the Court of Justice of the EU, the national law is still valid. The national law is founded on a constitutional provision and it includes specific safeguards for the protection of privacy; for example, communication data are released only following a court order.
6. Law 112(I)/2004 Regulating Electronic Communication and Postal Services.
7. Law implementing Directive 2013/40/EU on attacks against information system, 147(i)/2015.

The National Cybersecurity Strategy was also adopted by the Ministerial Council. The Office of the Commissioner of Electronic Communications and Postal Regulations is responsible for its monitoring and implementation.

Furthermore, the use of the Safe Internet Centre and Digital Technologies, promoted by the Ministry of Education and Culture, has been suggested within the framework of the National Strategy for research and training purposes in the field of criminal justice.

Cyprus has put a great emphasis on prevention and awareness-raising. Thus, partnerships were established between public sector (Ministry of Education and Culture through the Cyprus Pedagogical Institute) and the private sector, through the Industry (e.g. ISPs), non profit organisations (e.g. Cybersafety, Hope for Children, CNTI), organised groups (School for Parents) which are contributing with enthusiasm in awareness and prevention programmes.

CZECH REPUBLIC

Neither cyberviolence, nor gender-based cyberviolence has a specific place as a separate legal regulation in Czech legislation. However, the Czech law contains a number of provisions that can possibly cover gender-based cyberviolence:

Bullying (resp. cyberbullying) is defined by Act No.198/2008 Coll. on equal treatment and legal means of protection against discrimination and on amendments to certain acts (Anti-Discrimination Act)

Stalking (resp. cyberstalking) - section Nr. 453 of the Penal Code defines stalking as dangerous persecution which can cause the victim fear for life or health or for the life and health of persons close to him/her.

Hate speech - violence (incl. verbal attacks and threats) against a group of people or against an individual is defined as an offence by § 352 of the Criminal Code. Defamation of a nation, race, ethnic or other group of persons is defined by § 355 of the Criminal Code. Incitement to hatred against a group of persons or to restriction of their rights and freedoms is defined in § 356 of the Criminal Code.

Sexual violence⁷ is included in Czech law among sexual and moral offences, crimes listed in particular in the Criminal Code in Articles 185-193b). This group includes in particular the following offences: threatening freedom of sexual decision-making (rape and sexual coercion), threatening the moral and physical development of children (e.g. sexual abuse, enticing a child to have sexual intercourse and using a child to produce pornography), threatening moral principles (e.g. production and other disposal of child pornography, pimping). The offense of trafficking in human beings for the purpose of sexual exploitation or production of pornography may also be included. Gender-based sexual online violence can in some cases be prosecuted in relation to these crimes, or assessed as crimes such as extortion or the offence of enticement to sexual intercourse (cybergrooming; Article 202 of the Criminal Code).

REPUBLIC OF CROATIA

Since 1991, Croatia has been a signatory to the UN Convention on the Elimination of All Forms of Discrimination Against Women, which seeks to oblige the signatory states to act against discrimination against women and for the equal position of women and men.

It is also a signatory to the Council of Europe Convention on preventing and combating violence against women and domestic violence, better known as the Istanbul Convention.

⁷ <https://www.policie.cz/clanek/sexualni-a-mravnostni-trestne-ciny.aspx>

In Croatia, the Criminal Code does not have clearly defined sections that refer exclusively to CGBV. However, it has parts related to protection against domestic violence, which foresees a prison sentence for perpetrators who "severely violate the regulations on protection against domestic violence and thereby cause a family member or a close person to fear for his or her safety or the safety of those close to him or puts her in a humiliating position or a state of long-term suffering, and thus a more serious crime is not committed".

It also recognizes as a criminal offense intrusive behavior that includes stalking and unwanted contact. This crime includes cyberstalking. The latest amendment to this law includes revenge pornography, as well as doxing. This law stipulates that defamation is a criminal offense, and stricter penalties are provided for defamation through the media. Sexual harassment is also a criminal offense, as well as public incitement (hate speech), which can take place over the Internet, to hatred and violence against different minorities, including gender minorities. Part of gender-based violence is also covered by the Act on protection against domestic violence, under the definition of psychological violence that causes a violation of dignity or distress in the victim.

There are different protocols of action that can be partially applied in the case of CGBV - the protocol of action in the case of violence among children and young people, in the case of sexual violence, and in the case of hate crimes.

Greece

By Law No. 4531/2018 the **Istanbul Convention** was ratified and incorporated into the Greek legal order. Among other things, Article 34 of the Convention calls on its States Parties to criminalise stalking or, as translated into Greek, "non-obvious surveillance or harassment/harassing surveillance". Subsequently, and in order to comply with the Convention, the first paragraph of Article 333 of the Criminal Code was amended to include the offence of Stalking manifested through the use of electronic media and the internet, taking the form of Cyber Stalking.

This is undoubtedly an extremely innovative development for Greek standards. The offences in question take the form of a misdemeanour and their potential perpetrators are threatened with a prison sentence of up to one year or a fine. For the time being, there is no relevant national case law defining the case law of cyber stalking.

However, by interpreting the letter of the law somewhat broadly, we could cite illustrative examples. A key element of the object of the offence is that the harassing conduct must knowingly be unwanted by the offender and create fear or anxiety for the victim, e.g. a. by sending continuous unwanted e-mails - either by e-mail or social

media; b. by persistent and also unwanted requests for friendship. Interesting in any case is the definition and case study of the offence of cyber stalking as set out under English law: "Stalking can take place on the Internet and by email. This is known as 'cyber stalking'. Indeed it may involve the use of social networking sites, chat rooms and other forums facilitated by technology. The Internet can be used for various purposes related to stalking, such as:

- The identification of the victim's personal details.
- Contacting the victim.
- Monitoring the victim.
- The theft of the victim's identity information, such as registering for services, purchasing goods and services in the victim's name.
- Defamation of the victim.
- Electronic sabotage such as spamming and sending viruses.
- Deceiving other internet users to harass or threaten a victim."

