The digital dimension of violence against women and girls in Slovenia

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

The digital dimension of violence against women and girls in Slovenia

Aleš Završnik, national consultant
Louise Hooper, international consultant

This report has been prepared as part
of the Council of Europe's "Ending Violence Against Women:
Multi-Country Programme".

Council of Europe

The opinions expressed in this work are the responsibility of the authors and do not necessarily reflect the official policy of the Council of Europe.

All other correspondence concerning this publication should be addressed to the Directorate General of Democracy and Human Dignity. Violence against Women Division Council of Europe F-67075 Strasbourg Cedex France, Council of Europe

E-mail: conventionviolence@coe.int

Cover and layout: Documents and Publications Production Department (SPDP), Council of Europe

Cover Photos: Shutterstock

This publication has not been copy-edited by the SPDP Editorial Unit to correct typographical and grammatical errors.

Contents

Introduction

Under the framework of the Council of Europe "Ending violence against women: multi-country programme", the Slovenian authorities have requested the Council of Europe to produce a report to assess the current capacity of the Slovenian authorities to respond to the problem of digital forms of violence against women and girls and provide recommendations where necessary and relevant to address shortcomings. As early as 2014 research conducted by the European Fundamental Rights Agency demonstrated that Data for Slovenia showed that 12% of the responding women were victims of violence, 4% were victims of sexual violence and one out of three respondents was a victim of psychological violence by their partner since reaching the age of 15. Furthermore, data for victims of sexual harassment and stalking showed that almost every other respondent in Slovenia was a victim of some form of sexual harassment since the age of 15, and 14% were victims of one form of stalking. Some 7% of the surveyed Slovenian women said that since the age of 15, they had experienced an inappropriate approach by people on social networks or received electronic mail or SMS messages with sexual content, while 3% said that they had been victims of online stalking.[1]

A survey in 2018 by the Faculty of Social Sciences of the University of Ljubljana (the "Click-off Digital Bullying" project, 2017 – 2019) of 5000 young people aged between 12 and 18 showed that boys are the most frequent online harassers of both girls and boys and also the serious consequences of the online harassment of girls.[2] The results also show that among the primary school population, 56% of female students and 50% of male students (grades 7 to 9) experienced at least one form of harassment in the past school year. Among the secondary school population, 65% of female students and 55% of male students experienced at least one form of harassment in the past school year.[3]

According to the NGO Association for Non-Violent Communication[4] (*Društvo za nenasilno komunikacijo)*, the women who contact the NGO are victims of intimate partner violence and report that digital forms of violence present another layer and extension of other forms of violence. The most common digital forms of violence victims report are spreading rumours or intimate material via social media and emailing lists, flooding with emails and short text messages (SMSs), and sometimes even installing spying apps on mobile phones to reveal their locations (such as "search my phone" app).

Legislative frameworks often fail to keep up with developments in technology and the threats this can pose to women's and girls' lives and safety. States are then forced to resort to expanding the scope of existing legislation that was often designed to cover very different offences and that might not accurately reflect the true harm of violence in the digital dimension. This report aims to outline some key legal and other challenges in Slovenia to tackle the threat of the digital dimensions of violence against women. This should help to ensure that professionals working with victims or perpetrators of gender-based violence against women in the digital dimension are properly trained and equipped to identify and respond to these new forms of violence arising from emerging technologies.

1. GREVIO Baseline Evaluation Report, Slovenia
2. GREVIO Baseline Evaluation Report, Slovenia, fn 29
3. Odklikni webpate available at: https://odklikni.enakostspolov.si/raziskave/
4. Društvo za nenasilno komunikacijo (Association for Nonviolent Communication), webpage www.drustvo-dnk.si interview with Tjaša Hrovat from 20 September 2024

Methodology and scope

This report is based on an analysis of the relevant international and domestic legal frameworks, desk research and fieldwork. This included a detailed analysis of Slovenian legal provisions and their implementation identified through written reports, information gathered through the media and interviews with key stakeholders, including representatives of two NGOs working in the field of equality and citizenship and providing support to women victims of violence, a Senior Criminal Police Inspector and Head of Juvenile Crime Section from the Police, the Academic and Research Network of Slovenia (ARNES) running SI-CERT, a designated national computer security incident response team, two academics working in the field of domestic violence and one of the partners of the "Click-off Digital Bullying" project from the Faculty of Social Sciences at the University of Ljubljana. The research was designed to identify key gaps in legislation or practice that require action to ensure the protection of women and girls in the digital sphere, including levels of awareness and understanding of the problem and of the technical and legal definitions and evidential issues amongst law enforcement actors, NGOs and victims/survivors. It also covers cross-border cooperation in respect of electronic evidence and other relevant matters.

In defining the scope and conducting the research, key Council of Europe standards and documents considered included:

- Council of Europe Convention on preventing and combatting violence against women and domestic violence (CETS No. 210, known as the Istanbul Convention)
- GREVIO General Recommendation No. 1 on the digital dimension of violence against women (GREVIO General Recommendation No. 1)
- Thematic paper on the digital dimension of violence against women. The Platform of Independent Expert Mechanisms on Discrimination and Violence against Women (EDVAW Platform)
- 'Protecting women and girls from violence in the digital age' (Council of Europe study (Van der Wilke 2021))

International Legal Framework

Slovenia succeeded to the UN Convention on the Elimination of Discrimination against Women on 1 July 1992 under the Act on Succession, on the basis of which it took effect in Slovenia on the day of its independence, 25 June 1991. The Optional Protocol to the Convention on the Elimination of all Forms of Discrimination against Women was adopted on 6 October 1999 and has been in force in Slovenia since 15 May 2004.

Although the UN Convention on the Elimination of Discrimination against Women (CEDAW) does not explicitly condemn violence against women, the CEDAW Committee, through its General Recommendations, has made clear since 1992 (CEDAW, 1992, para 6, Rec No. 19) that gender-based violence may breach specific provisions of the Convention. General Recommendation No. 35 (2017) acknowledges that violence against women 'manifests itself on a continuum of multiple, inter-related and recurring forms, in a range of settings, from private to public, including technology mediated settings' (CEDAWa, 2017 para 6). Gender-based violence occurs in all spaces and spheres of human interaction, whether public or private and the redefinition of public and private through technology-mediated environments such as contemporary forms of violence occurring online and in other digital environments [para 20]. The CEDAW Committee recommends States Parties to gather data on the digital dimensions of violence against women (para 34(b)) and prompt the private sector, including businesses and transnational corporations, to implement suitable measures for eliminating violence against women on their services and platforms (CEDAW, 2017a, para 30(d)). General recommendation No. 36 (201) on the right of women and girls to education refers directly to cyberbullying and requires states to enact legislation that defines and penalises harassment through the use of ICT and the online harassment of women and girls in all its forms (CEDAW 2017b: paras 70-72).

The CEDAW 7th periodic report on Slovenia (CEDAW 2023) noted a range of legislative improvements with respect to equality, domestic violence, and discrimination, but it also recognised some areas of concern. In the context of gender-based violence against women, concerns were raised that sentences should be commensurate with the gravity of harm suffered and include, as appropriate, restitution, compensation and rehabilitation (paragraph 15a). In the context of digital dimensions of gender-based violence, the Committee noted that there had been a survey conducted relating to the prevalence and identification of cyber-harassment among young people and a media campaign launched in 2019 focused on raising awareness of various forms of cyberviolence, particularly those that frequently affect women and girls (para 25). The committee recommended that Slovenia adopt a comprehensive strategy to combat all forms of violence against women and girls, establish a permanent mechanism to coordinate, monitor and assess whether measures taken are effective and ensure appropriate and disaggregated data collection. In the context of increasing women's participation in public life, CEDAW recommended the adoption of legislation to prevent harassment and threats against women in political and public life, including by strengthening monitoring and reporting mechanisms and holding social media companies accountable for discriminatory user-generated content and ensuring investigation, prosecution and punishment of those responsible (para 32(e)).

Istanbul Convention

Slovenia signed the Istanbul Convention on 8 September 2011, ratified it on 5 February 2015, and it entered into force on 1 June 2015.

Due to the rapid spread of the internet and technology-related harmful activities within the newly emerged digital sphere, the Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) acknowledged the escalating global concern in respect of violence against women occurring in the digital realm and during its 21st plenary meeting decided to prepare its first General Recommendation dedicated to the application of the Istanbul Convention in relation to the digital aspect of violence against women. Article 69 of the Istanbul Convention empowers GREVIO to adopt general recommendations on the implementation of the convention.

As outlined in the Explanatory Report to the Istanbul Convention, General Recommendations are intended to have a uniform interpretation for all parties involved, addressing articles or themes within the convention. While not legally binding, General Recommendations play a pivotal role as a crucial reference point for parties, fostering a deeper comprehension of convention themes and furnishing explicit guidance for effective implementation. They are structured to be incorporated into future monitoring endeavours.

GREVIOS's General Recommendation No. 1 on the digital dimension of violence against women, adopted on 20 October 2021, seeks to align the ICT discourse with the narrative of gender-based violence against women by clearly positioning manifestations of violence against women and girls in the digital sphere as expressions of gender-based violence against women covered by the Istanbul Convention. GREVIO stressed the importance of separately defining violence in this newly formulated sphere. It places particular focus on all forms of online sexual harassment, online and technology-facilitated stalking and the digital dimension of psychological violence.

The digital dimension of violence against women encompasses a wide range of acts online or through technology that are part of the continuum of violence that women and girls experience for reasons related to their gender, including in the domestic sphere, in that it is an equally harmful manifestation of the gender-based violence experienced by women and girls offline.

