

PUBLIC POLICY PAPER

ANALYSIS OF NATIONAL LEGISLATION IN RELATION TO EUROPEAN STANDARDS FOR PROTECTION AGAINST DIGITAL GENDER-BASED VIOLENCE



Contents

Executive summary.....	3
1. Introduction	4
1.1. Terminology	5
2. Methodology.....	5
3. International Acts Establishing the Foundations for the Prevention of and Protection from Gender-Based Violence against Women at the National Level	6
3.1 Convention on the Elimination of All Forms of Discrimination against Women (CEDAW).....	6
3.2. Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention).....	7
4. National Legal Framework for the Prevention and Protection from Gender-Based Violence.....	8
4.1. Law on Prevention and Protection from Violence against Women and Domestic Violence.....	9
4.2. Criminal Code	10
4.3. Law on Free Legal Aid	11
4.4. Rights Holders and Duty Bearers	11
5. Review of Compliance with EU Acts Governing the Response to Digital Gender-Based Violence.....	12
6. Overview of the Identified Legal and Institutional Gaps.....	17
6.1. Absence of Comprehensive Regulation of Digital Gender-Based Violence	17
6.2. Limited Substantive Scope of Digital Forms of Violence.....	18
6.3. Insufficient Operationalization of Protective Measures in the Digital Context	18
6.4. Lack of Clear Procedural and Institutional Guidance	18
6.5. Limited Integration Between the Sanctioning System and the Protection System in Cases of Digital Gender-Based Violence.....	18
7. Conclusions.....	19
8. Recommendations.....	19

This document has been produced with the financial assistance of the European Union. The contents of this document are the sole responsibility of [Your Organization/Project Name] and do not necessarily reflect the views of the European Union. The European Union is not responsible for any use that may be made of the information contained herein.

Executive summary

Digital gender-based violence is an increasingly prevalent manifestation of violence against women and girls that is perpetrated, continued, or exacerbated through the use of information and communication technologies. Although this is not a new form of gender-based violence, the digital environment enables different patterns of perpetration, greater exposure of victims, and more enduring consequences, thereby necessitating an adapted legal and institutional response.

This Public Policy Paper analyses the existing legal and institutional framework in the Republic of North Macedonia with regard to digital gender-based violence, using Directive (EU) 2024/1385 on combating violence against women and domestic violence as the primary reference framework for assessing alignment. Other relevant international instruments, including the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention) and GreVio General Recommendation No. 1 (2021) on the digital dimension of violence against women are used as horizontal interpretative frameworks to support the interpretation and clarification of the gender and digital dimensions of violence.

The analysis demonstrates that the national legislative framework contains certain criminal law and protective mechanisms that may also be applied in cases of digital gender-based Violence, particularly through the provisions on stalking, endangering security, and hate speech, as well as through the measures provided for under the Law on the Prevention and Protection from Violence against Women and Domestic Violence. However, these legal provisions do not provide for a clear and systematic approach to addressing digital gender-based violence, nor do they consistently take into account the gender dimension, the specific vulnerability of victims, and the cumulative consequences resulting from violence perpetrated in digital and public spaces.

The Public Room¹ case demonstrates that the mere existence of criminal acts is insufficient if the legal framework fails to recognize the nature of digital violence as collective, public, and repetitive, or to take into account the vulnerability of victims, the gender dimension of such attacks, and their psychosocial consequences. At the time of decision, the legal qualification was limited to individual criminal acts, without the possibility of fully recognizing the extent of the harm or providing appropriate procedural and protective mechanisms, such as those subsequently established as a European standard.

Based on the analysis conducted, the document proposes a set of recommendations for strengthening the national framework, with the aim of aligning it with Directive (EU) 2024/1385. The recommendations focus on clarifying and strengthening criminal law protection, integrating the digital dimension into the victim protection system, enhancing procedural mechanisms and access to justice, as well as strengthening institutional coordination and prevention.

¹ Further details on the Public Room case can be found on page 14 of this document.

The purpose of this document is to contribute to the development of a clearer, gender-sensitive, and practically applicable response to digital gender-based violence in the Republic of North Macedonia, in line with the obligations arising under European Union law.

1. Introduction

Digital gender-based violence is an increasingly prevalent phenomenon in modern society, with serious consequences for the safety, dignity, and mental health of women and girls. This phenomenon encompasses all forms of harassment, threats, blackmail, abuse or the non-consensual sharing of content carried out through information and communication technologies, and disproportionately targets women and girls on the basis of their sex or gender.²

The Republic of North Macedonia, in line with global trends and international standards, recognizes the need for a strengthened institutional response to the prevention of and protection against gender-based violence. In 2021, the Law on Prevention and Protection from Violence against Women and Domestic Violence was adopted, recognizing online sexual harassment as a specific form of gender-based violence and among the principles on which the Law is based is the principle of due diligence by institutions in the prevention, protection, investigation, and sanctioning of all forms of violence against women.³ However, the rapid development of technology continually creates new opportunities for abuse that are not fully addressed by the existing laws.

Over the past few years, the European Union has taken concrete steps to address these gaps. In 2021, the European Parliament adopted a Resolution calling for gender-based violence, including cyber violence, to be recognised as a new criminal offense at EU level pursuant to Article 83(1) of the Treaty on the Functioning of the EU⁴. This resulted in the initiation of legislative measures at EU level to harmonize definitions and sanctions. In May 2024, the first comprehensive Directive (EU) 2024/1385 on combating violence against women and domestic violence⁵ was adopted, specifically addressing digital forms of gender-based violence. This Directive sets minimum standards for regulating offenses such as online harassment, cyberstalking, the non-consensual sharing of intimate images, digital sexual harassment ("cyberflashing"), and the incitement to violence or hatred online on the grounds of sex or gender, as criminal offenses.