Furthermore, as far as sexual harassment is concerned, it was only in 2006 that it became a criminal offence in Greece. Previously other provisions filled the gap. A typical example is Article 361 of the Penal Code on insult. Today, the criminal provisions relating to sexual harassment are contained in Article 337 par. 1 CC (insult to sexual dignity). According to what is defined therein, the offence of sexual harassment is committed when a person insults the dignity of another person in the sphere of sexual life very seriously with proposals that may be either in the form of explicit statements or gestures and that involve the performance of sexual acts without physical contact.

The term 'sexual intercourse' has the meaning of intercourse and any act of equal importance to it, e.g. 'sexual intercourse', hetero masturbation, pederasty, pederasty and promiscuity or the use of substitutes. The crime of sexual harassment is also a misdemeanor and is punishable by up to one year in prison or a fine, as is Stalking/Cyber Stalking. According to the statistics of the official website of the Hellenic Police in 2019, only 39 people were arrested for offences falling under the jurisdiction of the Cybercrime Unit, including none for committing sexual harassment via the internet.

Good practices:

We have collected some practices from various EU countries that are useful for the legal guidance of victims of CGBV

- The STOP online, operated by the National Security Team, is a pivotal initiative in the fight against illegal online content. This hotline allows users to report

content that raises suspicion or is clearly illegal, such as child pornography, child abuse, inappropriate child nudity, or cyber grooming. The effectiveness of this hotline lies in its accessibility and responsiveness, providing a direct channel for the public to aid in the detection and prevention of online abuses. By enabling swift reporting, the hotline plays a crucial role in the early intervention and potential prevention of cybercrimes.

- Justýna Help Center serves as a sanctuary for individuals who face various forms of bias crimes and hate speech, including racism, antisemitism, islamophobia, homophobia, transphobia, and other forms of gender-based violence. Their approach is comprehensive, offering free support to those affected by violence due to age, health condition, social status, or belonging to a particular subculture. The center's work is critical in providing immediate support to victims, while also working towards broader societal change through awareness and education. (www.matesvaprava.cz)
- Chat help line Persefona - is an innovative approach to supporting survivors of sexual violence and those in abusive intimate relationships. This service also extends its support to issues like child pornography, providing a confidential and accessible platform for victims to seek help. The anonymity and immediacy of a chat help line can be particularly effective for victims who might hesitate to seek help in more traditional settings, thereby bridging a crucial gap in support services.
- The Czech non-profit Konsent plays a critical role in the Czech Republic by focusing on prevention, awareness, and education in the field of sexualized violence. Their work extends to providing resources for victim-support organizations and educators, as well as directly assisting survivors of sexualized violence and online gender-based violence. One of their key campaigns is to redefine the legal definition of rape to emphasize consent, signaling a significant shift towards a more victim-centric approach in the legal system.
- #spasime movement (spasi me = save me)

Prominent (female) members of public scene in Croatia like actress Jelena Veljača have started movement #spasime . They have used their fame to raise the awareness of domestic violence and violence against women and to organize protests against violence. After those protests, the Prime minister received a delegation who advocated changes in legislation. One member of #spasime initiative Una Zečević Šeparović (lawyer) became a member of the

work group who proposed changes in Criminal code. One of the changes is including revenge porn as a crime act and those who commit that crime could face up to three years in prison . Their newest initiative aims to include femicide as a specific crime in Croatian Criminal code. They co-founded Croatian Women's Fund with the leading role of SOLIDARNA - Foundation for Human Rights and Solidarity.

9. Conclusion

Drawing this training curriculum to a close, we reflect critically on the landscape of Cyber Gender-Based Violence (CGBV) and the multifaceted strategies outlined to combat it. This curriculum, traversing through the complexities of legal frameworks, psychological impacts, and preventive measures, underscores a stark reality: the digital world, while a frontier of innovation and connectivity, is also a breeding ground for new forms of violence and abuse.

The persistent rise of CGBV highlights a significant gap in our collective digital literacy and societal norms. While technological advancements have leapfrogged, our understanding of digital ethics, empathy, and respect lags behind. This disconnect not only perpetuates existing forms of abuse but also paves the way for new ones. The curriculum emphasizes that combating CGBV is not just about reactionary measures but also about fostering a digital culture rooted in respect and dignity.

Critically, the curriculum points to a concerning inconsistency in legal responses to CGBV across different jurisdictions. While some regions have robust laws protecting individuals from online abuse, others have gaping legislative voids. This disparity not only hinders effective cross-border cooperation but also leaves many victims without recourse. The curriculum advocates for harmonized legal frameworks that can adapt to the fluid nature of the internet, offering comprehensive protection against online abuse globally.

Another critical issue addressed is the role of internet platforms and technology companies. Their policies and algorithms often dictate what is permissible online. However, there's a growing concern that these entities, driven by profit and scalability, are inadequately equipped or motivated to address the nuances of CGBV. The curriculum calls for greater accountability and transparency from these digital giants, urging them to be active participants in safeguarding their users.

On the flip side, the curriculum highlights exemplary practices from various EU countries, showcasing that change is possible and effective. Initiatives like the STOP online hotline, Justyna Help Center, and the #spasime movement demonstrates the power of proactive measures, community involvement, and legislative advocacy in creating safer digital spaces. These examples serve as beacons of hope and blueprints for action.

However, a critical gap remains in the collective societal response to CGBV. Too often, the responsibility of prevention and action falls on the victims. This curriculum challenges us to shift this paradigm, advocating for a community-driven approach where every internet user, policy-maker, educator, and tech company is a stakeholder in combating CGBV. It calls for a cultural shift towards collective responsibility, where

combating online abuse is not just a reactive measure, but a foundational aspect of our digital existence.