Other Council of Europe relevant standards

Other relevant standards include CM/Rec (2019) 1 of the Committee of Ministers to Member States on preventing and combating sexism, which includes a dedicated section on online sexist hate speech, and CM/Rec (2022)16 on combatting hate speech adopted 20 May 2022.

The Parliamentary Assembly of the Council of Europe (PACE) has issued Recommendation 2098 (2017) on ending cyber discrimination and online hate and two relevant resolutions, firstly Parliamentary Assembly Resolution 2144 (2017) on ending cyber-discrimination and online hate and secondly Parliamentary Assembly Resolution 2177 (2017) on putting an end to sexual violence and harassment of women in public space.

Finally, the European Commission against Racism and Intolerance has produced General Policy Recommendation No. 15 on Combating Hate Speech, which also covers hate speech in the digital sphere.

European Union law

The European Union's Digital Services Act (DSA)[5] obliges providers of intermediary services, such as online platforms and online search engines, to provide a safer online experience for all and establish a framework for managing illegal content online through transparency reporting obligations (Art. 15), "notice and action" mechanisms (Art. 16) and "trusted flaggers" (Art. 22) that act as a bridge between regulators, platforms, and users, ensuring illegal content is identified and managed effectively.

Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combatting violence against women and domestic violence[6] recognises the need to provide for harmonised definitions of cyberviolence where violence is intrinsically linked to the use of ICT, and those technologies are used to significantly amplify the severity of the harmful impact of the offence, thereby changing the character of the offence. It especially highlights that cyber violence targets and impacts women politicians, journalists and human rights defenders with the effect of silencing women and hindering their societal participation on an equal footing with men. It recognises that cyber violence disproportionately affects women and girls in educational settings with detrimental consequences to their further education and to their mental health and asks EU Member states to criminalise non-consensual sharing of intimate or manipulated material, cyberstalking, cyber harassment and cyber incitement to violence and hatred.

Definitions and basic conceptsThere is a lack of standardised definitions both nationally and internationally. Terms that are often used include 'online violence', 'cyberbullying', 'cyberabuse' and tech-facilitated violence. Some terms, such as bullying and doxing, cannot be translated from English in a non-descriptive way into Slovenian (e.g. bullying equals harassment in Slovenian translation). For the purposes of this report, we use definitions from GREVIO General Recommendation No. 1 on the digital dimension of violence against women.

5. Regulation (EU) 2022/2065, Digital Services Act
6. Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence

Prevention

Analysis of existing national legislation

The analysis below aims to examine whether the existing legislation aligns with GREVIO General Recommendation No. 1 on the digital dimension of violence against women and any other relevant international legal standards to provide policymakers with a guide to identifying gaps and possible shortcomings. It addresses the main legal provisions in constitutional, civil, criminal, and administrative law related to **online and tech-facilitated violence against women and domestic violence**.[7]

Domestic Violence Prevention Act (Zakon o preprečevanju nasilja v družini, ZPND)[8]

This Act is transversal in the sense that non-repressive means to tackle domestic violence are at the centre of the Act, e.g. the goal is to encourage social work centres and employers to act and prevent domestic violence. When the Court decides on a restriction order, for instance, the procedure to be followed is the Non-Contentious Civil Procedure Act (*Zakon o nepravdnem postopku*, ZNP-1). Hence, the transversal nature of the Act primarily aims to protect victims through all possible means, without restricting state agencies to criminal law definitions of crime or strict criminal procedures rules in order to take action.

General rules, Criminal Code (Kazenski zakonik, KZ-1)[9]

Provisions relevant to the digital dimension of violence against women in the General part of the Criminal Code impacting individual criminal offences include provisions related to hate crime[10], ex officio prosecution for minor[11] victims[12], specific security measures as a type of a criminal sanction imposed on a perpetrator in addition to a sentence[13]; specific provision on access to the criminal record[14]; enforcement of criminal sanctions with the protection order[15]; and limitation periods for crimes against children[16].

A special part of the Criminal Code includes offences directly or indirectly relevant to digital forms of violence against women.

7. Translations of Slovenian legislation: https://pisrs.si/aktualno/zakonodaja-v-anglescini.
8. The Domestic violence prevention act (*Zakon o preprečevanju nasilja v družini*), 1 February 2008, and subsequent modifications.
9. The Criminal code (*Kazenski zakonik*), 20 May 2008, and subsequent modifications.
10. Article 49/3 of the Criminal Code stipulates that if the victim's gender or "any other personal circumstance" was a factor contributing to the commission of the offence, this should be considered as an aggravating circumstance.
11. Criminal Code KZ-1 distinguishes two categories of children (as defined in the UN Convention on the Rights of the Child): a *minor* is a person younger than 18 years, while a *child* is a person below 14 years, which is also a threshold for criminal liability.
12. Prosecution *ex officio* is envisaged if a case involves a minor – a person younger than 18 years (Art. 15a), and concerns an offence referred to in the chapters relating to 1) offences committed against life and limb, 2) against human rights and freedoms (e.g. Violation of the right to equality, Art. 131; Stalking, Art. 134a; Threats, Art. 135; Abuse of personal data, Art. 143) and 3) offences against sexual integrity or other criminal offences with elements of violence (e.g. Sexual assault of a person younger than fifteen years of age, Art. 173; Solicitation of persons under fifteen years of age for sexual purposes, Art. 173a; The presentation, manufacture, possession and distribution of pornographic material, Art. 176). On the contrary, if the victim is an adult, then, e.g., prosecution for Stalking or Identity theft may be initiated only upon a proposal.
13. Art 71a, see below under Protection
14. Art 84 provides an exception on access to data where the offence is related to the abuse of children in institutions or associations entrusted with education, guidance, protection or care of children.
15. See Chapter 10 on the enforcement of criminal sanctions. Art 88/8 provides for protection orders in respect of those conditionally released which can include a restriction on contact via electronic means
16. Limitation starts to run from the day the child reaches adulthood save for cases of Misuse of personal data – see Art 90/3 of Criminal Code KZ-1

Online sexual harassment

Article 40 of the Istanbul Convention defines sexual harassment as 'any form of unwanted verbal, non-verbal or physical conduct of a sexual nature with the purpose or effect of violating the dignity of a person, in particular when creating an intimidating, hostile, degrading, humiliating or offensive environment'. General Recommendation No. 1 on the digital dimension of violence against women identifies five particular forms: i) non-consensual image or video sharing, ii) non-consensual taking, producing or procuring of intimate images or videos, iii) "exploitation, coercion and threats" (within the remit of Article 40 of the Convention), iv) sexualised bullying and v) cyberflashing. Some of these behaviours can be considered sexist hate speech.

In Slovenia, sexual harassment, harassment and discrimination are prohibited by the Protection against Discrimination Act, criminal law and labour law but the scope of application is limited to the workplace. **Workplace harassment** is an offence (*Šikaniranje na delovnem mestu*, Art. 197 of the KZ-1). The offence can be committed in the workplace or in relation to work. It includes humiliating or intimidating another person by sexual harassment, psychological violence, ill-treatment or unequal treatment in the workplace or in relation to work. Some of the elements, such as sexual harassment and psychological violence, can also be conducted via digital means.

However, although there is no general criminal offence of harassment, Slovenia does criminalise other forms of digital violence that constitute harassment, including some forms of non-consensual image-based abuse, some forms of sexualised bullying and exploitation and has other offences that, alongside exploitation, coercion and threats could theoretically be applied to digital offences.

Non-consensual image-based abuse

The GREVIO General Recommendation no. 1 on the digital dimension of violence against women includes the non-consensual taking, producing or procuring of intimate images or videos and the non-consensual sharing of nude or sexual images or videos. Technology enables non-consensual images to be created and shared rapidly across larger audiences. New and emerging technologies, such as the use of generative and other AI for non-consensual production, manipulation or altering of images or creation of deep-fakes, require explicit inclusion in the law.

Slovenia has several offences targeting non-consensual image abuse through images and videos, which can be or have been adapted to the digital dimension. The offence **Unlawful image recording** (*Neupravičeno slikovno snemanje*) (Art. 138 of the KZ-1) concerns the invasion of privacy by taking photographs or making video recordings without the victim's consent, with an additional condition that, in such a manner, the offender significantly invades the victim's privacy or transmits the material directly to a third party, or shows such a recording to a third party, or otherwise makes such material accessible to a third party.

While some forms of the harm, such as "making such material accessible to a third party", covers, e.g. posting unlawfully recorded material on social media, the provision requires further adaptation to cover the full nature of the digital harm. This offence does not appear to cover the situation where either the image was created by the victim or with consent but later shared without consent.

Other forms of non-consensual image-taking or sharing, manipulation or creation may be covered under the Misuse of Personal Data offence (*Zloraba osebnih podatk*ov, Art. 143/6 of the KZ-1). The Data Protection Authority (*Information Commissioner of the Republic of Slovenia*) has also issued an opinion[17] that deep fake entails using personal data; hence, making a deep fake without consent can lead to the offence of Misuse of Personal Data.

17. Opinion 092-4/2024/11, 'Deep fakes as personal information'

Misuse of personal data

Within the Criminal Code (KZ-1), misuse of personal data to commit digital harm is an offence. Under Slovenian law, therefore, revealing a victim's personal data online, such as in the case of outing, creepshots, deadnaming, doxing or image-based sexual abuse, a perpetrator will commit the criminal offence **Misuse of Personal Data** (*Zloraba osebnih podatk*ov, Art. 143 of the KZ-1). The forms of offence relevant to the digital dimension of violence can be committed in several ways: if a person publishes, or causes to be published, without consent of a data subject or without legal basis, personal data processed on a legal basis or consent (§ 1). Another form can be committed by breaking into a computerised database to acquire such personal data from § 1 (§ 2). A qualified form of the offence, e.g. typically committed by digital means against women in the form of image-based abuse ("revenge porn"), is committed by publishing photographs or messages with *sexual content* without the victim's consent and severely affecting the victim's privacy (§ 6). Another qualified form of the above-mentioned offence includes the case when special categories of personal data[18] are revealed, e.g., sexual orientation or gender identity (§ 5). The offence also incriminates "identity theft" (§ 4, while the term itself is not used in the code), defined in a two-fold manner as assuming the identity of another person or processing the personal data of another person by exploiting his or her rights, obtaining material or non-material benefit or adversely affecting a victim's personal dignity. The notion of personal dignity should be interpreted according to Article 34 of the Constitution of the Republic of Slovenia (*Right to personal dignity and safety*), which refers to the way people are recognised as worthy human beings.[19]

These offences are punishable with sentences of imprisonment ranging from 3 months to three years.