² See: UN Women, Online and ICT-facilitated violence against women and girls, 2022; UNDP, Analysis of Legislation Related to Technology-Facilitated Gender-Based Violence, 2024; Directive (EU) 2024/1385 of the European Parliament and of the Council on combating violence against women and domestic violence, which recognizes digital forms of gender-based violence as a distinct area of regulation, given their disproportionate impact on women and girls.

³ Law on Prevention and Protection from Violence against Women and Domestic Violence, Official Gazette of the Republic of North Macedonia, No. 24/21 and 39/25.

⁴ European Parliament, Resolution of 14 December 2021 with recommendations to the Commission on combating gender-based violence: a new criminal offence at EU level (2021/2035(INL)), calling for the inclusion of gender-based violence, including cyber violence, in the list of criminal offenses set out in Article 83(1) of the Treaty on the Functioning of the European Union.

⁵ Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence, Official Journal of the European Union, L 2024/1385.

It is particularly important to emphasise that digital gender-based violence constitutes a distinct mode of perpetrating, manifesting, continuing, or intensifying existing forms of gender-based violence and violence against women.⁶ This distinction is emphasized in order to prevent such conduct from being reduced solely to cybercrime or technologically facilitated criminal offenses, without recognising its gender dimension.

Taking into account the country's efforts to align its legislation with European Union law as part of the accession process, as well as its national commitment to the full implementation of the Istanbul Convention, through this Public Policy Paper, we provide an analysis of the existing domestic legal and institutional framework and an assessment of the extent of its alignment with the new European standards. Hence, the objective of this Public Policy Paper is to adopt a comprehensive and evidence-based approach to identifying the key regulatory gaps and challenges within the system for protection against digital gender-based violence, and to propose concrete recommendations for addressing them.

1.1. Terminology

Although Directive (EU) 2024/1385 does not introduce a single overarching term, it clearly recognizes gender-based violence perpetrated through the use of information and communication technologies by regulating specific criminal acts such as online harassment, cyberstalking, and the non-consensual sharing of intimate content. A similar approach is reflected in the national legislation, where the digital dimension of gender-based violence is addressed through specific criminal offences and protective measures, without the use of a single overarching term. On the other hand, UN Women uses the term technology-facilitated violence against women and girls in its strategic and expert publications, emphasizing that the use of technology does not create new forms of violence but rather amplifies existing forms of gender-based violence. GREVIO, in turn, stresses that the digital dimension must be systematically integrated into prevention, protection, and access to justice in accordance with the Istanbul Convention.

All of this demonstrates that, although legal frameworks recognize and regulate violence in the digital sphere, they do so through different approaches and without a common terminology. For these reasons, this paper uses the term digital gender-based violence as a common analytical concept for linking European, national, and international normative approaches, which allows for terminological consistency and provides a foundation for further policies and recommendations aimed at achieving a more effective institutional response. When analyzing the acts, however, the term used in each individual act will be used.

2. Methodology

This Public Policy Paper is based on an analysis of the existing domestic legal and institutional framework, as well as a comparative review of the relevant European Union legal framework in the area of digital gender-based violence.

⁶ According to GREVIO General Recommendation No. 1 (2021), available at: <https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147>

Taking into account the obligations incumbent upon the State under the ratified international conventions, the analysis also covers the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (hereinafter: the Istanbul Convention) and the Convention on the Elimination of All Forms of Discrimination against Women (hereinafter: CEDAW), as a legally binding framework for the Republic of North Macedonia, with the aim of assessing the extent of its implementation within the national legislative framework and institutional practice, as well as identifying normative and institutional gaps.

An analysis was conducted of the national legislative framework intended to ensure the implementation of the State's obligations under the Istanbul Convention and CEDAW. Particular attention was given to the analysis of the Law on Prevention and Protection against Violence against Women and Domestic Violence, as well as the relevant provisions of the Criminal Code and the Law on Free Legal Aid, with a focus on their applicability in the context of digital gender-based violence.

In parallel, a comparative review of the European legal framework was conducted, focusing on the European Parliament Resolution of 14 December 2021 on the criminalization of gender-based violence and Directive (EU) 2024/1385 on combating violence against women and domestic violence, including digital forms of violence. This review serves as the basis for identifying the obligations arising under European Union law and for comparing them with the existing national regulatory framework.

3. International Acts Establishing the Foundations for the Prevention of and Protection from Gender-Based Violence against Women at the National Level

3.1 Convention on the Elimination of All Forms of Discrimination against Women (CEDAW)

The Convention on the Elimination of All Forms of Discrimination against Women (CEDAW)⁷ is a fundamental international instrument in the field of the protection of women's rights and establishes an obligation for States to adopt appropriate measures to prevent and eliminate discrimination against women in all spheres of social life. Although the text of the Convention does not explicitly use the term "violence against women", its normative logic lays the foundation for the subsequent recognition of violence as a form of discrimination.

This interpretation is further developed in the jurisprudence of the Committee on the Elimination of Discrimination against Women, particularly through its General Recommendation No. 19, and subsequently through General Recommendation No. 35⁸, which updates and expands upon the earlier approach. In these General Recommendations, the Committee establishes that gender-based violence against women constitutes a form of

⁷ Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), adopted by Resolution 34/180 of the United Nations General Assembly of 18 December 1979;

⁸ General Recommendation No. 35 is available at: <https://docs.un.org/en/CEDAW/C/GC/35>

discrimination within the meaning of Article 1 of the Convention, as it seriously impairs women's ability to enjoy their human rights and fundamental freedoms on an equal basis with men.