In conclusion, this curriculum is more than an educational tool; it's a call to arms in the fight against CGBV. It demands a critical reassessment of our digital behaviors, a unified legislative approach, corporate accountability, and a societal commitment to fostering a safer, more respectful online world. The path ahead is complex, but with collective effort, commitment, and the guidance provided in this curriculum, a safer digital future is within our reach. Let's embrace this challenge, not just as a necessity but as a responsibility to current and future digital citizens.

10. ANNEX

Chapter 2 - Activity 1 Scenarios :

Scenario 1: Cyber Grooming

- **Characters:**
 - Alex (Victim): A 16-year-old high school student.
 - Pat (Groomer): An online persona who gains Alex's trust.
- **Setting:** Online messaging platform.
- **Script Template:**
 - **Introduction:** Pat starts by commenting on Alex's public posts, gradually initiating private conversations.
 - **Building Trust:** Pat shows interest in Alex's hobbies and problems, becoming a confidante.
 - **Boundary Crossing:** Slowly, Pat starts asking more personal questions and requests pictures, initially innocent but gradually more inappropriate.
 - **Recognition of Grooming:** Alex starts feeling uncomfortable with the requests but is conflicted due to the established trust.
 - **Conclusion:** The role-play should end before any explicit content is requested or shared. Focus on the realization and internal conflict experienced by Alex.
- **Safety Measures:**
 - No actual sharing of personal information or photos.
 - Focus on the emotional aspect rather than the explicit content.
 - End the role-play at the point of recognition, not progression.

Scenario 2: Sexting

- **Characters:**
 - Jordan (Victim): An 18-year-old college student.
 - Chris (Peer): A classmate of Jordan.
- **Setting:** Text messages.
- **Script Template:**
 - **Initiation:** Chris compliments Jordan and gradually shifts the conversation to intimate topics.
 - **Request for Photos:** Chris asks for intimate photos, promising they will remain private.

- **Pressure and Doubt:** Jordan feels unsure and pressured but also trusts Chris.
- **Decision Point:** Jordan decides whether to send the photos. (Note: The decision should not be enacted; instead, focus on the thought process and conflict.)
- **Conclusion:** Discuss the potential consequences and feelings involved without enacting the sending of photos.
- **Safety Measures:**
 - Avoid graphic descriptions or enactments.
 - Concentrate on emotional conflicts and decision-making processes.

Scenario 3: Online Harassment

- **Characters:**
 - Sam (Victim): A 20-year-old social media user.
 - Riley (Harasser): An anonymous online account.
- **Setting:** Social media platform.
- **Script Template:**
 - **Onset:** Riley starts posting negative comments on Sam's posts.
 - **Escalation:** The comments become more frequent and hateful, including threats.
 - **Impact on Victim:** Show Sam's emotional reaction and coping mechanisms.
 - **Seeking Help:** Sam considers reporting to the platform or seeking advice.
 - **Conclusion:** Focus on the steps to address harassment without portraying extreme distress.
- **Safety Measures:**
 - Use fictional but realistic comments that are not overly graphic or triggering.
 - Emphasize Sam's response and support mechanisms.

Scenario 4: Catfishing

- **Characters:**
 - Taylor (Victim): A 22-year-old who enjoys meeting new people online.
 - Alex (Catfisher): Someone posing with a fake identity.
- **Setting:** Online dating platform.
- **Script Template:**
 - **Connection:** Taylor and Alex connect online, sharing interests and chatting regularly.

- **Deepening Relationship:** The relationship appears to grow, with plans to meet up.
- **Discovery:** Taylor discovers inconsistencies in Alex's stories or pictures.
- **Confrontation and Realization:** Taylor confronts Alex, leading to the revelation of the deception.
- **Conclusion:** Focus on Taylor's reaction to the betrayal and steps to move forward.
- **Safety Measures:**
 - Prioritize the emotional journey over the details of the deception.
 - Do not enact detailed lies or manipulative tactics.

Chapter 2 - Activity 3 - Story Prompts

Story Prompt 1: Cyberstalking

- **Scenario:** Nikos, a university student in Greece, starts receiving persistent and personal anonymous messages online, making them feel increasingly unsafe.

Story Prompt 2: Non-consensual Image Sharing

- **Scenario:** Maja, a young adult in Croatia, shares a personal photo with a friend, which is then shared online without her consent, leading to public shaming and ridicule.

Story Prompt 3: Identity Theft

- **Scenario:** Eleni, living in Cyprus, finds out someone is using her identity online to solicit money and spread false information, causing reputational damage.

Story Prompt 4: Hate Speech

- **Scenario:** Ivan, a Bulgarian advocating for minority rights, faces online hate speech, affecting his mental well-being and safety concerns.

Story Prompt 5: Technology Misuse for Control

- **Scenario:** Petra, in the Czech Republic, experiences her partner using technology to monitor and control her actions, like tracking her location, leading to feelings of entrapment and fear.

Story Prompt 6: Xenophobia and Hate Speech Online

- **Scenario:** Dimitris, a Greek belonging to a minority ethnic group, encounters xenophobic insults and hate speech on a social network, causing distress and a sense of isolation.

Story Prompt 7: Sexism in Online Spaces

- **Scenario:** Ana, a Croatian active in online gaming communities, faces persistent sexism and gender-based harassment, affecting her confidence and participation in these communities.

Story Prompt 8: Fatshaming on Social Media

- **Scenario:** Stavros, a young adult from Cyprus, becomes a target of fatshaming on social media, leading to embarrassment and a negative self-image.

Story Prompt 9: LGBTQ+ Online Hate

- **Scenario:** Georgi, an openly LGBTQ+ individual in Bulgaria, receives hateful messages and threats based on their sexual orientation, leading to anxiety and fear for their safety.

Story Prompt 10: Toxic Online Communities

- **Scenario:** Katerina, from the Czech Republic, becomes involved in an online community that promotes harmful stereotypes and behaviors, leading to negative influences on her beliefs and actions.