Slovenia could:

- **Review the criminal law to ensure image-based abuse in all its forms and across all digital media is appropriately criminalised and sanctioned. In particular, consideration should be given to the methods of unlawful sharing of information and whether 'private' sharing of information as opposed to 'public' sharing is appropriately covered. Consideration may also be given to whether reform is required to paragraph 143/6 of the Criminal Code KZ-1 to remove the requirement of severity on the grounds that sharing material containing sexual content without consent is sufficiently serious in and of itself. Issues with respect to severity would continue to be relevant to punishment.**

Child sexual exploitation and abuse

The legal framework with respect to the protection of children under the age of 15 goes further to cover incrimination of **the presentation, manufacture, possession and distribution of pornographic material** (Art. 176 of the KZ-1). The offence includes several types of actus reus, which can be committed via digital services or online: selling, presenting or publicly exhibiting documents, pictures or audio-visual or other items of a pornographic nature to persons under fifteen years of age, enabling them to gain access to these in any other manner, or presenting to them a pornographic or other sexual performance (§ 1).

The aggravated form of the offence is committed if a perpetrator by force, threat, deception, excessive or abusive powers, recruitment or solicitation, or for exploitative purpose instructs, obtains or encourages a **minor** (meaning a person below 18 years and not only below 15 years as in § 1) to produce photographs, audio-visual or other items of a pornographic or other sexual nature, or uses them in a pornographic or other sexual performance, or knowingly attends at such performances (§ 2). Especially acts of deception, recruitment or solicitation of a minor to produce photographs may often be the case in online sextortion cases, when a perpetrator threatens to reveal intimate details to parents or friends and extort more sexually explicit images or other content.

Moreover, another aggravated form is committed when a person produces, distributes, sells, imports, or exports pornographic or other sexual materials depicting minors or their realistic images, or supplies them in any other way, or possesses such materials, or obtains access to such materials by means of ICT, or discloses the identity of a minor in such materials either for him- or herself or any third person (§ 3).

However, an offence under § 3 is not committed (§ 5) if the following conditions are met (cumulatively): 1) the act was committed between minors of comparable age; 2) minors consented to the act, 3) the act corresponds to the level of their mental and physical maturity, and 4) the sexual material displays these consenting minors

18. Personal data are defined in Personal Data Protection Act (ZVOP-2) and Regulation (EU)2022/2065 General Data Protection Regulation.
19. Constitutional Court of the Republic of Slovenia, Judgement U-I-54/99 from 28 June 2002.

(a new § 5 was added with the amendments from 2021). The limitation period for the aggravated form (§ 2 and 3) is 60 years from the day the offence was committed (extended with the amendment of the KZ-1 from 2020).

Child sexual abuse material is any form of depiction of sexual abuse of minors (whether of an individual or their realistic images), e.g. it can be an image or video, as well as text, audio, or other format. The perpetrator can be an adult or a minor aged between 14 and 18 who produces, possesses, transmits to others, and/or intentionally accesses child abuse material.

For children under 15, therefore, the protection is greater than for children over 15 only for selling, presenting or publicly exhibiting documents, pictures or audio-visual or other items of a pornographic nature (§ 1), while producing photographs, audio-visual or other items of sexual child abuse, including realistic images of children, is prohibited under § 2 and § 3 for all minors. Pornographic material of non-consensual women is not protected similarly, but only with § 6 of the Misuse of Personal Data (Art. 143) offence. Making non-consensual pornographic material of adult women publicly available is not addressed under this article and appears to be dealt with solely under the misuse of personal data provisions. This may not be wholly appropriate.

- **Review the criminal law on the presentation, manufacture, possession and distribution of pornographic material to make sure it adequately covers the digital dimensions, and consider whether the law adequately covers digital pornographic offences committed against adults, e.g. women whose images or videos are used to create pornography without their consent.**

Cyberflashing

The Protection of Public Order Act (*Zakon o varstvu javnega reda in miru*, ZJRM-1) contains the misdemeanour of indecent behaviour, which could potentially be used for cases of cyberflashing, but it is recommended the Act be amended in order to clearly include the digital realm.

Misdemeanour "**Indecent behaviour"** (Art. 7 of the Protection of Public Order Act, *Zakon o varstvu javnega reda in miru*, ZJRM-1[20]) may be committed by someone who argues, shouts, or acts indecently in a public place. Indecent behaviour means the behaviour of a person or a group causing distress or upset or posing a threat to a person or a group or damage or when due to offensive speech and actions, the reputation of a person or a group or an official in the performance of official duties is harmed (point 5, Art. 2 of the ZJRM-1). All the acts must be committed in a *public space*. Moreover, a qualified form of the misdemeanour may be committed by a person who has sexual intercourse in a public place, exposes his or her genitals, or offers sexual services in an intrusive manner, thereby disturbing people and causing distress or outrage amongst people (§ 3 Art. 7 of the ZJRM-1). This could cover unsolicited "flashing" of intimate parts online if the "online space" could be defined as a public space. The Act defines a public space as any place accessible to everyone unconditionally or under certain conditions (Point 2 Art. 2 of the ZJRM-1). Sending a nude picture, for instance, as an MMS (Multimedia Messaging Service) via phone or an instant messaging app (e.g. Snapchat) is not covered as these cannot be defined as a public space.

Finally, the Sexual Violence offence (Art. 171 of the Criminal Code, KZ-1) may criminalise some forms of flashing if the element "causing someone to suffer a sexual act" is interpreted more broadly and the victim is trapped or surprised to suffer a sexual act and can not escape flashing.

- **Review and amend the law to clearly address unsolicitated cyberflashing in public and in private spaces, whether as a misdemeanour or criminal offence.**

Exploitation, coercion and threats

Exploitation, coercion and threats coming within Article 40 of the Istanbul Convention include sexting, sexual extortion, rape threats, sexualised/gendered doxing, impersonation and outing.

Online grooming for the purpose of exploitation

Solicitation of persons under fifteen years of age for sexual purposes (Art. 173a of the Criminal Code, KZ-1), known as grooming, is committed when an offender proposes, by means of ICT, to meet with a person under fifteen years of age for the purpose of committing a Sexual assault (Art. 173 of the KZ-1) or for the purpose of producing photographs or audio-visual or other items with pornographic or other sexual content (Art. 176

20. The Protection of Public Order Act, at: https://pisrs.si/pregledPredpisa?id=ZAKO3891

of the KZ-1), and such a proposal is followed by material acts to realise such a meeting. The offence is hence limited in scope as it criminalises only 1) online (not offline) grooming of victims under 15 years of age, and 2) the online conversation must be followed by specific "material steps" to arrange a meeting, e.g. an agreement on the time and place of the meeting or on the distinguishing signs for the meeting in person. The offence is not unlawful if committed with a person of comparable age and mental and physical maturity (§ 5 Art. 176 of the KZ-1).

If, in the course of grooming, a perpetrator actually meets with a person under the age of 15 and makes sexual abuse material, then the perpetrator will commit a separate offence under Art. 176 of the KZ-1, which consumes the prior grooming conduct of the perpetrator. If the encounter between the perpetrator and a victim is proceeded by direct sexual contact, then the latter amounts to a more serious offence of sexual assault on a person under the age of 15 (Art. 173 of the KZ-1), which also consumes the prior grooming conduct (ideal concurrence).

- **There is a clear gap with respect to the online grooming of victims over the age of 15, which should be reviewed. The provision on solicitation reflects the European Convention on Action against Trafficking in Human Beings at Art. 23 in respect of grooming children under the legal age of consent for sexual activity. The digital dimension of violence against women and domestic violence can lead to women also being groomed online either for human trafficking or for other forms of manipulation and exploitation. It does not appear that the legal framework currently covers these acts for adult women (or men). Moreover, Slovenia could consider extending the grooming provision to cover other crimes of exploitation in the context of digital violence. It could also consider the criminalisation of any attempt under Article 173a of the Criminal Code.**

Extortion and blackmail (*Izsiljevanje*, Art. 213 of the KZ-1) include extortion with disclosure of information, such as intimate recordings, and can also be committed via digital means. A constitutive element of the offence is, however, the perpetrator's intent to obtain financial or other pecuniary gain and not intent, such as shaming or humiliation of a victim. This may not sufficiently cover the types of psychological harm experienced by victims.

Coercion (*Prisiljenje*, Art. 132 of the KZ-1) can be committed if a person, by means of force or serious threat, coerces another person to perform an act or omit the performance of an act or suffer any harm. The act is punishable by imprisonment for up to one year and may be initiated only upon the victim's proposal.

The criminal offence **Threat** (*Grožnja*, Art. 135 of the KZ-1) can also be committed in the digital sphere, as it is completed by someone who seriously threatens another person with the intention of intimidating or upsetting this person with an attack on his or her life or body or freedom, or threatens to destroy property of his or hers of substantial value or to commit any of these acts against a person close to him or her. The prosecution may be initiated only upon the victim's proposal.