General recommendation no. 35 further reinforces this approach, emphasizing that States' obligations are not confined to traditional or "classic" forms of violence, but also extend to new, evolving and transnational forms of gender-based violence. In this context, the Committee explicitly recognizes that gender-based violence may also be perpetrated through modern technologies and digital means⁹, including online harassment, threats, stalking and the misuse of personal data, and that States have an obligation to ensure appropriate legal and institutional protection in such cases as well.

Hence, although CEDAW does not establish a detailed framework for the recognition of and response to individual forms of violence, through its general recommendations, particularly General Recommendation No. 35, provides a substantive foundation for regulating gender-based violence within domestic legislation, including the digital forms and manifestations in which it occurs.

3.2. Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention)

Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence, (hereinafter: Istanbul Convention)¹⁰, is the first legally binding international instrument to establish a comprehensive and integrated framework for the prevention of, protection against and prosecution of violence against women. The Convention treats violence against women as a form of gender-based discrimination and a violation of human rights, arising from the historical and structural inequality between women and men, while explicitly rejecting the notion that such violence is an isolated or private phenomenon.

Unlike CEDAW, which lays the foundations for the protection of women against discrimination, the Istanbul Convention introduces specific and precise obligations for States in relation to the criminal law framework, institutional arrangements, and the practical protection of victims. It establishes a clear obligation for States to incorporate a range of forms of violence into their domestic legislation as criminal offenses. These include psychological violence, stalking, sexual violence, sexual harassment, and other forms of violence that frequently manifest themselves in the context of intimate relationships and unequal power dynamics.

Although the Istanbul Convention does not explicitly use terminology relating to "digital" or "online" violence, its provisions are formulated in a manner that is equally applicable to acts perpetrated through modern means of communication. The forms of violence established by the Convention, such as stalking, psychological violence and sexual harassment, by their very

⁹ See point 6 of General Recommendation No. 35

¹⁰ Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence, (the Istanbul Convention - hereinafter: IC), ratified by the Law Ratifying the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (Official Gazette No. 198/2017)

nature encompass behaviors perpetrated through digital platforms, social media and other electronic means of communication.

Of particular significance is the Convention's insistence on a gender-sensitive approach to criminal law and protection policies, requiring States to recognize the specific risks faced by women, as well as the continuous and recurring nature of violence. It also provides for an obligation to ensure effective prosecution, appropriate sanctions and protective measures, while the burden of proof must never fall upon the victim.

In this context, the Istanbul Convention serves as the basis for analyzing national legislation on gender-based violence, including digital gender-based violence, in order to assess whether the existing legal framework encompasses the relevant forms of violence, regulates them in a gender-sensitive manner, and provides effective protection and legal certainty for victims.

To clarify the application of these obligations in the contemporary digital context, in 2021 GREVIO adopted General Recommendation No. 1 on the digital dimension of violence against women¹¹, which clarifies that the obligations arising under the Istanbul Convention apply in full to violence perpetrated through the use of information and communication technologies. The Recommendation points out that forms of violence such as stalking, psychological violence and sexual harassment frequently manifest themselves in the digital environment, where their impact on victims may be exacerbated by their accessibility, repetitive nature and persistence. GREVIO calls upon States to systematically incorporate the digital dimension into the prevention of violence, the protection of victims, and access to justice.

In the context of these international obligations, the Republic of North Macedonia has recently undertaken a number of legislative measures to strengthen protection against gender-based violence, primarily through the adoption and amendment of the systemic laws governing this area. The following section examines the extent to which these legislative measures comply with the established international standards, with particular emphasis on the digital environment.

4. National Legal Framework for the Prevention and Protection from Gender-Based Violence

The Republic of North Macedonia has recently taken a series of legislative measures aimed at strengthening the system for the prevention of and protection against gender-based violence against women. These efforts are reflected primarily in the adoption and enhancement of the systemic laws in the area of prevention of violence, protection of victims, and sanctioning of perpetrators, through the establishment of institutional mechanisms and coordination among the competent authorities.

Although the national legal framework formally recognizes gender-based violence as a matter of public interest and State responsibility, the degree of alignment with international

¹¹ Available at: <https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147>

standards and the effectiveness of the protection mechanisms varies considerably, particularly with regard to modern and digital forms of violence.

4.1. Law on Prevention and Protection from Violence against Women and Domestic Violence

The Law on Prevention and Protection from Violence against Women and Domestic Violence is the central systemic legislative act within the national legal framework for prevention and protection from gender-based violence.¹² The Law establishes a comprehensive approach to violence against women by defining the key concepts, setting out protection measures, victim support services, and mechanisms for coordination among the competent institutions.

The Law establishes the normative basis for institutional action in cases of gender-based violence, including through emergency and temporary protection measures, risk assessment, and the provision of support to victims. Its approach is based on the principles of victim protection, respect for human rights, and multi-sectoral cooperation, in line with the obligations arising under the Istanbul Convention.

The glossary and the substantive provisions of the Law recognise and regulate certain forms of gender-based violence that may be perpetrated through digital means. In particular, sexual harassment is defined in a manner that encompasses verbal, non-verbal, or other conduct of a sexual nature perpetrated through the internet or other means of electronic communication. Thus, the Law represents a significant step forward in recognising the digital dimension of gender-based violence and enables the application of protective measures even in cases where the violence manifests itself beyond the physical space.

However, this normative solution does not evolve into a comprehensive and systematic regulation of digital gender-based violence. The Law does not contain a detailed conceptualisation of the various forms of digital violence, nor does it include specific provisions addressing the distinctive dynamics of online threats, continuous online harassment, the non-consensual sharing of intimate content, or other forms of abuse perpetrated through digital technologies.