Chapter 3 - Activity 1 Interactive Prevention Strategy Development

Primary Prevention Principles

- **Objective:** To prevent the occurrence of cyber GBV before it happens.
- **Focus:** Addressing the root causes and risk factors associated with cyber GBV.
- **Key Strategies:**
 - **Education and Awareness:** Raising awareness about what constitutes cyber GBV and its effects. This includes educating people about respectful online behaviors and gender equality.
 - **Targeting At-Risk Groups:** Developing specific programs for groups most at risk of experiencing or perpetrating cyber GBV, such as people in intimate relationships, public figures, and those with prior experience of gender-based violence.
 - **Community Engagement:** Involving various community stakeholders in promoting a safe digital environment and challenging gender stereotypes and norms that contribute to GBV.

Secondary Prevention Principles

- **Objective:** To intervene after an incident of cyber GBV has occurred but before it escalates or becomes chronic.
- **Focus:** Early detection and timely response to incidents of cyber GBV.
- **Key Strategies:**
 - **Training on Recognition and Response:** Educating the community on how to recognize signs of cyber GBV and providing guidance on appropriate responses.
 - **Support Services:** Establishing accessible support services for victims, including counseling, legal advice, and reporting mechanisms.
 - **Bystander Intervention:** Empowering bystanders to recognize and safely intervene in situations where cyber GBV is occurring or likely to occur.

Tertiary Prevention Principles

- **Objective:** To minimize the long-term consequences of cyber GBV and prevent reoccurrence.
- **Focus:** Comprehensive support for victims and appropriate interventions for perpetrators.
- **Key Strategies:**
 - **Crisis and Long-term Support:** Providing immediate crisis intervention and ongoing support to victims, including psychological counseling and advocacy.
 - **Legal and Policy Measures:** Implementing legal actions against perpetrators and advocating for policies that protect victims and hold perpetrators accountable.
 - **Rehabilitation Programs:** Developing programs for perpetrators to address and change their abusive behaviors.

Chapter 5 - Activity 2

1. Cognitive Behavioral Therapy (CBT)

- **Description:** CBT focuses on changing negative thought patterns and behaviors. It helps individuals recognize and alter distorted perceptions they may have of themselves and others, leading to better emotion regulation and reduced aggressive behavior.
- **Interactive Element:** A short quiz or activity to identify negative thought patterns and ways to reframe them positively.

2. Motivational Interviewing

- **Description:** This approach encourages individuals to find their internal motivation to change. It involves open-ended questions and active listening to help perpetrators understand the impact of their actions and motivate them toward change.
- **Interactive Element:** Role-play scenarios where participants practice asking open-ended questions to understand motivations.

3. The Duluth Model

- **Description:** This model focuses on gender equity and social change. It teaches that violence is a learned behavior rooted in societal norms, and it can be unlearned by promoting respectful and non-violent relationships.
- **Interactive Element:** A matching game with cards that show examples of respectful versus disrespectful behaviors.

4. Anger Management

- **Description:** This approach teaches individuals how to recognize signs of anger and use strategies to manage it. It involves learning stress reduction techniques, communication skills, and ways to solve problems peacefully.
- **Interactive Element:** A stress-management activity, like deep-breathing exercises or a simple guided meditation.

5. Narrative Therapy

- **Description:** Narrative therapy involves separating the person from the problem and rewriting their life story. It helps perpetrators see how their actions are influenced by broader societal narratives and choose more positive narratives for their lives.
- **Interactive Element:** A creative writing exercise where participants write short stories from a perspective of positive change.

6. Trauma-Informed Care

- **Description:** This approach recognizes that many perpetrators have histories of trauma. It focuses on understanding past trauma's role in current behavior and addresses it in a safe, supportive environment.
- **Interactive Element:** An anonymous 'wish box' where participants can write down a trauma-informed support they think would be helpful.

7. Restorative Justice

- **Description:** This approach involves perpetrators understanding the harm they have caused and finding ways to make amends. It focuses on the needs of the victims, community, and perpetrators, promoting healing and reconciliation.
- **Interactive Element:** A group discussion or activity on the concept of making amends and understanding the impact of one's actions.

Chapter 6 - Activity 1

These are examples of the ideas for case studies, each focusing on a specific principle of persuasion. Based on these suggestions you can develop case studies or use real-life examples, making them more relatable to your participants.

Reciprocity:

Case Study: The Unwanted Gifts

A young woman receives unsolicited explicit images from an unknown sender. The sender later requests intimate images in return. The victim, feeling pressured, may comply to avoid potential harm or harassment.

Consistency:

Case Study: Manipulative Online Relationships

An individual, posing as a friendly acquaintance online, engages the target in conversations that gradually escalate, and the victim reveals some personal information and secrets. By building a virtual relationship, the perpetrator gains the victim's trust, making it more challenging for the victim to break away or report the harassment.

Social validation:

Case Study: Targeted Online Shaming

A group of individuals starts spreading false rumours about a person's personal life through social media. As others join in commenting or sharing the content, the victim experiences negative emotions, leading to increased isolation and emotional distress.

Authority:

Case Study: Impersonation and Manipulation

An individual with a fake LinkedIn profile claims to represent a renowned company. Posing as a recruiter, they pressure female job seekers to share personal information and participate in inappropriate video interviews, leveraging the perceived authority of the organization.

Liking:

Case Study: Online Impersonation through Flattery

A perpetrator impersonates a popular social media influencer admired by the victim. Using compliments and flattery, the impersonator convinces the victim to share personal photos and information, exploiting the principle of liking for malicious purposes.

Scarcity:

Case Study: False Threats of Exposure

Perpetrators gain access to compromising photos of an individual and threaten to release them publicly unless the victim complies with their demands within an hour. The perception of scarcity, where the victim believes they have limited time to prevent harm, increases the pressure to comply.