- **Review the law to ensure that threats, coercion, extortion and blackmail in the digital sphere that constitute harassment are sufficiently criminalised, recognising both the often 'private' sphere in which the offences take place and the relevant impact of repeated events and a course of conduct.**

Cyberbullying and Sexualised bullying

NGO Research Institute 8 March (*Zavod raziskovalni inštitut 8. Marec*, www.8marec.si) (interview with Kristina Krajnc from 27 September 2024).

The NGO and its members have been a frequent target of misogynic hate speech, threats of sexual violence ("you will be raped") and insults due to their political involvement in various issues (e.g. even for a referendum on the Water Act). They are also targets of SLAPP suits due to their political involvement.

The NGO is an organisation fighting for civil rights, however, it is widely perceived as a feminist organisation known by the public as an organisation fighting for women's rights (hence the name "8 March"), e.g. abortion.

The NGO has prepared its own internal guidelines for the protection of its members and their volunteers.

Trolling, i.e. deliberately posting abusive comments online, with the direct intention of causing alarm, distress or humiliation, can fulfil elements of the **hate speech** offence. Public incitement to hatred, violence or intolerance (*Javno spodbujanje sovraštva, nasilja ali nestrpnosti*, Art. 297 of the KZ-1) incriminates forms of publicly inciting or stirring up hatred, violence or intolerance with respect to, inter alia, gender and "any other personal circumstance", if the act is committed in a manner that can jeopardise or disturb public law and order, or

with the use of threats, verbal abuse or insults. However, the offence is not particularly well-suited to protect women victims of digital forms of violence, as the perpetrator's behaviour must influence the will, reason, emotions and passions of other people. Expressing derogatory, dismissive, negative or otherwise hostile views directed against women (or other protected groups) is not in itself sufficient to constitute a criminal offence (Great Scientific Commentary of the Special Part of the Criminal Code KZ-1, Volume 3, p. 475). Moreover, until the landmark Supreme Court Judgement I Ips 65803/2022 from 4 July 2019, the prosecution relied on "Legal Position on the Prosecution of a Criminal Offence Public incitement to hatred, violence or intolerance under Art. 297 KZ-1" (adopted by the College of the Criminal Division of the Supreme State Prosecutor's Office on 27 February 2013) according to which the offence was not sufficiently used in practice because prosecutors interpreted it as meaning an act that would imminently jeopardise or disturb public order which often is not the case particularly in instances of violence against women and girls.

Alongside an offender, editor or person acting as an editor may be punished to the same extent if an offence is committed by publication in the mass media or "on websites", except if this involves the live broadcast of a show that the editor cannot prevent or publication on a website that enables users to publish content in real-time or without prior review. The Criminal Code KZ-1 still uses the obsolete notion of a website, but social media or messenger services could also be regarded as "websites".

- **The use of the hate speech offence following the Supreme Court judgement should be monitored to ensure the offence is effective in practice. It is also unclear whether the offence as currently drafted would cover hate speech in mobile and other applications, including messenger services such as Telegram, Signal or WhatsApp, which could lead to hate speech being allowed to proliferate in quasi-private groups.**

Trolling may also fulfil elements of several offences protecting honour and reputation. **Crimes Against Honour and Reputation** (Chapter 8 of the KZ-1) includes offences that can be committed digitally against women: Insult (*Razžalitev*, Article 158), Slander (Obrekovanje, Article 159), Defamation (*Žaljiva obdolžitev*, Article 160), Calumny (Opravljanje, Article 161), Contemptuous accusation of a criminal offence (Article 162) can all be committed via digital services, such as on social media. According to theory, the **insult** reflects disparagement, it is contempt, disregard for another person's dignity, ridicule, ascribing negative character traits to another or expressing a negative judgement of another's worth.[21] The offence **Slander** incriminates making false claims or spreading untruths about someone even though a person knows that what he claims or spreads is untrue and by doing so damages the victim's honour or reputation. An aggravated form is stipulated for an act committed through mass media and "websites". The **Defamation** offence criminalises claims or circulation of a statement of fact and not value judgements about someone. The "proof of truth" is allowed, which means that if the suspect proves the veracity of his or her claims or that he or she had a valid reason to believe in the truthfulness of what he or she claimed or circulated, he or she shall not be punished for defamation. However, the suspect may be punished for insult (Art. 158) or for the false and Contemptuous accusation of a criminal offence (Art. 162). **Calumny** commits whoever claims or circulates any information about the personal or family affairs of another person which could tarnish that person's honour and reputation; the "proof of truth", i.e. to prove in court the veracity of what has been claimed or circulated about another person's personal or family life, is not allowed. The issue being about personal or family affairs is enough, except in cases of the performance of an official duty, or a political or other social activity. Aggravated forms are stipulated for cases of an act committed through mass media and "websites" and for grave consequences for the victim. For **Contemptuous accusation of a criminal offence**, accusations must be made with the intention to expose a victim to contempt. An aggravated form is stipulated for an act committed through mass media and "websites".

In the case of "swatting", i.e. the use of telephones or computer systems to deceive an emergency service in order to send law enforcement to a specific location based on a false report, a person may commit the offence of **Abuse of distress and warning signals** (Article 309 of the KZ-1). The statutory elements of the offence include "making an unwarranted call for help" or "providing false information on a threat", thus causing the public authorities or other authorised organisations to act without the necessity.

- **Ensure that any existing gaps in the law that relate to harassment offences committed by strangers or in private space are remedied. In particular, ensure that the law reflects the repeated or continuous nature of harassment in addition to criminalising one-off offences.**

21. Slovenia, KZ-1 Commentary, Book 1, p. 986.

In conclusion, it would therefore appear that harassment in the context of work and harassment in the context of a familial or personal relationship (considered below under domestic violence) is covered by the law. It does however appear that there is a gap in the legislation in respect of harassment where the person is unknown to the perpetrator. Although the constituent elements of harassment appear above, there is nothing that clearly encompasses the repeated or continuous nature of this offence. There also appears to be a distinction between harassment committed publicly and harassment committed privately which, although important, could lead to gaps in protection. Finally, the unsolicited sending of images, videos or other material depicting genitals has not been criminalised.

Online and technology-facilitated stalking

Article 34 of the Istanbul Convention defines stalking as 'intentional conduct of repeatedly engaging in threatening conduct directed at another person causing him or her to fear for his or her safety.' It can be ongoing even if the victim changes her residence (Volodina v. Russia, ECtHR).

The Explanatory Report to the Istanbul Convention further clarifies this definition and acknowledges that stalking committed via the use of ICT is covered by Article 34.

The threatening behaviour may consist of repeatedly following another person, engaging in unwanted communication with another person, or letting another person know that he or she is being observed. This includes physically going after the victim, appearing at her or his place of work, sports or education facilities, as well as following the victim in the virtual world (chat rooms, social networking sites, etc). Engaging in unwanted communication entails the pursuit of any active contact with the victim through any available means of communication, including modern communication tools and ICT devices.

Stalking in the digital sphere includes threats (of a sexual, economic, physical or psychological nature), damage to reputation, monitoring and gathering of private information on the victim, identity theft, solicitation for sex, impersonating the victim and harassing with accomplices to isolate the victim. It usually involves the tactic of surveilling or spying on the victim, on their various social media or messaging platforms, their e-mails and phone, stealing passwords or racking or hacking their devices to access their private spaces, via the installation of spyware or geo-localisation apps, or via stealing their devices. Perpetrators can also take on the identity of the other person or monitor the victim via technology devices connected through the Internet of Things (IoT), such as smart home appliances.

Stalking offence (*Zalezovanje,* Article 134a of the KZ-1) incriminates repeated observation, pursuit or intrusive efforts to establish direct contact or unwanted contacts physically or via electronic means of communication. A qualified form of the offence is stipulated when a person being stalked is a minor (§ 2). Stalking can be directed against a victim or against someone close to her, and it must lead a victim (or someone close to her) to fear for their safety or a feeling of being threatened. The prosecution is initiated upon a victim's proposal only (§ 3).

Stalking may also potentially be dealt with as a misdemeanour under the Protection of Public Order Act (*Zakon o varstvu javnega reda in miru*, ZJRM-1). The misdemeanour "**Violent and reckless behaviour**" (Art. 6 of the ZJRM-1) stipulates that a person who provokes another person or instigates a fight or acts in a reckless, violent, rude, offensive, or *similar manner* or *follows another person and* thereby causes a feeling of humiliation, endangerment, distress, or fear shall be fined. If the misdemeanour is committed against a (former) partner, a close relative or a person living in a shared household (§ 3 Art. 6)[22], the fine is higher. It is not clear whether "following" should be understood as digital following someone, similar to a criminal offence stipulated in the Art. 134a of the Criminal Code. However, the element "in a similar manner" could be interpreted to cover acts in the digital sphere, but more clear provision is needed.

Stalking practices committed in the digital sphere may fulfil statutory elements of several other criminal offences. **Unlawful eavesdropping and audio recording** (*Neupravičeno prisluškovanje in zvočno snemanje*, Art. 137 of the KZ-1) encompasses two forms: the first is committed by unlawfully eavesdropping by means of special devices on a conversation or statement not intended for an offender, while the second is committed by making an audio recording of a confidential statement intended for an offender by another, without his or her consent, with intent to misuse such statement. Instead of eavesdropping, the act can also be committed by recording, directly transmitting to a third person, or otherwise directly enabling access to a third party. For instance, hacking and switching on computer cameras in the victim's home can fulfil statutory elements of this offence. For the first form, the prosecution is initiated upon a victim's proposal, while the second may be initiated only upon a private action.