As a consequence, protection from digital gender-based violence under this Law remains limited to individual forms of violence and relies on a broad interpretation of the existing provisions, without providing clear guidance on their application in the digital context. Furthermore, although the Law provides for institutional coordination and a multi-sectoral approach, it does not establish specific protocols or guidelines for responding to cases of gender-based violence perpetrated through digital technologies, particularly with regard to risk assessment and the urgency of protection.

Hence, although the Law on the Prevention and Protection from Violence against Women and Domestic Violence constitutes a key pillar of the national framework for protection and already recognises certain digital forms of violence, its applicability to digital gender-based

¹² Law on Prevention and Protection from Violence against Women and Domestic Violence, Official Gazette of the Republic of North Macedonia, No. 24/21 and 39/25.

violence, whether in the form of gender-based violence in the online environment or technology-facilitated gender-based violence, remains partial and insufficiently defined.

This indicates the need for further legislative refinement and clarification in order to ensure clear, predictable and effective protection in the digital environment as well.

4.2. Criminal Code¹³

The Criminal Code of the Republic of North Macedonia regulates the punitive dimension of protection against gender-based violence and, through its most recent amendments, marks a clear shift towards a gender-sensitive approach. The Criminal Code explicitly uses the terms "gender-based violence against women" and "victim of gender-based violence", defining gender-based violence as violence directed against a woman because of her gender identity, which results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering, regardless of whether it occurs in public or private life.

The Special Part of the Criminal Code regulates a number of criminal offenses which, by their nature and context, constitute forms of gender-based violence. Particular significance is attached to the criminal offense of stalking, which criminalises repeated unauthorised monitoring, persecution and harassment, including through means of communication and the misuse of personal data, while providing for an aggravated form of the offense where it is committed against a person with whom the perpetrator is or has been in an intimate relationship, or against a child. The Criminal Code also recognizes the most serious form of gender-based violence—femicide, through a qualified form of the criminal offense of murder.¹⁴ With this solution, the gender-based motive and the context of the violence are explicitly incorporated into the criminal law classification of the offense. In addition, the Criminal Code covers other criminal offenses that may constitute forms of gender-based violence, including threats, violations of privacy, unauthorized recording or publication, as well as sexual harassment via the internet. These provisions enable the sanctioning of certain acts committed through digital means, while the gender-based motive and the relationship between the perpetrator and the victim may be taken into account when determining the sentence.

Nevertheless, despite the explicit legislative recognition of gender-based violence, the introduction of femicide as an aggravated form of murder, and the recognition of certain individual digital manifestations of violence, the criminal law framework does not establish a systematic and comprehensive regulatory framework for digital gender-based violence. Although the existing criminal offenses may also be applied where the conduct is perpetrated through digital means, there are no specific criminal offenses or clearly defined aggravated forms that explicitly address the distinctive dynamics, continuity and consequences of violence in the digital environment. In other words, the existing provisions enable an

¹³ Criminal Code, "Official Gazette of the Republic of Macedonia" No. 37/96, 80/99, 4/02, 43/03, 19/04, 81/05, 60/06, 73/06, 7/08, 139/08, 114/09, 51/11, 135/11, 185/11, 142/12, 166/12, 55/13, 82/13, 14/14, 27/14, 28/14, 41/14, 115/14, 132/14, 160/14, 199/14, 196/15, 226/15, 97/17 and 248/18 and the "Official Gazette of the Republic of North Macedonia" No. 36/23 and 188/23

¹⁴ Pursuant to Article 123(2), point 2-a, the deprivation of the life of a woman or a girl under the age of 18 committed in the course of perpetrating gender-based violence is criminalised as an aggravated form of murder, punishable by a term of imprisonment of at least ten years or life imprisonment.

individualized response, but do not provide for a systematic approach to addressing such conduct.

Accordingly, protection against digital gender-based violence under the Criminal Code remains fragmented and is largely dependent on the interpretation and practice of the competent authorities. This indicates the need for further legislative refinement and alignment with contemporary European standards in order to ensure clearer, more predictable and more effective criminal law protection in the digital context as well.

4.3. Law on Free Legal Aid¹⁵

The Law on Free Legal Aid constitutes a significant element of the national framework for ensuring access to justice for victims of gender-based violence, by establishing mechanisms for primary and secondary legal aid funded by the State.

The Law explicitly includes victims of gender-based violence and domestic violence among the beneficiaries of free legal aid and provides for expedited procedures and exemptions from the financial eligibility assessment where urgent protection is required. However, although the legislative framework provides formal access to legal aid, digital forms of gender-based violence are not recognised as a distinct category, nor are they treated as a factor affecting the urgency, risk or complexity of cases. The Law does not contain provisions that explicitly address the needs of victims of online harassment, digital threats or the misuse of personal data, nor does it provide for specialised legal assistance in the collection and assessment of digital evidence. As a result, the effectiveness of free legal aid in cases of digital gender-based violence depends to a large extent on the interpretation and practice of the competent authorities, indicating the need for further legislative clarification and the adaptation of the Law to contemporary forms of violence.