Unity:

Case Study: Cyberbullying through Group Dynamics

A high school student becomes the target of a coordinated online attack by a group of classmates. They use derogatory language, create fake profiles, and share offensive content, exploiting the principle of unity to amplify the impact on the victim's mental well-being.

Chapter 6 - Activity 3

Scenario Cards

1. Phishing Email:

- Description: "You receive an email that appears to be from a popular social media site asking you to confirm your password and username due to a security breach."
- Key Point: Recognizing phishing attempts.
- 2. **Cyberbullying Encounter:**
 - Description: "Someone starts posting hurtful and threatening messages on your social media page."
 - Key Point: Dealing with online harassment.
- 3. **Personal Information Request:**
 - Description: "A new online friend you met in a gaming chat room starts asking for personal information like your home address and phone number."
 - Key Point: Safeguarding personal information.
- 4. **Insecure Public Wi-Fi:**
 - Description: "You're at a café and connect to an open Wi-Fi network to check your email and social media accounts."
 - Key Point: Risks of using unsecured Wi-Fi networks.
- 5. **Suspicious Download Link:**
 - Description: "You receive a message with a link to download a free version of a popular paid game."
 - Key Point: Avoiding unsafe downloads and software.
- 6. **Oversharing on Social Media:**
 - Description: "You're considering sharing details about your upcoming vacation, including dates and locations, on your social media."
 - Key Point: The risks of oversharing online.

Digital Defense Toolkit Cards

1. **Strong Password Creation:**
 - Description: "Use a combination of letters, numbers, and symbols in your passwords. Avoid common words and personal information."
 - Applicable Scenarios: Phishing Email, Personal Information Request.
2. **Enable Two-Factor Authentication:**
 - Description: "Add an extra layer of security to your accounts by enabling two-factor authentication."
 - Applicable Scenarios: Phishing Email.
3. **Recognize and Report Bullying:**
 - Description: "Learn how to recognize cyberbullying and use platform tools to report and block harassers."
 - Applicable Scenarios: Cyberbullying Encounter.
4. **Use Secure Networks:**

- Description: "Avoid conducting sensitive activities over unsecured public Wi-Fi networks."
 - Applicable Scenarios: Insecure Public Wi-Fi.
5. **Beware of Suspicious Links:**
- Description: "Do not click on links or download files from unknown sources. Verify authenticity before proceeding."
 - Applicable Scenarios: Suspicious Download Link.
6. **Mindful Sharing:**
- Description: "Think before you post. Avoid sharing sensitive personal information and consider the long-term impact."
 - Applicable Scenarios: Oversharing on Social Media.

Game Setup

- **Number of Players:** Ideal for groups of 4-10 participants.
- **Game Flow:** Each round, a participant draws a scenario card and reads it aloud. Other players suggest strategies using their toolkit cards. The facilitator or group then discusses the effectiveness of each strategy and awards points based on creativity and practicality.
- **Scoring System:** Points can be awarded for effective strategies, creative solutions, and correct identification of risks.

Chapter 7 - Activity 1

Scenario Card 1: Online Harassment

- **Situation:** "Ivana, a high school student in Croatia, has been receiving a series of aggressive and threatening messages on social media from an anonymous account."

Scenario Card 2: Cyberbullying at School

- **Situation:** "Dimitar, a college freshman in Bulgaria, is being ridiculed and mocked on a popular student forum for their appearance and academic performance."

Scenario Card 3: Revenge Porn

- **Situation:** "Elena, a young adult in Greece, discovers that an ex-partner has shared private photos of her online without consent, leading to public shaming."

Scenario Card 4: Identity Theft

- **Situation:** "Andrei has recently found out that someone has been using their identity to post offensive content online, damaging their reputation in Romania."

Scenario Card 5: Doxxing

- **Situation:** "Luka, an avid gamer in Serbia, becomes a target of doxxing, where their personal information, including their home address, has been leaked on a gaming forum."

Scenario Card 6: Discriminatory Abuse

- **Situation:** "Petra, who openly identifies as LGBTQ+ in Slovenia, is facing derogatory and homophobic comments on their blog and social media pages."

Scenario Card 7: Cyberstalking

- **Situation:** "Maja, a young professional in Bosnia and Herzegovina, is being followed and contacted incessantly online by someone they met briefly at a networking event."

Scenario Card 8: Social Media Manipulation

- **Situation:** "Nikola, a teenager in North Macedonia, is struggling with a drastic decrease in self-esteem due to constant exposure to manipulated images and unrealistic standards on social media."

Instructions for Role-Play:

- One participant takes the role of the victim as described in the scenario.
- The other participant assumes the role of a friend, family member, or counselor providing support.
- The supporter should practice active listening and empathy, responding to the victim's experience with understanding and care.

Updated Bibliography

1. Adikari, N. (2016). Cyber violence crimes against women and girls. Proceedings of the Second Conference on Women's Studies, 1, 2-4. Retrieved from <https://www.academia.edu/>
2. AIContentfy Team. (2023). Designing effective awareness programs: Strategies for maximum impact. Retrieved from <https://aicontentfy.com/en/blog/designing-awareness-programs-strategies-for-maximum-impact>
3. Brody, S. (2020). Gender-inclusive children's literature as a preventative measure: Moving beyond a reactive approach to LGBTQ+ topics in the classroom. Occasional Paper Series, (44), 7.
4. Ceia, V., Nothwehr, B., & Wagner, L. (2021). Gender and technology: A rights-based and intersectional analysis of key trends.
5. Cesar, S. (Ed.). (2021). Elektroničko seksualno i rodno uvjetovano nasilje u mladenačkim vezama - priručnik za nastavnike i nastavnice. Zagreb: Centar za edukaciju, savjetovanje i istraživanje.
6. Cesar, S., Horváth, É., Kallós, L., Andras, R., Vives, E. P., Ileš, M., Ignjatović, T., & Bijelić, N. (2019). AUTONOMNI ŽENSKI CENTAR (AWC), Beograd, Srbija. Retrieved from <https://api.ps-cgbv.eu/media/file/637d151844d4c.pdf>
7. Cognitive Behavioural Group Therapy for Male Perpetrators of Intimate Partner Violence: A Systematic Review. Retrieved from <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC/>
8. Crooks, C. V., Goodall, G. R., Hughes, R., Jaffe, P. G., & Baker, L. L. (2007). Engaging men and boys in preventing violence against women: Applying a cognitive-behavioral model. *Violence Against Women*, 13(3), 217-239.
9. Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA.