22. Protection of Public Order Act (Zakon o varstvu javnega reda in miru, ZJRM-1)

Violation of the secrecy of communications (*Kršitev tajnosti občil*, Art. 139 of the KZ-1) protects communication privacy as guaranteed by the Constitution of the Republic of Slovenia (Art. 37). The offence can be committed by someone who takes undue note of a message transmitted by telephone or any other means of electronic telecommunication with the use of technical means (§1, point 2 of the KZ-1). For instance, the Supreme Court of the Republic of Slovenia identified as "other means of electronic telecommunication" a secretly photographing a victim's mobile phone screen at a distance and improving the photo in postproduction in order to identify the content of the message on the screen (Judgement I Ips 3155/2014 from 15 December 2016).

Stalking practices may come in the form of **hacking** victim's devices, e.g., installing spyware to track the activities of the device (stalkerware). Attack on an information system (Art. 221 of the KZ-1) is an offence committed by unlawfully entering or breaking into an information system or unlawfully intercepting data during a non-public transmission (§ 1). An aggravated form of the offence is committed when a person makes unlawful use of data in an information system, or changes, copies, transmits, destroys, or illegally imports data into an information system, or obstructs data transmission or the operation of an information system (§ 2).

- **From the above information it would appear that Slovenia has a legal framework that is capable of covering stalking by digital means. Consideration may be given to ensuring that the misdemeanour in the Protection of Public Order Act is adequate to cover stalking in the digital environment or by digital means.**

Digital dimension of psychological violence

Article 33 of the Istanbul Convention describes psychological violence as "the intentional conduct of seriously impairing a person's psychological integrity through coercion or threats". As explained in the Explanatory Report to the convention, the provision refers to a course of conduct rather than a single event and is designed to capture the criminal nature of an abusive pattern of behaviour occurring over time within or outside the family.

All forms of violence against women perpetrated in the digital sphere have a psychological impact and could fall under this definition. Online psychological violence can be threats, whether in text, visual or verbal format, use of actual images or generative AI to perpetuate image-based abuse. It may also take the form of threatening the victim's family, insults, shaming and defamation. Incitement to suicide or self-harm is a specific behaviour online. Most forms of online violence can be amplified or exacerbated by the reach of the internet, mob mentalities, and focused or targeted attacks. AI may be used to facilitate or generate large-scale attacks, increasing the harm to the victim.[23]

Economic abuse, which is another form of psychological violence, can manifest itself in the digital sphere as controlling the bank accounts and financial activities of the victim through internet banking, damaging the victim's credit rating by using credit cards without permission or filing all financial contracts (leases, loans, utilities, etc.) in the name of the victim and failing to make payments on time or at all (in particular alimony payments)[24]. Women may also become victims of cyber extortion and financial exploitation, where money is demanded under threat of exposing compromising images or online activity.

Psychological violence is not specifically criminalised in Slovenia although the offences discussed above of criminal coercion (Art. 132 of the Criminal Code, KZ-1), threat (Art. 135 of the KZ-1) and workplace mobbing (Art. 197 of the KZ-1) could cover some of the forms of psychological abuse frequently experienced by women.[25]

In the context of domestic violence, however, Slovenia has both criminal and civil law provisions to protect victims of psychological violence committed in or through digital means.

The criminal offence of **Domestic Violence** (*Nasilje v družini*, Art. 191 of the KZ-1) focuses on the family community (§ 1) and a permanent living community (§ 2). The two communities are not defined in either KZ-1 or Family Code (*Družinski zakonik*),[26] as the latter protects families – communities of a child and one or both parents. According to the Supreme Court of the RS, a family community is "a community in which the members have various ties and relationships that are economically, psychologically and biologically conditioned, and which are governed or determined not only by law but also by tradition and the immediate social environment. Domestic violence is usually about the abuse of these relationships, or of the relationships that have been established between members of the community."[27] Moreover, the Domestic Violence Prevention Act, which[28] defines a family member very broadly (Art. 2) for its own purposes of providing protection measures against victims of crime (and not punishing offenders), should be used supplementary to KZ-1, according to the Supreme Court decision.[29] "Permanent living community" is also not defined in the Criminal Code (KZ-1), but it has to resemble familial or other relationships from the Domestic Violence Prevention Act in terms of rights, obligations and emotional ties between its members.[30] It is important to note that, when assessing the existence of a family or living community, its members do not necessarily need to reside together. However, if violence was committed after the community of people that lived together broke up and the violent act is

23. Choudhury, Rumman, Lakshmi Dhanya, UNESCO (2023))
24. GREVIO General Recommendation No. 1, para 48
25. GREVIO Baseline Evaluation Report, Slovenia E, para 243
26. Family Code (*Družinski zakonik*), adopted 21 March 2017.
27. Supreme Court of the Republic of Slovenia, Judgement RS I Ips 194/2009 from 3 September 2009.
28. Domestic Violence Prevention Act (Zakon o preprečevanju nasilja v družini), adopted 1 February 2008.
29. Supreme Court of the Republic of Slovenia, Judgement RS I Ips 16812/2015-108 from 15 December 2016.
30. Korošec, D.; Filipčič, K.; Devetak, H. (2023) p. 313.

linked to the community, then an offence under (§ 3 Art. 191) of the Domestic Violence may be committed. Of some concern is that a mitigating form of offence (§ 3 Art. 191) is committed against a person with whom the perpetrator had lived in a family or other permanent community that broke up, since digital forms of violence typically increase after break-ups of relationships.

The basic form of the Domestic Violence offence is committed by treating another family member badly, beating her, or, in any other way, treating her in a painful or humiliating manner. It is also committed by expelling a family member from their joint residence by threatening with a direct attack on her life or body, or in any other way limiting her freedom of movement, stalking her, forcing her to work (or to give up her work), or in any other way putting her into a subordinate position by aggressively limiting her equal rights. Several of these forms can be committed digitally, e.g. stalking as the clearest example, but also treating badly or treating in a painful or humiliating manner. The offender may be sentenced to imprisonment for up to five years.

The Domestic Violence Prevention Act specifically includes the ability to commit psychological harm through digital means. Art. 3 (§ 5) states, "psychological violence are actions and the dissemination of information with which the perpetrator of violence causes the victim fear, humiliation, a feeling of inferiority, threat and other mental distress, including when committed using information and communication technology." Definitions of violence are also very broad in the Domestic Violence Prevention Act, e.g. psychological violence can be perpetrated by commission and omission and, hence, also includes ignoring or excluding someone from the social media circle of "friends".

Psychological violence may come in the form of **solicitation to suicide**. The offence of Solicitation to and assistance in suicide (*Napeljevanje k samomoru in pomoč pri samomoru*, Art. 120 of the KZ-1) can be committed by intentionally soliciting suicide via digital services. An aggravated form is committed if the victim is a minor above fourteen years (§ 2). When a minor is under fourteen years of age, the act is punished in the same manner as manslaughter or murder. A case of, e.g. sextortion or cyberbullying, may fall under § 4, which stipulates that whoever treats his or her subordinate or a person who is his or her dependant in a cruel or inhuman manner, resulting in this person's suicide will be sentenced to imprisonment for between six months and five years.

- **In recognition of the fact that online psychological violence can take place outside the context of personal relationships, including often being perpetrated by strangers and without additional motive, Slovenia may wish to review whether psychological violence, either in general or specifically in the digital sphere, should be incorporated into the Criminal Code.**

Other forms of violence against women in the digital dimension

Physical violence in the digital sphere

The offence **Violent conduct** (*Nasilništvo*, Art. 296 of the KZ-1) has traditionally been understood as physical violence and was not adopted from a digital dimension perspective. However, the courts have extended its scope as the object of protection is the personal safety, physical and mental integrity and freedom of movement of the person. Some of the statutory elements of the offence can be committed with digital tools or in digital space. For instance, while beating is conventionally understood as physical conduct, "other ways of painful or humiliating punishing", "threat of imminent attack on life and limb" (e.g. courts have recognised such a threat sent in the form or SMS - Short text message), "forcing someone to work or to abandon work", "otherwise putting someone in a subordinate position by violently restricting his or her equal rights", can be committed digitally. Importantly, the intensity of the offender's behaviour may not result in any bodily injury; if it does, which will not be possible with digital tools,[31] an aggravated form will be committed (§ 2). The offence consumes several other offences which are typically part of gender-based violence, such as Threat (*Grožnja*, Art. 135 of the KZ-1); Coercion (*Prisiljenje*, Art. 132), Insult (*Razžalitev*, Art. 158).[32] Violent conduct differs from these offences in that it requires the victim to assume a subordinate position, which indicates "the exercise of violence for violence's sake, the extortion of violence, where the victim becomes the object of violence which he or she is unable or incapable of avoiding".[33]

Other offences in the Criminal Code's chapter Crimes against sexual integrity (Chapter 19) may be relevant only to some extent, as they do not explicitly mention ICT, websites or digital technology. While the legal theory acknowledges that physical contact is not necessary for the concept of sexual behaviour between people, the Commentary does not analyse digital tools that can be misused, e.g. in virtual sexual encounters ("teledildonics") or with specific VR (Virtual reality) or haptic technologies. For the offences of **Rape** (Art. 170 of the KZ-1) and **Sexual violence** (Art. 171 of the KZ-1) to be committed, physical contact is necessary.[34] Similarly, physical contact is fundamental for an offence of **Sexual assault on a person younger than fifteen years of age** (Art. 173 of the KZ-1), which criminalises as a basic form of sexual intercourse or performing any other sexual act with a person of the same or opposite sex under the age of fifteen years. However, it is not yet clear, whether the law will recognise physical contact that has been technologically mediated via, e.g. full-body haptic suit.