4.4. Rights Holders and Duty Bearers

The primary duty bearers responsible for protection against gender-based violence, including its digital manifestations, are institutions within the executive, judicial, and local government branches, as well as independent bodies provided for by law. The key institutional mechanisms include:

¹⁵ Law on Free Legal Aid, "Official Gazette of the Republic of North Macedonia" No. 101/19 and 194/24. This Law transposes Council Directive 2003/8/EC of 27 January 2003 to improve access to justice in cross-border disputes by establishing minimum common rules relating to legal aid for such disputes, CELEX 32003L0008

Institution	Competences established under the law
Ministry of Social Policy, Demography and Youth	Development of policies and measures for prevention and protection; coordination of the protection system; monitoring the implementation of the Law; and ensuring the conditions necessary for the operation of victim support services
Centers for Social Work	Receiving reports of violence; conducting risk assessments; developing individual protection plans; proposing and implementing emergency and long-term protection measures; referring victims to appropriate services; and monitoring the victim's situation.
Ministry of Justice	Provision of primary and secondary legal aid
Ministry of Interior	Receiving reports; taking emergency protection measures; ensuring the victim's safety; filing criminal charges; and cooperating with other institutions
Public Prosecutor's Office	Acting upon criminal charges; undertaking actions for criminal prosecution and the collection of evidence; and proposing protection measures within criminal proceedings
Courts	Deciding on emergency and long-term protection measures; adjudicating misdemeanor and criminal proceedings; and providing judicial protection
Healthcare institutions	Providing healthcare services; documenting injuries; notifying the competent authorities; and issuing medical documentation
Educational institutions	Protecting children who are victims or witnesses of violence; notifying the competent authorities; and carrying out preventive activities
Local self-government units	Providing and supporting local services; carrying out preventive activities; and cooperating with institutions and CSOs
Civil society organizations – service providers	Providing specialized support services; cooperating with institutions
Coordination and inter-institutional bodies	Coordinating institutional responses; facilitating information sharing; and strengthening inter-institutional cooperation

5. Review of Compliance with EU Acts Governing the Response to Digital Gender-Based Violence

In recent years, the European Union has developed a comprehensive policy framework for combating violence against women, recognising both the urgency of the issue and its cross-border dimension (particularly online). In September 2021, the European Parliament adopted Resolution 2021/2035(INL), in which it called, for the first time, for gender-based violence to be included as a distinct area of crime under the EU Treaties (the list of so-called EU criminal offenses). This Resolution highlights that violence against women, including online violence, is widespread and undermines the fundamental values of the European Union - equality, human dignity and fundamental freedoms. The European Parliament highlights alarming data

on the increase in cyber violence: Since the beginning of the COVID-19 pandemic, a significant increase has been reported in cases of online harassment, threats, and the non-consensual sharing of explicit material. It also emphasizes that women and girls are disproportionately targeted by such forms of digital violence, with young people being particularly vulnerable. The Resolution contains a number of recommendations addressed to the European Commission and the Member States, the most significant of which are:

Adopt comprehensive EU-level legislation criminalizing all forms of gender-based violence, including cyber-violence (online harassment, cyberstalking, the non-consensual sharing of intimate images, cyber-violence in the workplace, etc.). The European Parliament insists that the definition of "woman" in those initiatives also include girls under the age of 18, a position that has also been incorporated into the Directive.

Ensure the ratification and implementation of the Istanbul Convention in all Member States, while also going a step further: The Resolution recognizes that not all aspects of digital violence are explicitly covered by the Convention. It therefore calls on the Member States to update their legislation and to explicitly prohibit and penalize digital gender-based violence, including the non-consensual sharing of intimate images, online stalking, and all forms of cyber-harassment. This call is entirely in line with the recommendations of the specialized bodies of the United Nations and the Council of Europe (e.g., GREVIO General Recommendation No. 1 (2021) on the digital dimension of violence against women).

Increase funding and support for victims of gender-based violence, conduct awareness-raising campaigns (particularly among young people on non-violent behaviour online), and improve the quality of data through more harmonized indicators and the strengthened involvement of the relevant EU bodies (Eurostat and the European Institute for Gender Equality (EIGE)).

Emphasize equal access to justice for victims throughout the EU. The Resolution emphasizes the need to remove barriers to reporting, improve trust in institutions, and ensure that women victims (including child witnesses) are treated with due care and receive appropriate protection throughout the proceedings.

The European Commission's response to the Resolution was swift: Already in March 2022, a draft text for the Directive was released, which was adopted in 2024 as Directive (EU) 2024/1385.

- **Throughout its text, Directive 2024/1385 highlights dual objective:** to prevent and combat violence against women, including domestic violence, and to ensure comprehensive protection and support for victims. In this way, the directive also sets standards for victim support services, procedural safeguards, and inter-institutional coordination. In the digital context, the Directive recognizes that online violence may have an amplified impact due to the rapid dissemination, repeatability, and persistence of online content, which is particularly relevant when attacks target women in public roles (such as journalists, activists, and politicians). In this regard, the Directive explicitly provides that it constitutes an aggravating circumstance where the offence is committed because the victim is a public representative, a journalist, or a human rights defender. The key provisions of the Directive relevant to digital gender-based violence may be summarized as follows:

- **Digital dimension of criminal offences**¹⁶: All Member States are obliged to protect as criminal offences the following specific acts: “non-consensual sharing of intimate or manipulated material”, namely the publication or dissemination, through ICT, of sexually explicit or nude images or videos of a person without that person's consent, as well as the creation and sharing of manipulated intimate images (deepfakes) without that person's explicit consent. In both situations, the conduct must be likely to cause serious harm to the person. In addition, it is also necessary to criminalize threats to share such material with the aim of compelling the person to do, or to refrain from doing, something. This directly encompasses the practice of blackmailing women with their intimate images, including cases in which a partner demands the resumption of a relationship under the threat of publishing explicit photographs.
- **Online stalking**¹⁷: the intentional and persistent monitoring or tracking of a person's activities or movements through digital means, without that person's consent or any legal basis, in a manner that is likely to cause that person serious distress or harm. This essentially corresponds to the offense of stalking under our criminal law, while specifically identifying the use of technology as a constituent element of the offense. North Macedonia is in a relatively favorable position in this regard, as Article 144-a of the Criminal Code already covers stalking through means of communication, as well as the misuse of personal data for the purpose of harassment. The only minor difference is that the Directive requires such conduct to be punishable even where there is no direct communication with the victim, but only the monitoring of it's movements (e.g. through a phone's GPS or applications), something that is likewise covered by our legislation through the concept of "interfering with a person's private life ... by moving within the space where that person is located."
- **Online harassment**¹⁸ is perhaps the most comprehensively elaborated category, encompassing four forms: 1) repeated or persistent threatening conduct directed at a specific person through ICT, particularly where it involves threats to commit criminal offenses, and is likely to cause that person, or persons closely connected to that person, serious fear for their safety; 2) publicly accessible threatening or insulting conduct, carried out in concert with other persons and directed at a specific person through ICT, which is likely to cause serious psychological harm; 3) the unsolicited sending of images, videos, or other material depicting genitalia (so-called cyberflashing), where it is likely to cause significant distress to the recipient; and 4) the publication of a person's personal data without that person's consent (doxing), with the aim of inciting third parties to inflict physical or psychological harm on that person. Taken together, these four elements constitute the criminal offence of cyber-harassment. There is no such comprehensive provision in Macedonian legislation. Certain aspects are covered by individual offenses — for example, (1) largely corresponds to the offenses of "endangering security" and "stalking," while (4) is partially covered by the offense of "misuse of personal data"; however, (2) and (3) are, in practical terms, not covered at all. In particular, coordinated online harassment, whereby multiple persons target a single individual with abusive messages on social media, is a phenomenon that is not

¹⁶ Articles 5-8 of the Directive

¹⁷ Article 6

¹⁸ Article 7

currently treated as a criminal offense in our country, unless it contains an element of a serious threat or hate, in which case it could fall within the scope of the offense of hate speech. The Directive requires the most serious forms of such coordinated harassment to be punishable, recognizing the harmful effects of so-called "pile-on" attacks. Likewise, the unsolicited sending of pornographic images (cyberflashing) becomes a mandatory criminal offense under EU law, whereas in our country such conduct is not covered by any criminal offense (although, in certain cases, it could potentially be treated as sexual harassment under the Law on Prevention and Protection against Discrimination, but not as a criminal offense). Therefore, alignment with the Directive will require either implementation of these new criminal offenses or the expansion of the scope of the existing ones.

- **Incitement to violence or hatred online**¹⁹: this essentially constitutes an extension of the existing criminal offense of hate speech, with a particular focus on sex/gender. The Directive requires the criminalization of the intentional public dissemination, through ICT, of material inciting violence or hatred against a group of persons or a member of such a group defined on the basis of gender. States are permitted to limit criminal prosecution to cases where such conduct is likely to disturb public order or is genuinely threatening or abusive. This corresponds to Article 319 of our Criminal Code. It should be noted, however, that our provision employs the wording "on the grounds of ... sex, gender, ... or any other discriminatory ground," which is consistent with the Directive. Hence, from the perspective of the criminal-law regulation of hate speech, it may be concluded that an adequate legal basis already exists and it is necessary to monitor the implementation of these provisions (for example, by ensuring that perpetrators who engage in abusive sexist speech are also prosecuted).
- **Sanctions and aggravating circumstances**:²⁰ The Directive establishes minimum requirements regarding the maximum penalties that must be prescribed. for the most serious offenses, such as murder, rape, and grievous bodily harm, it requires that the maximum penalty be at least five years' imprisonment. For digital gender-based violence, the Directive provides that the maximum penalty shall be at least one year's imprisonment. This practically means that such conduct must be treated as criminal offenses (rather than misdemeanours) and must not be punishable solely by a fine. The Directive also lists aggravating circumstances that Member States are required to provide for: where the offense is repeated; where it is committed against a particularly vulnerable person (such as a child, a pregnant woman, or a person with a disability); where it is committed with particular cruelty; where it is committed by more than one person; where it is committed through the abuse of a position of trust (for example, by a partner, a family member, or a person exercising authority over the victim); etc. Many of these circumstances are already covered by the Macedonian Criminal Code: for example, an offense committed against a spouse or a child most often constitutes an aggravated form of the offense (as is the case with the offenses of endangering security and stalking). What may be lacking, however, is an explicit provision treating the fact that the offence was committed online and in a public manner which the Directive considers aggravating. Our legislation still does not contain a provision

¹⁹ Article 8

²⁰ Articles 10 and 11

explicitly stipulating that the commission of an offense online constitutes an aggravating circumstance.

- **Protection and assistance to victims:** The Directive prescribes detailed measures for victim support. Every Member State must provide a free 24/7 helpline, easily accessible shelter facilities, psychological counselling, legal advice, and specialized services tailored to the different needs of victims. Victims of digital violence must be able to report offences online or electronically²¹. The Directive encourages Member States to develop online reporting tools through which victims can also upload electronic evidence in support of their reports. This is a particularly important innovation. The traditional way of going to the police station can be discouraging for a young girl who is a victim of online bullying; enabling her to do so through a computer or mobile phone could significantly increase reporting rates. The Directive also emphasizes that the officials who first come into contact with the victim should be trained to provide specialized support, assess the level of risk and the urgency of the situation, and provide the victim with appropriate information about their rights and the available protection options. The Directive insists on a tailored approach²², particularly in relation to child victims or witnesses, as well as victims whose personal circumstances require special consideration, such as persons with disabilities, LGBTI persons, members of minorities, migrant women, and others.

Example from practice: The "Public Room" Case

The case known as "Public Room" highlighted significant gaps in the criminal-law regulation of digital gender-based violence. In the absence of a specific criminal offence covering the non-consensual sharing of intimate material, proceedings involving minor victims, or victims who were minors at the time the material was published, were conducted under the provisions governing criminal offences relating to child pornography. Although this approach was, at the time, the only legally available option, it did not always adequately reflect the nature of the violence or the harm suffered by the victims.

At the same time, the case contributed to legislative amendments introducing into the Criminal Code an explicit criminal offence of the non-consensual sharing of intimate images, thereby enabling a more appropriate legal classification of such forms of digital violence in line with modern European standards.

The "Public Room" case illustrates that, at the time of decision-making, the existing criminal-law framework did not provide for the systematic recognition of cyber-harassment as a form of digital gender-based violence. The legal classification failed to capture the gendered dimension of the attacks, the particular vulnerability of the victims, or the cumulative psychosocial consequences resulting from public and coordinated online exposure. At the same time, there were no procedural mechanisms in place to ensure a prompt response and effective protection, such as those subsequently established as standards by Directive (EU) 2024/1385.

²¹ Articles 14 and 15

²² Article 25

- **Content removal/blocking obligations:** The Directive is aligned with the EU's new Digital Decade Policy Programme and the implementation of the Digital Services Act (DSA), which generally require large online platforms to take measures against illegal content. Directive (EU) 2024/1385 specifically requires Member States to ensure that competent authorities are empowered to issue binding legal orders to hosting service providers, subject to transparent procedures, the principle of proportionality, and effective judicial protection for the parties concerned, as well as an obligation that the removal of content must not prevent the timely preservation and securing of evidence. In the Republic of North Macedonia, such measures would not constitute a novelty, as access restrictions are already imposed on certain websites and web applications that unlawfully provide games of chance, on the basis of an order issued by the Ministry of Digital Transformation.²³

In summary, the alignment of the North Macedonian legal framework with the Directive in the area of digital gender-based violence may be assessed as partial: the existing framework provides a foundation through the criminal offences addressing stalking and threats, as well as through provisions recognizing certain aspects of the incitement of hatred. However, the Directive establishes a more explicit and comprehensive framework for the non-consensual sharing of intimate or manipulated material, coordinated cyber-harassment by groups, cyberflashing, and doxing. Furthermore, the Directive's emphasis on online reporting accompanied by the submission of evidence, the development of electronic evidence capabilities, and mechanisms for the swift removal or blocking of content shifts the focus from the mere formal introduction of criminal offences to the practical effectiveness of victim protection. This approach is relevant to all victims of digital gender-based violence, and is of particular importance in situations where harm can spread rapidly and intensify within the public digital sphere, including where attacks are directed against women in public roles, such as journalists, activists, and politicians.

6. Overview of the Identified Legal and Institutional Gaps

Despite the significant normative advances achieved in the national legal framework, the analysis demonstrates that structural and conceptual legal gaps remain with regard to the comprehensive and systematic regulation of digital gender-based violence, particularly when assessed against the standards established at the European Union level.

6.1. Absence of Comprehensive Regulation of Digital Gender-Based Violence

Although the national legal framework recognizes certain forms of gender-based violence that may be perpetrated through digital means, particularly through the definition of sexual harassment committed via the internet. Digital gender-based violence has not been conceptualized or regulated as a distinct and complex phenomenon. Unlike Directive (EU)

²³ Further information is available at: <https://mdt.gov.mk/mk-MK/odnosi-so-javnost/soopstenija/zabrana-za-novi-42-nelegalni-onlajn-igri-na-srekja-vkupno-dosega-se-268>

2024/1385, which systematically identifies and regulates the various forms of digital violence against women, the national legal framework relies on the fragmented application of general legal provisions, without a clear normative framework encompassing the specific characteristics and dynamics of violence perpetrated in the digital environment.

6.2. Limited Substantive Scope of Digital Forms of Violence

The existing legal framework covers only certain forms of digital gender-based violence, primarily through the criminalization of sexual harassment and certain criminal offenses that may be committed by means of electronic communications. However, the national legislation does not explicitly recognize or regulate a number of key forms of digital gender-based violence, such as persistent online harassment, digital stalking as a broader pattern of conduct, the non-consensual sharing of intimate material, coordinated online attacks, and other forms of abuse that are recognized as distinct categories under the European regulatory framework. This results in difficulties in the legal classification of offences and in unequal protection for victims.

6.3. Insufficient Operationalization of Protective Measures in the Digital Context

Although the legislation provides for urgent and interim measures to protect victims of gender-based violence, these measures are not sufficiently adapted to situations in which the violence is perpetrated in the digital environment. The national legal framework does not provide clear legal mechanisms for prohibiting digital contact, removing or restricting access to harmful online content, nor does it establish obligations for coordination with online platforms and providers of digital services. As a consequence, the protection afforded to victims in cases of digital gender-based violence largely depends on the interpretation and practice of the competent authorities.

6.4. Lack of Clear Procedural and Institutional Guidance

The national legislation does not contain specific procedural provisions governing the handling of cases involving digital gender-based violence. This applies in particular to risk assessment, the determination of the urgency of protective measures, the collection and preservation of digital evidence, as well as the prevention of the re-victimization of victims. The absence of specialised protocols and clearly defined institutional responsibilities creates scope for inconsistent institutional practice and hampers effective access to protection and justice.

6.5. Limited Integration Between the Sanctioning System and the Protection System in Cases of Digital Gender-Based Violence

Although the Criminal Code has made a significant step forward by explicitly recognising gender-based violence and introducing femicide as an aggravated form of homicide, there remains insufficient functional integration between the criminal justice response and the mechanisms for the protection and support of victims in cases of digital gender-based violence. This is contrary to the holistic approach promoted by the European instruments,

under which prevention, protection, sanctioning and victim support are treated as interrelated and mutually reinforcing components of the system.

Hence, although the national legal framework contains important provisions for the recognition and sanctioning of gender-based violence, the existing legal solutions do not provide a comprehensive and systematic response to the specific challenges posed by the digital environment. The identified legal gaps point to the need for further normative regulation and institutional strengthening in order to achieve full alignment with contemporary European standards and to ensure effective protection for victims.

7. Conclusions

The analysis of the national legal and institutional framework shows that the Republic of North Macedonia has established a solid normative basis for the prevention of and protection against gender-based violence, which to a significant extent reflects the international obligations it has undertaken, particularly those arising from the Istanbul Convention. Through the Law on the Prevention and Protection from Violence against Women and Domestic Violence, together with the amendments to the Criminal Code, gender-based violence has been clearly recognized as a matter of public interest and state responsibility, while the criminal law framework has taken an important step towards a gender-sensitive approach.

However, the analysis shows that the existing legislative framework does not provide a comprehensive and systematic response to the specific forms and dynamics of gender-based violence as manifested in the digital environment. Although certain digital forms of violence, such as online sexual harassment, are explicitly recognized, digital gender-based violence has not been conceptualized as a distinct phenomenon, nor is it accompanied by clear procedural, protective and institutional mechanisms.

The absence of explicit definitions of the key forms of digital violence, the insufficient operationalization of protective measures in the digital context, and the lack of specialized protocols and institutional guidance result in the fragmented application of the law and unequal protection for victims. In practice, this leads to legal uncertainty, an inconsistent institutional response, and an increased risk of the re-victimization of victims, particularly in cases of persistent online violence.

With regard to European standards, particularly Directive (EU) 2024/1385, it may be concluded that the national framework does not yet provide the required level of alignment in relation to digital gender-based violence. This creates a need for further normative and institutional development in order to ensure clear, predictable and effective protection for victims, in line with contemporary European approaches.

8. Recommendations

Based on the identified legal and institutional gaps, and in the light of the obligations arising from the Istanbul Convention and the European Union's new legal framework, the following recommendations are proposed with a view to the systematic and sustainable enhancement of protection against digital gender-based violence:

1. Normative Development and Clarification of Digital Gender-Based Violence

This set of recommendations addresses the need for a clear and comprehensive criminal law framework governing the digital manifestations of gender-based violence, with a view to addressing the identified gaps and ensuring legal certainty and predictability in the application of the law.

- 1.1. Amend the Criminal Code to provide for the clear and explicit regulation of cyber harassment as a distinct form of digital gender-based violence, in accordance with Directive (EU) 2024/1385.
- 1.2. Ensure the recognition of group and publicly accessible online harassment, the unsolicited transmission of explicit content (cyberflashing), and the disclosure of personal data with the intention of inciting harassment (doxing), as well as their gendered dimension and cumulative consequences.
- 1.3. Amend Article 39 of the Criminal Code to provide that the commission of an offense in a public (online) space and its digital nature shall constitute an aggravating circumstance for the purpose of sentencing.

Competent institution: Ministry of Justice

2. Alignment of the Law on the Prevention and Protection from Violence against Women and Domestic Violence with Directive (EU) 2024/1385

This section focuses on integrating the digital dimension of violence into the existing mechanisms for the protection and support of victims, with particular emphasis on risk assessment and timely intervention.

- 2.1. Explicitly incorporate the forms of digital gender-based violence recognised under the Directive.

Competent institution: Ministry of Social Policy, Demography and Youth

- 2.2. Introduce clear and enforceable protective measures for cases of digital violence, including prohibitions on digital contact, obligations to remove or restrict harmful online content, and urgent measures to prevent further digital abuse.

Competent institution: Ministry of Social Policy, Demography and Youth, Ministry of Digital Transformation

- 2.3. Integrate the digital dimension of the threat into the risk assessment process.

Competent institution: Ministry of Social Policy, Demography and Youth, Ministry of Internal Affairs

3. Access to Justice

The recommendations in this area aim to improve practical access to justice through clear, accessible and effective procedural tools, particularly with regard to the reporting of offenses and the submission of electronic evidence.

- 3.1. Establish mechanisms for online reporting with the submission of electronic evidence.

Competent institution: Ministry of Justice, Ministry of Internal Affairs, Ministry of Digital Transformation

- 3.2. Introduce clear procedures for the urgent preservation of electronic evidence.

Competent institution: Public Prosecutor's Office of the Republic of North Macedonia, Supreme Court, Ministry of Internal Affairs

- 3.3. Specialized training on gender-sensitive handling of cases of digital gender-based violence and the preservation of digital evidence

Competent institution: Academy for Judges and Public Prosecutors, Ministry of Internal Affairs

4. Removal and Blocking of Illegal Content

This set of recommendations refers to the establishment of balanced mechanisms for the prompt protection of victims through the removal or blocking of illegal content, while ensuring respect for procedural safeguards and the right to a fair trial.

- 4.1. Develop a protocol for cases involving the non-consensual sharing of intimate content.
- 4.2. Establish mechanisms for issuing orders for the removal or blocking of illegal online content

Competent institution: Ministry of Digital Transformation, Ministry of Internal Affairs, Public Prosecutor's Office of the Republic of North Macedonia

5. Coordination, Data and Prevention

These recommendations are aimed at strengthening institutional coordination, improving the quality of data, and developing preventive policies as a prerequisite for a long-term and sustainable response to digital gender-based violence.

- 5.1. Strengthen inter-institutional coordination and data collection

Competent institution: State Statistical Office, Ministry of Social Policy, Demography and Youth, Ministry of Justice

- 5.2. Develop preventive and educational programmes on digital safety.

Competent institution: Ministry of Education and Science, Ministry of Social Policy, Demography and Youth, Agency for Audio and Audiovisual Media Services.