10. Dunn, S. (2020). Technology – facilitated gender – based violence: An overview. Centre of International Governance Innovation. Retrieved from <https://scholar.google.com/>
11. European Institute for Gender Equality. (2022). Combating cyber violence against women and girls. Retrieved from <https://eige.europa.eu/publications-resources/publications/combating-cyber-violence-against-women-and-girls>
12. Fatem – Zahra, A. (2018). Revenge porn: The dangers of hyperreality and gendered cyberviolence. IIS Brief, Issue 2. Retrieved from <https://www.academia.edu/>
13. Fernandes, M., Lomba, N., & Navarra, C. (2021). Combating gender-based violence: Cyber violence.
14. Fisher, D., Lang, K. S., & Wheaton, J. (2010). Training professionals in the primary prevention of sexual and intimate partner violence: A planning guide. Atlanta, GA: Centers for Disease Control and Prevention.
15. Flanery, C. J. (2023). Prevention at the university level. In Facing campus sexual assault and relationship violence with courage: A guide for institutions and clinicians on prevention, support, and healing (p. 39).
16. Gordon Jr, R. S. (1983). An operational classification of disease prevention. Public Health Reports, 98(2), 107-116.
17. Graffunder, C. M., Noonan, R. K., Cox, P., & Wheaton, J. (2004). Through a public health lens: Preventing violence against women – An update from the US Centers for Disease Control and Prevention. Journal of Women's Health, 13(1), 5-16.
18. Griffiths, H. (2013). Misunderstanding the internet. Digital Journalism, 1(1), 170-172. <https://doi.org/10.1080/21670811.2012.740286>
19. Harvey, A., Garcia-Moreno, C., & Butchart, A. (2007). Primary prevention of intimate partner violence and sexual violence: Background paper for WHO expert meeting May 2-3, 2007. Geneva: World Health Organization, Department of Violence and Injury Prevention and Disability.
20. Hummel, B. (2022). 5 Essential steps to teach information literacy in middle school. Digital Curriculum for CTE & Elective.

21. Kafonek, K., & Richards, T. N. (2017). An examination of strategies for the prevention of gender-based violence at four-year institutions of higher education. *Journal of School Violence*, 16(3), 271-285.
22. Kopecký, K., Szotkowski, R., & Krejčí, V. (2012). The risks of Internet communication 3. *Procedia - Social and Behavioral Sciences*, 69, 1348-1357. <https://doi.org/10.1016/j.sbspro.2012.12.072>
23. Liu, M. (2023). Are you really smiling? Display rules for emojis and the relationship between emotion management and psychological well-being. *Front Psychol.* <https://doi.org/10.3389/fpsyg.2023.1035742>
24. Livingstone, S., & Helsper, E. (2007). Taking risks when communicating on the internet: The role of offline social-psychological factors in young people's vulnerability to online risks. *Information, Communication & Society*, 10(5), 619-643. <https://doi.org/10.1080/13691180701657998>
25. Motivational Interviewing and Enhancement Therapies – Recovery Research Institute. Retrieved from <https://www.recoveryanswers.org/research-post/motivational-interviewing-and-enhancement-therapies/>
26. Osler, L., & Zahavi, D. (2023). Sociality and embodiment: Online communication during and after Covid-19. *Found Sci*, 28, 1125-1142. <https://doi.org/10.1007/s10699-022-09861-1>
27. Peebles, E. (2019). Cyberbullying: Hiding behind the screen. *Paediatr Child Health*, 19(10), 527-528. <https://doi.org/10.1093/pch/19.10.527>
28. Porta, M. (2018). *A dictionary of public health*. Oxford University Press.
29. Prevention Strategies: Involving and Engaging Perpetrators. Retrieved from <https://avertfamilyviolence.com.au/prevention-strategies-involving-and-engaging-perpetrators/>
30. Restorative Justice and Sexual Violence | European Forum for Restorative Justice. Retrieved from <https://www.euforumrj.org/en/restorative-justice-and-sexual-violence>
31. Silen, Y., & Keski-Rahkonen, A. (2022). Worldwide prevalence of DSM-5 eating disorders among young people. *National Library of Medicine*. Retrieved from <https://pubmed.ncbi.nlm.nih.gov/36125216/>

32. Stauffer, B. (2020). How to teach digital literacy skills. Digital Curriculum for CTE & Elective.
33. Suzor, N., Dragiewicz, M., Harris, B., Gillett, R., Burgess, J., & Van Geelen, T. (2019). Human rights by design: The responsibilities of social media platforms to address gender-based violence online. *Policy & Internet*, 11(1), 84-103.
34. Thaker, F. O. (2017). Understanding cyber violence in intimate partner relationships: A qualitative study. Georgia State University. Retrieved from <https://www.academia.edu/>
35. Ustavimo spletno nasilje nad ženskami in dekleti Priročnik za strokovnjakinje in strokovnjake, ki delajo z mladimi (Ljubljana, November 2019). Retrieved from <https://www.gov.si/assets/ministrstva/MDDSZ/Enake-moznosti/OdklikniPrirocnikMladina.pdf>
36. Violence, W. I. G. B. (1999). Ending violence against women. *Issues in World Health*, 11, 1-44.
37. Vogels, E. A. (2021). The state of online harassment. Pew Research Center, 13, 625.
38. Wirawan, G. B. S., Hanipraja, M. A., Chrysanta, G., Imtaza, N., Ahmad, K. T., Marlina, I., ... & Larosa, A. T. (2022). Anxiety and prior victimization predict online gender-based violence perpetration among Indonesian young adults during COVID-19 pandemic: Cross-sectional study. *Egyptian Journal of Forensic Sciences*, 12(1), 1-8.

WEBSITES:

- <https://babe.hr/en/ne-online-nasilju/>
- <https://nechupedia.sezamweb.net/>
- <https://www.commonsense.org/education>
- <https://www.youtube.com/watch?v=uZpiZ-e7E8c>
- <https://www.apc.org/en/about>
- <https://interagencystandingcommittee.org/sites/default/files/migrated/2020-11/IASC%20Guidelines%20on%20Mental%20Health%20and%20Psychosocial%20Support%20in%20Emergency%20Settings%20%28English%29.pdf>
- <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4126576/>
- <https://www.sciencedirect.com/science/article/pii/S2666557323000228>
- <https://www.uktherapyguide.com/cyberbullying>

- <https://domental.com/online-therapy/cyberbullying-therapy>
- [https://www.academia.edu/79061163/Cyberbullying and its impact on young peoples emotional health and well being](https://www.academia.edu/79061163/Cyberbullying_and_its_impact_on_young_peoples_emotional_health_and_well_being)
- <https://socialwork.buffalo.edu/social-research/institutes-centers/institute-on-trauma-and-trauma-informed-care/what-is-trauma-informed-care.html>
- https://aa.ecn.cz/img_upload/8b47a03bf445e4c3031ce326c68558ae/zhodnoceni-ef-final.pdf
- <https://www.thedubrovniktimes.com/news/croatia/item/6413-protests-against-domestic-violence-sees-thousands-on-the-streets-of-croatia>
- <https://vlada.gov.hr/news/amendments-to-penal-code-strengthen-mechanisms-to-protect-victims-of-violence/32304>
- <https://evaw-global-database.unwomen.org/en/countries>

Chapter 3

AIContentfy team (2023). Designing Effective Awareness Programs: Strategies for Maximum Impact. <https://aicontentfy.com/en/blog/designing-awareness-programs-strategies-for-maximum-impact>

Brody, S. (2020). Gender-Inclusive Children's Literature as a Preventative Measure: Moving Beyond a Reactive Approach to LGBTQ+ Topics in the Classroom. *Occasional Paper Series*, (44), 7.

Ceia, V., Nothwehr, B., & Wagner, L. (2021). *Gender and Technology: A rights-based and intersectional analysis of key trends*.

Cesar, S. (Ed.) (2021). *Elektroničko seksualno i rodno uvjetovano nasilje u mladenačkim vezama - priručnik za nastavnike i nastavnice*. Zagreb: Centar za edukaciju, savjetovanje i istraživanje.

Crooks, C. V., Goodall, G. R., Hughes, R., Jaffe, P. G., & Baker, L. L. (2007). Engaging men and boys in preventing violence against women: Applying a cognitive-behavioral model. *Violence against women*, 13(3), 217-239.

Directive 2012/29/EU of the European Parliament and of the Council of 25 October 2012 establishing minimum standards on the rights, support and protection of victims of crime, and replacing Council Framework Decision 2001/220/JHA.

Fernandes, M., Lomba, N., & Navarra, C. (2021). *Combating Gender Based Violence: Cyber Violence*.

Fisher, D., Lang, K.S., & Wheaton, J. (2010) *Training Professionals in the Primary Prevention of Sexual and Intimate Partner Violence: A Planning Guide*. Atlanta (GA): Centers for Disease Control and Prevention.

Flanery, C. J. (2023). Prevention at the University Level. *Facing Campus Sexual Assault and Relationship Violence With Courage: A Guide for Institutions and Clinicians on Prevention, Support, and Healing*, 39.

Gordon Jr, R. S. (1983). An operational classification of disease prevention. *Public health reports*, 98(2), 107.

Graffunder, C. M., Noonan, R. K., Cox, P., & Wheaton, J. (2004). Through a public health lens. Preventing violence against women: An update from the US Centers for Disease Control and Prevention. *Journal of Women's Health*, 13(1), 5-16.

Harvey, A., Garcia-Moreno, C., & Butchart, A. (2007). Primary prevention of intimate partner violence and sexual violence: Background paper for WHO expert meeting May 2-3, 2007. *Geneva: World Health Organization, Department of Violence and Injury Prevention and Disability*, 2

Hummel, B. (2022). 5 Essential Steps to Teach Information Literacy in Middle School. *Digital Curriculum for CTE & Elective*.

Kafonek, K., & Richards, T. N. (2017). An examination of strategies for the prevention of gender-based violence at four-year institutions of higher education. *Journal of school violence*, 16(3), 271-285.

Porta, M. (2018). *A dictionary of public health*. Oxford University Press

Stauffer, B. (2020). How to Teach Digital Literacy Skills. *Digital Curriculum for CTE & Elective*.

Suzor, N., Dragiewicz, M., Harris, B., Gillett, R., Burgess, J., & Van Geelen, T. (2019). Human rights by design: The responsibilities of social media platforms to address gender-based violence online. *Policy & Internet*, 11(1), 84-103.

Violence, W. I. G. B. (1999). Ending violence against women. *Issues in World Health*, 11, 1-44

Vogels, E. A. (2021). The state of online harassment. *Pew Research Center*, 13, 625.

Wirawan, G. B. S., Hanipraja, M. A., Chrysanta, G., Imtaza, N., Ahmad, K. T., Marlina, I., ... & Larosa, A. T. (2022). Anxiety and prior victimization predict online gender-based violence perpetration among Indonesian young adults during COVID-19 pandemic: cross-sectional study. *Egyptian journal of forensic sciences*, 12(1), 1-8.

Links:

<https://www.apc.org/en/about>

Chapter 4

Literature

Adikari, N. (2016). Cyber Violence Crimes against women and girls. Proceedings of the second Conference on Women's Studies, Vol. 1, 2-4. Ανακτήθηκε από : <https://www.academia.edu/>

Fatem – Zahra, A. (2018). Revenge porn : The dangers of hyperreality and gendered cyberviolence. Issue 2. IIS Brief. Ανακτήθηκε από : <https://www.academia.edu/>

Thaker, F.O. (2017). Understanding cyber violence in intimate partner relationships : A qualitative study. Georgia State University. Ανακτήθηκε από : <https://www.academia.edu/>

Dunn S. (2020). Technology – facilitated gender – based violence. An overview. Centre of International Governance Innovation. Ανακτήθηκε από : <https://scholar.google.com/>

Chapter 5

Prevention Strategies: Involving and Engaging Perpetrators
(avertfamilyviolence.com.au)

Cognitive behavioural group therapy for male perpetrators of intimate partner violence: a systematic review - PMC (nih.gov)

Motivational Interviewing and Enhancement Therapies – Recovery Research Institute (recoveryanswers.org)

Restorative Justice and Sexual Violence | European Forum for Restorative Justice (euforumrj.org)

Chapter 6.

6.5. Sources:

1. Osler, L. & Zahavi, D. (2023): Sociality and Embodiment: Online Communication During and After Covid-19. In: *Found Sci* 28, pp. 1125-1142, <https://doi.org/10.1007/s10699-022-09861-1>.
2. Griffiths, H. (2013): Misunderstanding the Internet. In: *Digital Journalism*, 1:1, pp. 170-172, <https://doi.org/10.1080/21670811.2012.740286>.
3. Kopecký, K. & Szotkowski, R. & Krejčí, V. (2012): The Risks of Internet Communication 3. In: *Procedia - Social and Behavioral Sciences*, Volume 69, pp. 1348-1357, <https://doi.org/10.1016/j.sbspro.2012.12.072>.
4. Livingstone, S. & Helsper, E. (2007): Taking risks when communicating on the internet: the role of offline social-psychological factors in young people's vulnerability to online risks. In: *Information, communication and society*, 10 (5). pp. 619-643. <https://doi.org/10.1080/13691180701657998>.
5. Liu, M. (2023): Are you really smiling? Display rules for emojis and the relationship between emotion management and psychological well-being. In: *Front Psychol*, <https://doi.org/10.3389/fpsyg.2023.1035742>.
6. Peebles, E. (2019): Cyberbullying: Hiding behind the screen. In: *Paediatr Child Health*, 19(10), pp. 527-528, <https://doi.org/10.1093/pch/19.10.527>.
7. European Institute for gender equality (2022). Combating Cyber Violence against Women and Girls. In: <https://eige.europa.eu/publications-resources/publications/combating-cyber-violence-against-women-and-girls>

Online Sources

1. <https://www.techwalla.com/articles/dangers-of-online-communication>
2. <https://www.coe.int/en/web/cyberviolence>
3. <https://psychcentral.com/lib/10-tips-for-setting-boundaries-online#3>
4. <https://www.allure.com/story/healthy-digital-boundaries-online-internet>

5. <https://zoella.co.uk/2020/08/31/8-ways-to-create-healthy-boundaries-online/>
6. <https://www.endcyberbullying.net/what-to-do-if-youre-a-victim>
7. <https://www.bitdefender.com/cyberpedia/what-is-online-privacy/>
8. <https://digitalhygiene.net/>
9. [https://www.onelogin.com/learn/what-is-mfa#:~:text=Multi%2Dfactor%20Authentication%20\(MFA\)%20is%20an%20authentication%20method%20that,access%20management%20\(IAM\)%20policy.](https://www.onelogin.com/learn/what-is-mfa#:~:text=Multi%2Dfactor%20Authentication%20(MFA)%20is%20an%20authentication%20method%20that,access%20management%20(IAM)%20policy.)
10. <https://www.kaspersky.com/resource-center/preemptive-safety/cyber-hygiene-habits>
11. https://eige.europa.eu/newsroom/news/safespaces-eige-highlights-widespread-forms-cyber-violence-against-women-and-girls-proposes-definitions?language_content_entity=en
12. <https://cocoslaw.ie/>
13. <https://www.humanrightscareers.com/issues/why-advocacy-is-important/>

Chapter

7

<https://interagencystandingcommittee.org/sites/default/files/migrated/2020-11/IASC%20Guidelines%20on%20Mental%20Health%20and%20Psychosocial%20Support%20in%20Emergency%20Settings%20%28English%29.pdf>

<https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4126576/>

<https://www.sciencedirect.com/science/article/pii/S2666557323000228>

<https://www.uktherapyguide.com/cyberbullying>

<https://domental.com/online-therapy/cyberbullying-therapy>

https://www.academia.edu/79061163/Cyberbullying_and_its_impact_on_young_people_emotional_health_and_well_being

<https://socialwork.buffalo.edu/social-research/institutes-centers/institute-on-trauma-and-trauma-informed-care/what-is-trauma-informed-care.html>

Chapter 8:

https://aa.ecn.cz/img_upload/8b47a03bf445e4c3031ce326c68558ae/zhodnoceni-ef-final.pdf

The 24-month project "Prevention and Support for Cyber Gender Violence (PS-CGBV)" aims to combat cyber gender-based violence through awareness-raising and empowerment of young people, as well as training of social service professionals and volunteers providing support to victims and youth workers.

Ali Honaramiz, Agáta Hrdličková, Anna Kotková, Andrei Ignatov, Silviya Miteva, Lucie Příbyl, Daniela Šincek, Viktorija Triuskaite, Raya Tsvetkova, Theodora Vainterli were responsible for writing and illustrating this manual.