31. It is doubtful if virtual reality equipment (e.g. body suits) can result in light injuries if the offender intends to cause harm since such equipment should be certified and disable such strong stimulus.
32. Slovenia, KZ-1 Commentary, Book III, p. 462.
33. Judgement Supreme Court of the Republic of Slovenia, I Ips 166/2010 from 17 March 2011.
34. See commentary, book 1, p. 1186, for the analysis of the notion of what counts as a "sexual act" in the context of the Sexual violence offence (Art. 171).

Protection

A range of measures to protect injured parties and witnesses from secondary victimisation, intimidation, or retaliation are available to Courts in Slovenia. The selection of these measures is based on an individual assessment of the victim, which is prepared by state authorities – such as the police, prosecution, or court – during the initial contact with the victim.[35] The individual assessment determines the extent to which the victim needs special protection (Article 143č of the Criminal Procedure Act, ZKP).

The **Ministry of Justice of the Republic of Slovenia**[36] indicated that in 2024, a new form for assessing the risk of victims of crime was put into practice, allowing for a more realistic assessment of the risks to victims of crime. Most of the questions are designed to take into account the requirements of the EU Directive on combating violence against women and domestic violence. The Ministry of Justice has tested the questionnaire with concrete closed cases.

In addition, the Ministry of Justice referred to the recently implemented amendment to the Criminal Procedure Act (ZKP-P),[37] which provides for a new entity, 'The Victim Support Service', that can make an individual assessment of the victim's risk and can now also prepare or amend the assessment, as it has contact with victims when they are summoned to court. (In practice, there are currently two such services – at the District Court in Ljubljana and Maribor). Under the previous regime, only the police and the public prosecutor's office could complete or supplement the threat assessment.

- **The protection measures outlined in the legislation are not specifically adapted to the digital dimension of violence against women and domestic violence, however, they do, in principle, broadly reflect good practice in supporting women and girls through the court process and encompass ICT communication in restraining orders.**

Availability of information

The Ministry of Justice (*Ministrstvo za pravosodje*) keeps an updated webpage on criminal procedure and publications about rights are published in several languages (Italian, Hungarian, English, German, Croatian). The Police maintains a webpage with key information for victims of domestic violence (English, Italian, Hungarian, Croatian, Romani etc.). This information does not currently cover the digital dimension of violence against women or domestic violence but is more general in nature.

- **Develop and disseminate information on the legal avenues and support services available to victims of violence against women perpetrated in the digital sphere and create online and offline complaints mechanisms within law enforcement and prosecution services that are easily and immediately accessible to women.**

Immediate response measures to protect victims

35. Šugman, K., Gorkič, P., Fišer, Z. (2020). Temelji kazenskega procesnega prava. Ljubljana: GV založba, pp. 292-293.
36. Correspondence from 21 October 2024
37. Act amending and supplementing the Criminal Procedure Act, ZKP-P (*Zakon o spremembah in dopolnitvah Zakona o kazenskem postopku*, ZKP-P), Official Gazette of the Republic of Slovenia, No. 53/24 from 19 June 2024.

Restraining and protection orders

Amendments to the Criminal Procedure Act (*Zakon o kazenskem postopku, ZKP*) and the Criminal Code (*Kazenski zakonik, KZ-1*) have led to the possibility of a restraining order to be imposed throughout the entire procedure, i.e. in pre-trial phase and in main criminal proceedings, with deferred prosecution measure, and also in the phase of enforcement of criminal sanctions. Probation decisions may also include a restraining order. The restraining order can always include restrictions on communication by electronic means.

A restraining order may be issued according to several legal grounds. A restraining order may be issued according to the Criminal Code (Art. 71a) as a form of security measure in addition to a sentence. The police may impose a restraining order against a person, place or area pursuant to Art. 60 of the Police Tasks and Powers Act (*Zakon o nalogah in pooblastilih policije*, ZNPPol)[38] for 48 hours. The measure must be confirmed within 24 hours by the investigating judge, who may extend it for up to 15 days (from the day the restraining order was given orally by the police). The victim may, before the expiry of the restraining order, propose to the same court or judge to extend the measure. The victim must prove she is still under threat (document all statements, text messages, letters, violations of the restraining order, etc.). The court may extend the measure to 60 days. The restraining order can also be issued within the transversal Prevention of Domestic Violence Act (*Zakon o preprečevanju nasilja v družini*, ZPND),[39] according to which, the court can issue a restraining order if the perpetrator of violence has caused physical injury to the victim, damage to the victim's health, or otherwise unlawfully interfered with her dignity or other personal rights (Art. 19). Moreover, the court can issue a restraining order also to the perpetrator of violence if he harasses the victim against her explicit will by, *inter alia*, stalking her or by using means of telecommunication (point 3, §2, Art. 19 of the ZPND); and if the perpetrator harasses the victim by publishing the victim's personal information or personal records referring to the victim (point 3, §2, Article 19 of the ZPND). In this second case, according to the ZPND, the Court can issue the order for a maximum of 12 months, but the victim may apply for an extension of the duration of the measure before the expiry of the period for which the measure was imposed, and the court may extend the duration of the measure several (indefinite) times, but each time for the maximum period of 12 months (§2, Art. 19 ZPND). Motions for protective measures are dealt with by courts as a matter of priority.

NGOs are of the view that digital forms of violence against women are not taken seriously enough by the police. One NGO generally attempts to present a case of digital violence against women in the form of either an offence of Stalking (Art. 134a of the KZ-1) or Domestic violence (Art. 191 of the KZ-1), which then provides more chances to be taken seriously by the police. They are also of the view that the restraining order system is "not working in practice" because there is no proper and consistent escalation of the sanctions against the perpetrator.

The police, however, report that offenders comply with restraining orders in 80 percent of cases. In the remaining 20 per cent of cases, Police (may) issue a fine and keep an offender in police custody for 12 hours (according to The Police Tasks and Powers Act, ZNPPol). They mention that the victim's fear, i.e. how frightened the victims are, is an important factor in deciding on the escalation of measures.

Between 2021 and 2023, the Institute of Criminology at the Faculty of Law carried out a **research project entitled Restraining Order**, which also analysed restraining orders imposed in the period 2010-2021 and evaluated the effectiveness of the measure. According to its findings,[40] 20 percent of perpetrators breach the order increasing to 30 percent if perpetrators are former intimate partners/husbands. The Institute also found that harassment by telecommunications is the predominant way of breaching the restraining order (36 percent).

- **The existence and use of restraining orders to cover the digital dimension of violence against women could be reviewed to ensure appropriate follow-up action is taken in cases of breach.**

- **Research could be conducted to examine whether, and if so, how, digital restrictions are imposed on offenders who stalk, harass or otherwise commit violence against women in the digital sphere to examine the success and gaps in implementation.**

38. Slovenia, The Police tasks and powers act (*Zakon o nalogah in pooblastilih policije*), 30 January 2013, and subsequent modifications.
39. Slovenia, The Domestic violence prevention act (*Zakon o preprečevanju nasilja v družini*), 1 February 2008, and subsequent modifications.
40. Filipčič, K.; Bertok, E. (2024).

Take down procedures

The Criminal Police Directorate, General Crime Division (Policija, *Uprava kriminalistične policije, Sektor za splošno kriminaliteto*) reported on well-established procedures for taking down child abuse material from social media platforms, however, when adult individuals are depicted in digital material, the procedure for takedown without a judicial order is complicated and tech companies will not react. The police stated that companies will take down material only if the material belongs to a victim, e.g. the material is stolen from or depicts a victim. If the disputed act is "only" a misdemeanour, the police believe they cannot do much ("our hands are tied"). The police themselves have no removal or take down agreement with the technology companies.[41]

In general, the police noted that social media platforms have helpdesk contacts where users can ask for content to be removed themselves. In child sex abuse and exploitation cases, the companies sometimes detect the material themselves, and the content is then removed and sent to the USA-based non-profit company NCMEC.[42] The NCMEC then forwards the requests to the individual countries or via Europol.[43] NCMEC accepts reports from providers of various networks. Hence, the Slovenian Police receive these reports via Europol. If the Police itself needs information in the course of investigating a crime, for example, if they need registration data and the IP address, they work directly with the providers. E.g. if an unknown offender has committed sexual abuse via a Snapchat profile, a police officer obtains a warrant and sends it directly to Snapchat via the channel the company has for cooperating with security authorities.

This is consistent with the views of NGOs interviewed, who stated that in most cases where they seek to remove material, they turn to the police. The NGO Association for Non-Violent Communication also often refers women victims to the national CERT team. A university-led platform, "Internet Eye" (*Spletno oko*,), which describes itself as a platform for reporting images of child sex abuse on the internet, also offers reporting for "sextortion" and sexting.

There are clear gaps and difficulties in successfully accessing take-down mechanisms for adult women.

The Slovenian authorities could:

- **Take action to ensure women have effective access to content take-down procedures, including help and support to remove content.**
- **Incentivise internet intermediaries, including ISPs, search engines and social media platforms, to ensure robust moderation of content that falls within the scope of the Istanbul Convention through the removal of accounts or content in multiple languages on the basis of transparent principles that protect the human rights of all. Require these intermediaries to provide easily accessible user guidance to flag abusive content and request its removal.**
- **Encourage media companies to work collaboratively with law enforcement agencies.**

41. Correspondence with the Police representative Robert Tekavc from 14 November 2024.
42. https://www.missingkids.org/HOME
43. The legal basis for the companies to do this in the EU area is the Regulation EU2021/1232

Prosecution

The report of GREVIO on Slovenia following the baseline evaluation procedure was published in 2021. GREVIO strongly encouraged the Slovenian authorities to develop and implement investigation and prosecution guidelines and to conduct specialist training on the gendered and serious nature of domestic violence, including its digital and post-separation dimension.[44]

The NGO Association for Non-Violent Communication reports on the regional differences in Police reactions in their first contact with victims. The police are reluctant to act, especially in rural areas where the police stations are understaffed and without specifically trained personnel for cases of this type of violence.

As identified above the legal framework itself creates some difficulties in ensuring successful investigations and prosecutions in respect of new offences of digital dimension of violence including potentially the classification of some incidents as 'misdemeanours' rather than more serious crimes (see, for example, Protection of Public Order Act). This is in part owing to the 'new' nature of these crimes and partly because some of them are not specific but included within general provisions. This is an area where guidance may assist stakeholders to ensure justice.

Slovenia may consider taking measures to ensure:

- **Law enforcement and other criminal actors are properly trained, issued with appropriate guidance and protocols and equipped with the necessary resources to effectively investigate and prosecute the digital dimension of violence against women in line with their due diligence obligations under Article 5 of the Istanbul Convention.**
- **Ensure women in all areas of Slovenia are able to access justice in respect of the digital dimension of violence against women by developing guidance, training and standardised protocols for all relevant agencies and municipalities.**
- **Improve cooperation between media companies and law enforcement agencies, particularly in respect of adult women victims of digital crimes.**

Coordinated Policies

Addressing the digital dimension of violence against women requires a comprehensive approach that integrates digital policies with existing legal frameworks on women's rights and criminal regulations. This integration is crucial for providing comprehensive protection, ensuring accountability and promoting a safe digital environment. The methods by which the digital aspect of violence against women is perpetrated, its investigation, forensic and prosecution protocols and the specific needs of victims need to be set out in policy.

Slovenia has included a response to forms of violence against women and girls in its digital dimension in three national strategies, as discussed below.

Central Resolutions adopted by the Parliament

The two most recent and relevant policies for preventing and responding to also digital forms of violence against women are the overarching Resolution on the National Programme for the Prevention and Suppression of Crime 2024-2028 (*Resolucija o nacionalnem programu preprečevanja in zatiranja kriminalitete za obdobje 2024–2028*), and the more specific Resolution on the National Programme for the Prevention of Domestic Violence and Violence against Women 2024-2029 (*Resolucija o nacionalnem programu preprečevanja nasilja v družini in nasilja nad ženskami 2024-2029*), both from 26 April 2024.

44. GREVIO, Baseline Evaluation Report, Slovenia, p. 52

The Resolution on the National Programme for the Prevention and Suppression of Crime 2024-2028 indicates goals related to the online/digital sphere, such as the goal to establish a national police unit to investigate sexual abuse of children via the internet, with a focus on identifying victims; establishing cooperation between all relevant stakeholders on hate speech, including state authorities and institutions, as well as the non-governmental sector, civil society initiatives, interest groups, the education, science and research sectors, internet and media providers; ensure the implementation of existing national awareness-raising and education programmes (Safe on the Internet, Safer Internet Centre (SAFE. SI, TOM telefon, Web Eye)), build on them, extend them and reach out to new target groups of users.

In regard to prevention and fight against hate speech, the Resolution identifies as particularly harmful hate speech directed to minorities and vulnerable and deprivileged groups, with the aim to oppress and subordinate these groups and create an intimidating and humiliating environment. The causes of hate speech are manifold, including power imbalances when individuals or groups use hate speech as a means of exerting their power over others. The power imbalance between men and women is, therefore, also reflected in the use of hate speech as a means for men to assert their power over women, according to the Resolution.

The Resolution mentions domestic violence, bullying among children and violence against women as three important forms of violence to be addressed in the coming period. As a specific form of peer violence, it mentions forms of psychological violence involving the misuse of modern ICT (internet, mobile telephony). It also identifies violence against children on the Internet or cyberbullying as a form of violence which needs to be addressed due to the development of ICT in the last 20 years, in particular, the Internet, various online software solutions and social media. The Resolution recognises that despite the positive features of ICT, its vulnerability, as well as the ignorance and naivety of children and adolescents and the passivity of their parents, are readily exploited by individual perpetrators or organised crime groups seeking to pursue their financial or material interests as well as their sexual paraphilias or preferences (see Strategy/programme 7.2.4.2).

The Resolution on the National Programme for the Prevention of Domestic Violence and Violence against Women 2024-2029 is the new comprehensive strategic document, which addresses *inter alia* also the digital dimension of violence against women. The Resolution is the umbrella document for tackling domestic violence and violence against women, and it has been 15 years, or seven governments, since the last adoption of such a document. The adoption of this Resolution is a positive move.

The Resolution contains a commitment to pay special attention to preventing online violence and harassment (p. 2). Among its OBJECTIVE 3 (Ensuring highly trained and professional staff to deal with domestic violence, **violence against women** and victims of such violence in their work), the Resolution stipulates a measure to train professional providers of social welfare programmes, workers in the judiciary and police on the sexual nature of **stalking** and its online dimension (p. 26). Among its OBJECTIVE 4 (Achieving zero tolerance of domestic violence and **violence against women**, high social awareness and preventive action), the Resolution envisages the following measures: regular annual awareness-raising and training on online violence against women and children for primary and secondary school pupils and students, which includes awareness of reporting violence (Measure no. 8, p. 30); Regular training and information on the pitfalls of online violence against **children** for educators and practitioners (Measure no. 9, p. 31); Raising parents' awareness of the pitfalls of online violence (Measure no. 10, p. 31).

In 2023, **the Resolution on the National Programme for Equal Opportunities for Women and Men 2023-2030** (*Resolucija o nacionalnem programu za enake možnosti žensk in moških za obdobje 2022-2030*) was adopted, which pursues objectives in the area of prevention of violence against women, including improved professional capacity and awareness of online violence by including a gender perspective (Goal 3, 2.4.3). It plans two measures: 1) Conducting training for professionals and women on online violence, in particular on online sexual abuse. 2) Raising public awareness, especially among young people, of the dangers and consequences of online violence and working with NGOs on various projects on online violence.

Relevant research

From 2017 to 2019, the EU project **Unclick! - Stop Online Violence and Harassment against Women and Girls** (*Odklikni – Ustavi spletno nasilje nad ženskami in dekleti*)[45] was implemented to build on national activities to prevent online violence by including a gender perspective in materials, training and education modules,

45. https://odklikni.enakostspolov.si

recommendations and actions. The results were also aimed at raising awareness among the general public, with the creation of promotional spots, leaflets, posters,[46] e-posters etc.[47]

- **Relevant national action plans, strategies and other relevant policies already embrace a great number of aspects of how to address the digital dimension of violence against women and girls over the age of 15 as well as younger children. However, the list of activities could be more coherent and activities more centrally monitored. These policies and those on digitalisation should include the development of appropriate co-operation mechanisms both across different sectors, including the NGO sector, and ensuring engagement with the private and ICT sectors.**
- **Undertake or support quantitative and qualitative research programmes and studies on the digital dimension of violence against women to understand the extent and nature of the problem and measure the financial, personal and social impacts of such violence, including self-censorship and digital exclusion.**

46. https://odklikni.enakostspolov.si/wp-content/uploads/2018/10/ANG_MDDSZ_ODKLIKNI_plakati_A2_v6_MKL4.pdf
47. https://odklikni.enakostspolov.si/wp-content/uploads/2018/10/ANG_MDDSZ_ODKLIKNI_brosura_A5_v5_MKL.pdf

Recommendations

Prevention

In respect of the law on online harassment, it is recommended that Slovenia considers:

- Reviewing the criminal law to ensure image-based abuse in all its forms and across all digital media is appropriately criminalised and sanctioned. In particular, consideration should be given to the methods of unlawful sharing of information and whether 'private' sharing of information as opposed to 'public' sharing is appropriately covered. Consideration may also be given to whether reform is required to paragraph 143/6 of the Criminal Code (KZ-1) to remove the requirement of severity on the grounds that sharing material containing sexual content without consent is sufficiently serious in and of itself. Issues with respect to severity would continue to be relevant to punishment.
- Review and amend the law to clearly address cyberflashing in public and in private, whether as a misdemeanour or criminal offence
- Review the criminal law on the presentation, manufacture, possession and distribution of pornographic material to make sure it adequately covers the digital dimension and consider whether the law adequately covers digital pornographic offences committed against adults, e.g. women whose images are used to create pornography without their consent.
- There is a gap in respect of online grooming of victims over the age of 15 which should be reviewed. The provision on solicitation reflects the European Convention on Action against Trafficking in Human Beings at Article 23 in respect of grooming children under the legal age of consent for sexual activity. The digital dimension of violence against women and domestic violence can lead to women also being groomed online either for human trafficking or for other forms of manipulation and exploitation. It does not appear that the legal framework currently covers these acts for adult women (or men). Moreover, Slovenia could consider extending the grooming provision to cover other crimes of exploitation in the context of digital violence.
- Review the law to ensure that threats, coercion, extortion and blackmail in the digital sphere that constitute harassment are sufficiently criminalised, recognising both the often 'private' sphere in which the offences take place and the relevant impact of repeated events and a course of conduct.
- The use of the hate speech offence following the Supreme Court judgement should be monitored to ensure the offence is effective in practice. It is also unclear whether the offence, as currently drafted, would cover hate speech in mobile and other applications, including messenger services such as Telegram, Signal or WhatsApp, which could lead to hate speech being allowed to proliferate in quasi-private groups.
- Ensure that any existing gaps in the law that relate to harassment offences committed by strangers or in private spaces are remedied. In particular, ensure that the law reflects the repeated or continuous nature of harassment in addition to criminalising one-off offences.

In respect of Online and technology-facilitated stalking:

- It would appear that Slovenia has a legal framework that is capable of covering stalking by digital means. Consideration may be given to ensuring that the misdemeanour in the Protection of Public Order Act is adequate to cover stalking in the digital environment or by digital means

In respect of the digital dimension of psychological violence:

- In recognition of the fact that online psychological violence can take place outside the context of personal relationships, including often being perpetrated by strangers and without additional motive, Slovenia may wish to review whether psychological violence, either in general or specifically in the digital sphere, should be incorporated into the Criminal Code.

Protection

The protection measures outlined in the legislation are not specifically adapted to the digital dimension of violence against women and domestic violence, however, they do, in principle, broadly reflect good practice in supporting women and girls through the court process and encompass ICT communication in restraining orders. In terms of information available to victims, however, Slovenia could:

- Develop and disseminate information on the legal avenues and support services available to victims of violence against women perpetrated in the digital sphere and create online and offline complaints mechanisms within law enforcement and prosecution services that are easily and immediately accessible to women.

Restraining and protection orders

- The existence and use of restraining orders to cover the digital dimension of violence against women could be reviewed to ensure appropriate follow-up action is taken in cases of breach.
- Research could be conducted to examine whether, and if so, how, digital restrictions are imposed on offenders who stalk, harass or otherwise commit violence against women in the digital sphere to examine the success and gaps in implementation.

Take-down measures could be improved, including:

- Take action to ensure women have effective access to content take-down procedures, including help and support to remove content.
- Incentivise internet intermediaries, including ISPs, search engines and social media platforms, to ensure robust moderation of content that falls within the scope of the Istanbul Convention through the removal of accounts or content in multiple languages on the basis of transparent principles that protect the human rights of all. Require these intermediaries to provide easily accessible user guidance to flag abusive content and request its removal.
- Encourage media companies to work collaboratively with law enforcement agencies.

Prosecution

Slovenia should take measures to ensure:

- Law enforcement and other criminal actors are properly trained, provided with guidance and protocols and equipped with the necessary resources to effectively investigate and prosecute the digital dimension of violence against women in line with their due diligence obligations under Article 5 of the Istanbul Convention.
- Ensure women in all areas of Slovenia are able to access justice in respect of the digital dimension of violence against women by developing guidance, training and standardised protocols for all relevant agencies and municipalities.
- Improve cooperation between media companies and law enforcement agencies, particularly in respect of adult women victims of digital crimes.

Coordinated Policies

Relevant national action plans, strategies and other relevant policies already embrace a great number of aspects of how to address the digital dimension of violence against women and girls over the age of 15 as well as younger children. However, the list of activities could be more coherent and activities more centrally monitored. These policies and those on digitalisation should include the development of appropriate co-operation mechanisms both across different sectors, including the NGO sector, and ensuring engagement with the private and ICT sector.

Undertake or support quantitative and qualitative research programmes and studies on the digital dimension of violence against women to understand the extent and nature of the problem and measure the financial, personal and social impacts of such violence, including self-censorship and digital exclusion.

References

United Nations

CEDAW 1981, United Nations Convention on the Elimination of all forms of Discrimination Against Women, available at: https://www.ohchr.org/sites/default/files/Documents/ProfessionalInterest/cedaw.pdf [accessed 20-Jan-25]

A/RES/54/4 Optional Protocol to the Convention on the Elimination of All Forms of Discrimination against Women, available at: https://www.ohchr.org/en/instruments-mechanisms/instruments/optional-protocol-convention-elimination-all-forms [accessed 20-Jan-25]

CEDAW 1992 UN Committee on the Elimination of Discrimination Against Women (CEDAW), CEDAW General Recommendation No. 19: Violence against women, 1992, available at: https://www.un.org/womenwatch/daw/cedaw/recommendations/index.html [accessed 25 June 2024]

CEDAW 2017a, CEDAW/C/GC/35 General Recommendation No. 35 (2017) on gender-based violence against women, updating general recommendation No. 19 (1992), available at: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-recommendation-no-35-2017-gender-based [accessed 25 June 2024]

CEDAW 2017b, CEDAW/C/GC/36 General Recommendation No. 36 (2017) on the right of women and girls to education, available at: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-recommendation-no-36-2017-right-girls-and [accessed 25 June 2024]

CEDAW/C/SVN/CO/7 Concluding observations on the seventh periodic report of Slovenia, 2 March 2023, available at: https://uhri.ohchr.org/en/document/f5ba215b-474a-463f-8c8e-3625214d4466 [accessed 20-Jan-25]

Council of Europe

CETS No. 185 Budapest Convention on Cybercrime

CETS No. 201 Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse (Lanzarote Convention)

CETS No. 210, The Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention)

CM/Rec (2019) 1 of the Committee of Ministers to member states on preventing and combating sexism, available at: https://rm.coe.int/cm-rec-2019-1-on-preventing-and-combating-sexism/168094d894 [accessed 2 July 2024]

CM/Rec (2022)16 of the Committee of Ministers to member states on combating hate speech adopted 20 May 2022, available at: https://search.coe.int/cm?i=0900001680a67955 [accessed 25 June 2024]

Council of Europe Study (Van der Wilke 2021) 'Protecting women and girls from violence in the digital age', Adriane van der Wilk, Council of Europe (2021), available at: https://edoc.coe.int/en/violence-against-women/10686-protecting-women-and-girls-from-violence-in-the-digital-age.html [accessed 25 June 2024]

ECRI 2015 ECRI General Policy Recommendation No. 15 on Combating Hate, available at: https://www.coe.int/en/web/european-commission-against-racism-and-intolerance/recommendation-no.15 [accessed 25 June 2024]

EDVAW Platform 2022, The digital dimension of violence against women as addressed by the seven mechanisms of the Platform of Independent Expert Mechanisms on Discrimination and Violence Against Women (EDVAW platform)', available at: https://rm.coe.int/thematic-report-on-the-digital-dimension-of-violence-against-women-as-/1680a933ae [accessed 20-Jan-25]

GREVIO Baseline Evaluation Report, Slovenia, 12 October 2021, available at: https://rm.coe.int/first-baseline-report-on-slovenia/1680a4208b [accessed 20-Jan-25]

GREVIO 2021, Recommendation No. 1 on the digital dimension of violence against women, available at: https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147 [accessed 25 June 2024]

PACE 2017a, Parliamentary Assembly of the Council of Europe Recommendation 2098(2017) Ending cyber-discrimination and online hate, available at: https://pace.coe.int/en/files/23456 [accessed 25 June 2024]

PACE 2017b Parliamentary Assembly of the Council of Europe Resolution 2144(2017 on ending cyber discrimination and online hate, available at: https://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-en.asp?fileid=23456&lang=en [accessed 2 July 2024)

PACE 2017c, Parliamentary Assembly of the Council of Europe Resolution 2177 (2017) Putting an end to sexual violence and harassment of women in public space, available at: https://pace.coe.int/en/files/23977 [accessed 25 June 2024]

EU Law

Regulation EU2021/1232 of the European Parliament and of the Council of 14 July 2021 on a temporary derogation from certain provisions of Directive 2002/58/EC as regards the use of technologies by providers of number-independent interpersonal communications services for the processing of personal and other data for the purpose of combating online child sexual abuse, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32021R1232 [accessed 20-Jan-25]

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?toc=OJ%3AL%3A2022%3A277%3ATOC&uri=uriserv%3AOJ.L_.2022.277.01.0001.01.ENG&utm_source=chatgpt.com [accessed 20-Jan-25]

Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ%3AL_202401385 [accessed 20-Jan-25]

Slovenian Law

A selection of relevant Slovenian legislation is available in English at: https://pisrs.si/aktualno/zakonodaja-v-anglescini.

Including:

The Criminal Code (Kazenski zakonik, KZ-1), 20 May 2008, and subsequent modifications.

The Domestic Violence Prevention Act (Zakon o preprečevanju nasilja v družini), 1 February 2008, and subsequent modifications. DVA

Family Code (Družinski zakonik DZ), adopted 21 March 2017

The Protection of Public Order Act ZJRM-1

Opinion 092-4/2024/11, 'Deep fakes as personal information', available at: https://www.ip-rs.si/mnenja-zvop-2/globoki-ponaredki-kot-osebni-podatki-1727941757 [accessed 20-Jan-25]

Articles and webpages

Choudhury, Rumman, Lakshmi Dhanya, UNESCO (2023) "Your opinion doesn't matter, anyway': exposing technology-facilitated gender-based violence in an era of generative AI" available at https://unesdoc.unesco.org/ark:/48223/pf0000387483 [accessed 25/11/24)

Društvo za Nenasilno Komunikacijo (Association for Nonviolent Communication) webpage www.drustvo-dnk.si interview with Tjaša Hrovat from 20 September 2024, [accessed 20-Jan-25]

Filipčič, K.; Bertok, E. (2024). Restraining Orders and Intimate Partner Violence (Slovenian). Journal for Criminalistics and Criminology, 75(1), pp. 44-58, available at: https://www.policija.si/images/stories/Publikacije/RKK/PDF/2024/01/RKK2024-01_KatjaFilipcic_PrepovedPriblizevanja.pdf

Korošec, D.; Filipčič, K.; Devetak, H. (2023). Big Scientific Commentary of the Criminal Code KZ-1, Second Edition, Second book, Uradni list RS, p. 313.

National Centre for Missing & Exploited Children, USA website, available at: https://www.missingkids.org/HOME [accessed 20-Jan-25]

Odklikni Webpage, available at: https://odklikni.enakostspolov.si/raziskave/ [accessed 20-Jan-25]

Odklikni webpage "Cyberbullying it can happen to you too', available at: https://odklikni.enakostspolov.si [accessed 20-Jan-25]

Šugman, K., Gorkič, P., Fišer, Z. (2020). Temelji kazenskega procesnega prava. Ljubljana: GV založba, pp. 292-293.

PREMS 022225

ENG

www.coe.int

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

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE