

NEW RULES ON COMBATING CYBERVIOLENCE AGAINST WOMEN: LEGAL FRAMEWORKS AND POLICIES OF THE EUROPEAN UNION

Ajna Jodanović, PhD, Associate Professor¹⁵⁶

*Faculty of Law, University of Bihać and Faculty of International Relations & Diplomacy, Sarajevo
School of Science and Technology (SSST)*

Vladimir M. Simović, PhD, Full Professor¹⁵⁷

*Faculty of Security and Protection, Independent University of Banja Luka and prosecutor's Office
of Bosnia and Herzegovina*

Abstract: As a result of the increasing use of advanced technologies and the internet in everyday life and activities, violence against women in the digital sphere has become a growing legal and social issue at European Union level. In an effort to provide an adequate response to this growing challenge, the Union has, in recent years, introduced comprehensive legal measures and policies aimed at protecting women from various forms of digital violence. Among the most prominent forms are cyber harassment, online stalking, gender-based hate speech, and the unauthorized sharing of intimate content. This paper analyses the latest legal regulations adopted by the European Union to improve the protection of women in the digital space, with a particular emphasis on the Directive on Combating Violence Against Women and Domestic Violence. Directive represents the first legislative act at the EU level that explicitly recognizes cyber violence as a form of gender-based violence. It mandates that member states criminalize specific forms of digital violence, establish effective mechanisms for victim protection, and ensure access to legal remedies. In analyzing the EU's legal approach to combating cyberviolence against women, special attention is given to the role of the General Data Protection Regulation (GDPR) in safeguarding women's privacy and security online, as well as the Digital Services Act (DSA), which introduces stricter obligations on digital platforms to remove illegal content and take preventive measures against cyberviolence. The objective of this paper is to present the EU's legal regulations and policies as a significant step forward in the context of combating violence against women in the digital sphere, while also highlighting the challenges in their implementation. Through an analysis of current policies and their impact, as well as the experiences of the European Union Member States in the field of implementing legislative measures, the paper highlights the importance of further developing integrated strategies that will ensure comprehensive protection of women in the digital space at the EU level.

Keywords: European Union, cyberviolence, women, EU legal framework and policies.

1. Introduction

As we are entering a period of increased scrutiny of social media platforms, the reach and use of these platforms and the new technologies they are based on continue to proliferate. Although women have benefited from outstanding possibilities on the internet and via new technologies, both in

¹⁵⁶ E-mail: ajna_x@hotmail.com; ORCID: 0000-0002-0146-411X.

¹⁵⁷ E-mail: e-mail: vlado_s@blic.net; <https://orcid.org/0009-0002-9640-6488>.

terms of power and visibility and in terms of access and opportunities, they are also at threat of violence in dire ways in the digital world. In Europe, one in ten women have experienced some kind of cyber violence since the age of 15.¹⁵⁸ Equality between women and men and non-discrimination are core values of the Union and fundamental rights enshrined, respectively, in Article 2 of the Treaty on European Union (hereinafter: TEU)¹⁵⁹ and in Articles 21 and 23 of the Charter of Fundamental Rights of the European Union (hereinafter: CFREU)¹⁶⁰. Violence against women and domestic violence endanger those very values and rights, undermining women and girls' rights to equality in all areas of life and hindering their equal societal and professional participation.¹⁶¹ Gender-based violence is not a new phenomenon, but its migration to the digital world has magnified its scale and impact. As early as the advent of email and chat rooms, women became targets of cyberstalking and harassment. With the rise of social media, these threats expanded, providing perpetrators with tools to harass, exploit, and demean on a global scale.¹⁶²

In response to this growing threat, the European Union has recently enacted comprehensive legal measures and policies to safeguard women in the digital sphere, targeting abuses such as cyber harassment, online stalking, gender-based hate speech, and the non-consensual sharing of intimate images. This paper examines these new EU frameworks for combating cyberviolence against women, with particular emphasis on the landmark Directive (EU) 2024/1385 on combating violence against women and domestic violence – the first EU law to explicitly recognize cyberviolence as a form of gender-based violence. Using a doctrinal analysis of EU legislation alongside a review of Member States' implementation practices, the research evaluates how this Directive and other relevant instruments (including the General Data Protection Regulation (GDPR) and the Digital Services Act (DSA)) strengthen protections for victims and what challenges arise in their enforcement. The findings indicate that while the EU's recent initiatives represent a significant step forward, gaps and inconsistencies remain in practice, pointing to the need for further integrated strategies and stronger coordination to ensure a truly effective EU-wide response to online violence against women.

2. Conceptual and Legal Definition of Cyberviolence Against Women

Cyber violence is often referred as a new form of violence, grounded in the increased use of new digital technologies and maximised by the constant connectivity of Web 2.0. In addition to this, it is often considered to be less harmful due to its remote nature. This is an absolute fallacy since it is more of an old problem. Thus, it can start online and continue offline or start offline and continue online; so, it can also come from or lead directly to physical harm. It reflects forms of abuse and victimisation in the physical world that are depicted via digital means, or it may be a precursor to abuse that will be pursued in the physical world.¹⁶³ Predominantly, the root cause of violence against women and girls is gender inequality (discrimination, gender stereotypes, sexism). Moreover, women who have more than one commonly-targeted characteristic – for example, women of color, members of minority religions, or people who identify as LGBTQ – may be attacked more frequently. Violence and abuse online may limit women's right to express themselves equally, freely and without fear. Cyberviolence affects women disproportionately, not only causing them psychological harm and suffering but also deterring them from digital participation in political, social and cultural life.¹⁶⁴

¹⁵⁸ Van Der Wilk, Adriane (2018.), *Cyber violence and hate speech online against women: WOMEN'S RIGHTS & GENDER EQUALITY*, European Parliament's Policy, Study for the FEMM Committee, Department for Citizens' Rights and Constitutional Affairs, Directorate General for Internal Policies of the Union, p. 10.

¹⁵⁹ Consolidated version of the Treaty on European Union, OJ C 326, 26.10.2012, pp. 13–390.

¹⁶⁰ Charter of Fundamental Rights of the European Union, OJ C 326, 26.10.2012, pp. 391–407.

¹⁶¹ Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence, OJ L, 2024/1385, 24.5.2024.

¹⁶² United Nations, *Cyberviolence Against Women and Girls: The Growing Threat of the Digital Age*, <https://unric.org/en/cyberviolence-against-women-and-girls-the-growing-threat-of-the-digital-age/> (3.4.2025.)

¹⁶³ Polyzoidou, Vagia (2024.), Digital Violence Against Women: Is There a Real Need for Special Criminalization?, *Int J Semiot Law*, Vol. 37, p. 1780.

¹⁶⁴ See more at: Council of Europe, Cyberviolence against women, <https://www.coe.int/en/web/cyberviolence/cyberviolence-against-women> (04.04.2025.)

The rapid expansion of the digital realm has brought immense benefits, from connectivity to education and economic opportunities. However, it has also created a fertile ground for gender-based violence to evolve and proliferate. Studies across the world show that 16 to 58 per cent of women and girls have been targeted by violence online. Cyberviolence against women and girls is a pervasive issue, encompassing a wide range of harmful behaviours that exploit the anonymity and reach of digital platforms.¹⁶⁵

Violence against women and domestic violence is a violation of fundamental rights such as the right to human dignity, the right to life and integrity of the person, the prohibition of inhuman or degrading treatment or punishment, the right to respect for private and family life, the right to liberty and security, the right to the protection of personal data, the right to non-discrimination, including on the grounds of sex, and the rights of the child, as enshrined in the Charter and the United Nations Convention on the Rights of the Child.¹⁶⁶ While technology-facilitated violence has an extensive reach, women and girls are disproportionately impacted. Available evidence suggests that women are more likely to be targeted because of their sex and gender identity, to experience more severe forms, and are also more likely to face serious and longer-lasting negative impacts.¹⁶⁷ We can agree that cyber violence against women and girls is an emerging new dimension of gender-based violence. While both women and men may experience incidents of online interpersonal violence and abuse, evidence at EU, international and national levels shows that women and girls are considerably more likely to experience repeated and severe forms of physical, psychological or emotional abuse and to suffer from severe consequences.¹⁶⁸

Cyber violence and hate speech online against women are a form of Gender-Based Violence (GBV). The terms “cyber violence” and “hate speech online against women” encompass different types of cyber violence such as cyber harassment, cyber stalking, non-consensual image-abuse, and also the specific term “sexist hate speech”.¹⁶⁹ Gender-based harassment today has evolved into a form of violence that can be broadly defined as the use of online aggression, such as attacks, negative comments, ridicule, and sexual references with women as targets when they display content online.¹⁷⁰ Furthermore, verbal expressions frequently serve as a tool for sexist harassment, often characterized by a blend of opinionated statements and language that is offensive, hostile, or demeaning. Individuals identified by feminine usernames or aliases in online chats, forums, and gaming environments are disproportionately targeted with sexually explicit threats and inappropriate content.¹⁷¹

Scientists define cyberviolence as: 1) deliberate systematic actions by one person or group of persons, performed through electronic communication means, against another person(s) and

¹⁶⁵ United Nations, *Cyberviolence Against Women and Girls: The Growing Threat of the Digital Age*, <https://unric.org/en/cyberviolence-against-women-and-girls-the-growing-threat-of-the-digital-age/>.

¹⁶⁶ See paragraph 3 of Preamble of Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence, *OJ L*, 2024/1385, 24.5.2024.

¹⁶⁷ Berryhill, Alex & Fuentes, Lorena (2023.), *Technology-facilitated Violence against Women: Taking stock of evidence and data collection*, UN Women and World Health Organization, p. 4.

¹⁶⁸ European Institute for Gender Equality (2022.), *Report: Gender-based violence: Combating Cyber Violence against Women and Girls*, pp. 10. Available at: https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf?utm_source=chatgpt.com (05.04.2025.)

¹⁶⁹ There is however no commonly accepted terminology for these relatively new forms of violence against women. Online platforms where these various forms of violence and abuse occur include social media (e.g. Facebook, Twitter, Instagram, LinkedIn), web content and discussion sites (e.g. Reddit), search engines (e.g. Google), messaging services (e.g. Whatsapp, Facebook Messenger, Snapchat, WeChat or Skype), blogs, dating websites and apps, comment sections of media and newspapers, forums (e.g. 4chan), chat rooms of online video games, etc. See more in: Van Der Wilk, Adriane, *op. cit.*, p. 11.

¹⁷⁰ Rodríguez-Darias, Alberto Jonay & Aguilera-Ávila, Laura (2018.), *Gender-based harassment in cyberspace. The case of Pikara magazine*, Women's Studies International Forum, Vol. 66, pp. 63-69. Available at: <https://doi.org/10.1016/j.wsif.2017.10.004>

¹⁷¹ Bosch, Núria Vergés & Gil-Juarez, Adriana (2021.), A situated approach to online gender-based violence and ways to counter them, *Revista Estudos Feministas*, Vol. 29, No. 3. Available at: <https://doi.org/10.1590/1806-9584-2021v29n374588>.

establishing a hostile, humiliating environment to frighten, violate a person's rights to life and health, honour, respect, dignity, property, safe education and limit the free will of the person(s), etc.; 2) aggressive, intentional actions committed by a group or an individual consisting of humiliation, harassment and intimidation of another person through using the means of information communications.¹⁷²

The Advisory Committee urges the EU and its Member States to formally recognise cyberviolence as a form of violence against women. While many institutions struggle to provide a comprehensive definition, the Committee builds on UN and Council of Europe standards to propose one that frames cyberviolence as gender-based harm—whether physical, sexual, psychological or economic—committed via digital technologies. It encompasses acts like harassment, stalking, hate speech, non-consensual image-sharing, and identity theft. Crucially, the definition emphasises that cyberviolence is not a separate digital issue but part of the broader continuum of violence against women.¹⁷³

The gender dimension of cyberviolence is a distinct and important feature. Certain forms of cyberviolence affect women and girls disproportionately,¹ take more severe forms and have a more debilitating effect on women and girls. They include stalking, harassment, misogynistic hate speech, non-consensual sharing of personal data or images, and other violations of privacy. Female politicians, journalists and human rights defenders face higher levels of public abuse in the online world than their male counterparts. The digital environment is a prolific medium for attacks and abuse against women politicians because such acts occur anonymously, reach large audiences and aim to silence their target. According to UNESCO „women journalists and media workers face increasing offline and online attacks and are subject to disproportional and specific threats“.¹⁷⁴

3. European Union Legal and Policy Responses to Cyberviolence Against Women

Violence against women is a persisting manifestation of structural discrimination against women, resulting from historically unequal power relations between women and men. It is a form of gender-based violence inflicted primarily on women and girls by men. It is rooted in socially constructed roles, behaviour, activities and attributes that a given society considers appropriate for women and men.¹⁷⁵

The European Union's approach to gender-based violence has progressively evolved, transitioning from an initial emphasis on gender equality in employment to recognizing violence against women as a fundamental human rights concern. A key development was the 1997 Amsterdam Treaty, which formally embedded gender equality into EU competences, paving the way for more robust legal measures. The 2011 Istanbul Convention, although signed by the EU in 2017, faced ratification delays due to member state resistance, exposing the need for a unified legal framework.

¹⁷² In the scientific literature, when referring to violence using communication, the concepts of “cyberbullying” and “cyberviolence” are used. Thus, researchers define cyberbullying: 1) online bullying, which denotes the commission of violent acts designed to annoy, harm, or humiliate a person through various information and communication media, such as: mobile phones, e-mail, social networks, forums, blogs, online video games; 2) bullying performed using electronic communications; 3) intentional, systematic, against a person's will, psychological influence of one person on the mind of another, performed with the purpose of defaming, humiliating, intimidating, insulting, harassing a person and using information and communication means and transmitted to another persons in the form of messages, videos, photos, video recordings. See more in: Medvedska, Viktoriia V. (2022.), Theoretical and Legal Aspect of Cyberviolence Against Women, *Law. Human. Environment.*, Vol. 13, No. 2, pp. 27-28.

¹⁷³ European Commission, Advisory Committee on Equal Opportunities for Women and Men (2020.), “*New notification: cyberviolence against women has been flagged*”: *Opinion on combatting online violence against women*, pp. 1-8. Available at: https://commission.europa.eu/document/download/eae53eb9-ca88-4fc0-8a6e-51e771c96f68_en?filename=opinion_online_violence_against_women_2020_en.pdf (06.04.2025.)

¹⁷⁴ Zamfir Ionel, Murphy Colin (2024.), *Cyberviolence against women in the EU*, European Parliamentary Research Service, p. 3. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767146/EPR_SBRI%282024%29767146_EN.pdf (07.04.2025.)

¹⁷⁵ See paragraph 10 of Preamble of Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence, *OJ L*, 2024/1385, 24.5.2024.

This culminated in the adoption of the 2024 Directive on Combating Violence Against Women and Domestic Violence, which builds on earlier EU legislation and introduces expanded protections, including the criminalisation of digital violence, while addressing the deep-rooted societal causes of such violence.¹⁷⁶

3.1. Directive (EU) 2024/1385 on Combating Violence Against Women and Domestic Violence

In 2021, the United Nations (hereinafter: the UN) declared violence against women (hereinafter: VAW) and girls a ‘shadow pandemic’. While the nature and extent of such violence and abuse was already significant, the Covid-19 pandemic had intensified rates of violence, particularly domestic violence and online abuse. Accordingly, the UN called for coordinated and worldwide action to reduce prevalence, support victims and ensure legal responses are comprehensive and effective. In this context, the European Commission published in March 2022 a landmark proposal for a Directive on combating violence against women and domestic violence. The overall aim of the Directive is to ‘effectively combat VAW and domestic violence throughout the EU’ by laying down minimum rules on the definition of relevant criminal offences and penalties, as well as proposing measures relating to access to justice, victim support and prevention.¹⁷⁷

The first-ever binding European Union legal instrument to combat violence against women and domestic violence was approved on the 14th of May 2024 by the EU and has already been published in the Official Journal of the EU. This Directive, known as Directive 2024/1385 on combating violence against women and domestic violence (Directive), marks a historic moment for equality and equal opportunities in the European Union and is a significant symbol of the EU’s dedication to achieving not only de jure but also de facto equality.¹⁷⁸ The Directive on Combating Violence Against Women and Domestic Violence represents a pivotal step in the European Union’s ongoing commitment to addressing gender-based violence. By introducing standardised measures across member states, the Directive seeks to prevent violence, protect victims, and prosecute offenders while tackling contemporary challenges, such as digital violence.¹⁷⁹ The Directive aims to establish a unified framework across the EU to prevent and combat violence against women and domestic violence by reinforcing legal definitions, ensuring victim protection and access to justice, improving support services, enhancing data collection, and promoting prevention and coordinated action.¹⁸⁰

The Directive criminalises at EU level several types of cyberviolence on the basis of Article 83 of the Treaty on the Functioning of the European Union (hereinafter: the TFEU) and sets minimum standards for defining the most severe forms of cyberviolence - those likely to cause significant harm or instill serious fear for the victim’s safety or that of their dependants. While cyber-incitement is limited to acts that threaten public order or are abusive or insulting, Member States may adopt stricter provisions to address such conduct.¹⁸¹

Importantly, the Directive is the first EU legislative instrument to explicitly acknowledge that violence against women stems from “historically unequal power relations”.¹⁸² Following the European

¹⁷⁶ Kumbisek, Akerke *et al.* (2025.), *An Analysis of the EU’s Directive on Combating Violence Against Women and Domestic Violence*, European Student Think Tank. Available at: <https://esthinktank.com/2025/02/24/an-analysis-of-the-eus-directive-on-combating-violence-against-women-and-domestic-violence/> (08.04.2025.)

¹⁷⁷ Rigotti, Carlotta & McGlynn, Clare, Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission’s proposal to criminalise image-based sexual abuse, *New Journal of European Criminal Law*, Vol. 13, No. 4, p. 453.

¹⁷⁸ Kasim, Ceren (2024.), *Advancing Gender Equality: The EU’s Landmark Directive 2024/1385 on Violence Against Women*, EU Law Analysis: Expert insight into EU law developments. Available at: <https://eulawanaly sis.blogspot.com/2024/06/advancing-gender-equality-eus-landmark.html>.

¹⁷⁹ Kumbisek, Akerke *et al.*, *op. cit.*

¹⁸⁰ Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence, *OJ L*, 2024/1385, 24.5.2024.

¹⁸¹ Zamfir Ionel, Murphy Colin, *op. cit.*, p. 6.

¹⁸² This language highlights the broader social and cultural factors perpetuating such violence, framing it as a structural issue requiring systemic change. However, the directive’s adoption process also reveals tensions

elections in 2019, gender equality emerged as a prominent issue on the political agenda, supported notably by Ursula von der Leyen, the first female President of the Commission, and the specific appointment of a Commissioner for Equality. The inaugural address of Ursula von der Leyen to the European Parliament emphasized a strong commitment to prioritizing gender equality within her agenda. Shortly thereafter, the Commission released its “Gender Equality Strategy” aiming to foster a Union where individuals of all genders and backgrounds have the freedom to pursue their aspirations, with equal opportunities to thrive and actively participate in shaping the European society.¹⁸³ The Directive contributes to the von der Leyen Commission’s broader goal of establishing a “Union of Equality,” as outlined in the EU Gender Equality Strategy 2020–2025. This strategy focuses on eliminating gender-based violence, combating stereotypes, promoting equal participation and pay, and ensuring gender balance in leadership and policymaking.¹⁸⁴

As a legally binding instrument, the Directive carries greater enforceability, with non-compliance potentially leading to infringement proceedings and financial penalties. It expands legal protection to previously underregulated forms of violence, notably digital abuse and targeted attacks on public figures such as female politicians, and places strong emphasis on prevention and victim support. While it marks a significant advancement — described by civil society as a “groundbreaking step”—notable shortcomings remain, particularly regarding protections for migrant women and the absence of a consent-based definition of rape.¹⁸⁵

However, there is a missing human rights perspective in the Directive. Neither in the Preamble nor anywhere else does the Directive acknowledge that gender-based violence is a human rights violation. This recognition is a core element of the Istanbul Convention. However, the Directive refers to VAW and domestic violence as a violation of fundamental rights and, thereby losing its connection to the most significant human rights document on VAW and domestic violence in Europe. (Compare Art. 3(a) IC to Art. 2(a) Directive 2024/1385) The Directive missed an opportunity to align closely with the Istanbul Convention’s human rights approach, which would have been a groundbreaking step in addressing gender-based violence and domestic violence at the EU level.¹⁸⁶

The Directive also lacks a dedicated chapter addressing migrant women. The absence of an independent residence status, a secure status, or any status poses challenges for women, increasing their vulnerability to violence or exploitation in a variety of contexts by employers, intimate partners, or other individuals. As a result, they are less likely to report violence and abuse., limiting their access to justice and their ability to escape abusive situations, rendering them vulnerable to further abuse. Recently, the European Court of Justice in two landmark cases *WS v Bulgaria* (C-621/21)¹⁸⁷ and *K, L v*

among member states, with debates over terminology and scope. For instance, the final text excluded a unified definition of “gender”, and “sexual violence” based on consent, reflecting resistance from countries like Poland and Bulgaria that sought to limit progressive interpretations of these terms. Thus, while the 2024 directive builds on decades of advocacy and legal advancements, setting a new standard for combating violence against women in the EU, the political and cultural debates surrounding its adoption underscore the ongoing challenges of achieving consensus on gender equality across diverse member states. See more in: *Kumbisek, Akerke et al., op. cit.*

¹⁸³ Rigotti, Carlotta, McGlynn, Clare & Benning, Franziska (2024.), Image-Based Sexual Abuse and EU Law: A Critical Analysis, *German Law Journal*, Vol. 25, p. 1478.

¹⁸⁴ Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions a Union of Equality: Gender Equality Strategy 2020–2025, COM/2020/152 final.

¹⁸⁵ Overall, this can be used to great effect. For now, it is a welcome development, understood as a baseline level of protective and preventative measures that must be built upon. As far as accountability goes, the real test is whether the EU has the political willpower and desire to follow through on their words. This is a directive that fails to protect to the degree necessary, and as any other EU directive will, it faces barriers and challenges. It must not be mistaken as achieving total protection and must be supplemented with protections for migrant women, and definitions surrounding rape, and as the needs of victims and survivors, both preventative and responsive, develop it too must develop. However, it is the strongest stance the EU has taken and the most progressive one since the Istanbul Convention. It provides greater scope for future legislation on this and gives hope to campaigners. It is important, and at the same time, flawed. See: *Kumbisek, Akerke et al., op. cit.*

¹⁸⁶ See: Kasım, Ceren, *op. cit.*

¹⁸⁷ Case C-621/21, *WS v Bulgaria*, ECLI:EU:C:2024:47

Staatssecretaris van Justitie en Veiligheid (C-646/21)¹⁸⁸ reaffirmed the status of women as a whole, including minors, and women facing domestic violence in their country of origin in particular, and women who identify themselves with the fundamental value of equality between women and men qualify as a protected ‘social group’ in reference to Istanbul Convention. While the initial proposal included provisions to ensure that no personal data about victims of abuse, including residence status, would be shared by police with immigration authorities, the final text omits these safeguards (Art. 16(5) Proposal). As stated by many human rights organisations, this approach would run counter to the EU's rules on victims' rights (Victims' Rights Directive) and data protection (General Data Protection Regulation), which mandate rights and safeguards for all individuals without discrimination. This discrepancy with the Istanbul Convention contradicts the Convention's requirement that all women be treated equally, irrespective of their residence status.¹⁸⁹

In conclusion, the Directive represents a significant advancement in promoting gender equality within the European Union. It recognises the shared responsibility of Member States in addressing violence against women and domestic violence, advocating for a comprehensive framework to effectively prevent and combat such issues. By criminalising offences that were previously overlooked in EU Member States and establishing minimum standards that Member States can exceed, the Directive serves as a robust legal instrument.¹⁹⁰

3.2. Complementary EU Legal Instruments and Regulatory Frameworks

In addition to the dedicated Directive on violence against women, the EU's digital regulatory landscape includes several other instruments that complement the fight against cyberviolence. This section reviews three key frameworks – *Directive 2011/93/EU* on combating sexual abuse and exploitation of children, the *General Data Protection Regulation (GDPR)*, and the *Digital Services Act (DSA)* – and explains their supportive role in addressing online abuse of women. Though these instruments are not aimed exclusively at gender-based violence, each contributes to closing gaps in protection. For example, Directive 2011/93/EU harmonises the criminalization of online child sexual exploitation, which strengthens overall EU efforts against sexual abuse in digital environments (an area that can overlap with abuse targeting girls and young women). The GDPR empowers individuals (including victims of cyberstalking or “revenge porn”) with a “right to be forgotten,” enabling them to request the removal of personal data or intimate content posted without consent. Meanwhile, the DSA imposes robust duties on online intermediaries to detect and remove illegal content: it requires platforms – especially very large online platforms – to swiftly take down unlawful material, including non-consensual intimate images and hate speech, and to assess systemic risks to users' rights. Together, these complementary instruments bolster the EU's legal framework against cyberviolence by enhancing criminal accountability, victim remedies, and platform responsibility, working in tandem with the gender-focused Directive to protect women in digital spaces.

¹⁸⁸ Case C-18/16, *K, L v Staatssecretaris van Justitie en Veiligheid*, ECLI:EU:C:2017:680

¹⁸⁹ Kasim, Ceren, *op. cit.*

¹⁹⁰ It takes a holistic approach, providing detailed regulations and guidelines spanning from prevention and early intervention to protection, access to justice, victim support, and coordination and cooperation. While the Directive is a positive step forward, it falls short of the initial Proposal's ambition, lacking a clear gender perspective and specific regulations on certain forms of violence, particularly in the context of the world of work. Nevertheless, the Directive is poised to bring about significant changes in the legal norms of Member States and pave the way for a cultural shift in understanding and addressing gender inequality that persists in EU countries. This milestone should be celebrated, while also acknowledging that there is still much work to be done to enhance legal safeguards in preventing and eradicating gender-based violence and domestic violence. See: *Ibid.*

3.2.1. Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography

Although the escalation in online child sexual abuse material (CSAM) is not a novel problem, recent digital proliferation has brought about new alarming challenges in addressing the issue.¹⁹¹ For more than a decade, the EU has made consistent efforts to develop a comprehensive legal framework to address the challenge of child sex abuse. Crimes of this nature are particularly severe in that they cause long-term physical and psychological harm to victims who, by their very nature, are particularly vulnerable.¹⁹² In the EU, Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography¹⁹³ replaced the earlier Council Framework Decision 2004/68/JHA¹⁹⁴, introducing harmonised rules under Articles 82(2) and 83(1) TFEU¹⁹⁵. It defines relevant offences and penalties, includes these crimes among those warranting EU-level legal alignment, and sets out measures for prevention, prosecution, and victim protection.

This Directive establishes minimum rules concerning the definition of criminal offences and sanctions in the area of sexual abuse and sexual exploitation of children, child pornography and solicitation of children for sexual purposes. It also introduces provisions to strengthen the prevention of those crimes and the protection of the victims thereof.¹⁹⁶

3. 2. 2. General Data Protection Regulation (GDPR): Right to Be Forgotten and Its Limitations

The General Data Protection Regulation (hereinafter: GDPR)¹⁹⁷ governs how personal data must be collected, processed, and erased. The right to be forgotten appears in Recitals 65 and 66 and in Article 17 of the GDPR¹⁹⁸. It states, “The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay” if one of a number of conditions applies.

¹⁹¹ Parti, Katalin & Szabó, Judit (2024.), The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe, *Laws*, Vol. 13, No. 7, p. 1.

¹⁹² Buono, Laviero (2020.), *EU strategy for a more effective fight against child sexual abuse*, ERA Forum, Vol. 21, p. 361.

¹⁹³ Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335, 17.12.2011, p. 1–14.

¹⁹⁴ Council framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, *OJ L 13*, 20.1.2004, p. 44–48.

¹⁹⁵ Consolidated version of the Treaty on the Functioning of the European Union. *OJ C 326*, 26.10.2012, p. 47–390.

¹⁹⁶ Article 1 of Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335, 17.12.2011, pp. 1-14.

¹⁹⁷ Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), *OJ L 119*, 4.5.2016, pp. 1-88.

¹⁹⁸ In Article 17, the GDPR outlines the specific circumstances under which the right to be forgotten applies. An individual has the right to have their personal data erased if: a) the personal data is no longer necessary for the purpose an organization originally collected or processed it; b) an organization is relying on an individual's consent as the lawful basis for processing the data and that individual withdraws their consent; c) an organization is relying on legitimate interests as its justification for processing an individual's data, the individual objects to this processing, and there is no overriding legitimate interest for the organization to continue with the processing; d) an organization is processing personal data for direct marketing purposes and the individual objects to this processing; e) an organization processed an individual's personal data unlawfully; f) an organization must erase personal data in order to comply with a legal ruling or obligation; g) an organization has processed a child's personal data to offer their information society services.

“Undue delay” is considered to be about a month. You must also take reasonable steps to verify the person requesting erasure is actually the data subject.¹⁹⁹

The GDPR, in force since 2018, grants users the right to request deletion of personal data deemed inaccurate, excessive, or no longer relevant, and allows penalties for unauthorized disclosures. However, this right has shown limited effectiveness in addressing gender-based abuse, as victims face complex procedures and must identify every platform hosting the harmful content. Enforcement is further hindered by jurisdictional issues, with some non-EU platforms ignoring EU rules. Certain platforms, including some based in Cyprus - a hub for largely unregulated pornographic websites—have drawn criticism and are under investigation for potential data protection breaches.²⁰⁰

The right to be forgotten (or as it is called in the scientific literature “the right to erasure”, “the right to oblivion” or “the right to delist”) is a “product” of the judicial activism of the CJEU. The emergence and development of the right to be forgotten in the European legal practice is mainly connected with the unprecedented case of Google Spain (or the “Costeja case”), This judgment brought to the fore a lot of new questions about the legal essence and nature of the right to be forgotten and the scope and limits of application of this right in the European legal practice.²⁰¹ So in 2014, the Court of Justice of the European Union (CJEU) issued a notable decision declaring that individuals had a right to demand that search engines not report certain data about them in searches²⁰². The CJEU derived this right from the right to erasure, and this right has become known as the “right to be forgotten.”²⁰³

3.2.3. Digital Services Act (DSA): Platform Accountability and VLOPs Designation

The Digital Services Act (DSA)²⁰⁴ is a much awaited platform regulation reform in the European Union that was adopted on 1 November 2022, with the ambition to set a global example in terms of accountability and transparency. Among other obligations, the DSA emphasizes the need for online platforms to report on their content moderation activities.²⁰⁵

The DSA obliges platforms to implement tools for identifying and removing illegal content, including systems for user reporting and cooperation with 'trusted flaggers'. Recital 87 specifically addresses very large online platforms (VLOPs) distributing pornographic content, requiring them to ensure swift removal of non-consensual intimate or manipulated material. Under Article 34(1), VLOPs must also assess risks related to illegal content and threats to human dignity. As of December 2023, the EU designated Pornhub, Stripchat, and XVideos as VLOPs due to high user volumes, imposing stricter obligations. While these platforms challenge the designation before the Court of Justice, they are still required to implement additional safeguards—such as revising terms, interfaces, or

¹⁹⁹ See more at: GDPR.EU, *Everything you need to know about the “Right to be forgotten”*, <https://gdpr.eu/right-to-be-forgotten/> (14.04.2025.)

²⁰⁰ Zamfir Ionel, Murphy Colin (2024.), *Cyberviolence against women in the EU*, European Parliamentary Research Service, p. 6. Available at: [https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767146/EPRS_BRI\(2024\)29767146_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767146/EPRS_BRI(2024)29767146_EN.pdf) (14.04.2025.)

²⁰¹ KocharyanI, Hovsep *et al.* (2021.), *Critical Views on the Right to Be Forgotten After the Entry Into Force of the GDPR: Is it Able to Effectively Ensure Our Privacy?*, *International and Comparative Law Review*, Vol. 21, No. 2, p. 97.

²⁰² Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317

²⁰³ Solove, Daniel J. (2022.), *The Limitations of Privacy Rights*, *Notre Dame Law Review*, Vol. 98, No. 3, pp. 981.

²⁰⁴ 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), *OJ L 277*, 27.10.2022, pp. 1–102.

²⁰⁵ Kaushal, Rishabh, *Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database*, in: *ACM Conference on Fairness, Accountability, and Transparency (ACM FAccT '24)*, June 3–6, 2024, Rio de Janeiro, Brazil. ACM, New York, NY, USA, p. 1121.

algorithms—to prevent the spread of illegal and harmful content, including child sexual abuse material and deep-fake pornography.²⁰⁶

3. 3. Role of the Istanbul Convention and GREVIO Recommendations

The EU accession to the Istanbul Convention had long been a matter of debate. The Convention, adopted eight years earlier, outlines the potential for EU accession in Articles 75 and 76, a move that the European Parliament consistently supported through numerous resolutions and the Commission issuing a roadmap in 2015 for EU accession. Following a number of initiatives, in 2017 the EU signed the Convention, but there was considerable uncertainty around the legal basis, and the Council was reluctant to proceed with the ratification in the absence of a common accord among Member States, blocking the process for several years. Consequently, in 2019, the European Parliament sought an opinion from the European Court of Justice (“ECJ”) to clarify the appropriate legal basis and therefore the scope of EU accession and the ratification procedure. The ECJ delivered its Opinion 1/19 in October 2021,²⁰⁷ determining that the appropriate legal basis is Articles 78(2), 82(2), 84 and 336 of the Treaty of the Functioning of the European Union (“TFEU”), enabling the Council to adopt the Convention with qualified majority, without having to wait for agreement across the Member States. Indeed, a number expressed opposition to the ratification, objecting to the inclusion of the term “gender” and reflecting victim-blaming attitudes, gender stereotypes, and resistance to same-sex rights and sexual education in schools.

Accordingly, in 2023 the EU acceded to the Convention on those matters falling under its exclusive competence. This is a significant milestone, not only for its normative and symbolic implications but also because the Istanbul Convention now constitutes an integral part of EU law, serving as a legal source.²⁰⁸ In late 2023, the EU acceded to the Istanbul Convention²⁰⁹, which, although not explicitly addressing cyberviolence, includes it under the broader scope of gender-based violence defined in Article 3a. GREVIO, the Convention’s monitoring body, issued recommendations in 2021 urging state parties to strengthen their responses to cyberviolence²¹⁰. The Convention's monitoring framework highlights existing national measures and calls for greater efforts by EU Member States to enhance legal and institutional responses to digital gender-based violence.

GREVIO is the body of independent experts responsible for monitoring the implementation by the parties of the Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul Convention).²¹¹ In monitoring the implementation of the Istanbul Convention, GREVIO has identified that the digital dimension of VAW is often being overlooked in domestic laws and policies. In its General Recommendation No.1 on the digital dimension of violence

²⁰⁶ Zamfir Ionel, Murphy Colin, *op. cit.*, pp. 6-7.

²⁰⁷ Case C-1/19, Istanbul Convention, ECLI:EU:C:2021:832

²⁰⁸ Rigotti, Carlotta, McGlynn, Clare & Benning, Franziska (2024.), Image-Based Sexual Abuse and EU Law: A Critical Analysis, *German Law Journal*, Vol. 25, pp. 1479.

²⁰⁹ Council of Europe Convention on preventing and combating violence against women and domestic violence, Council of Europe Treaty Series - No. 210, Istanbul, 11.05.2011.

²¹⁰ GREVIO General Recommendation No. 1 on the digital dimension of violence against women (2021.), Council of Europe. Available at: <https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147>.

²¹¹ GREVIO draws up and publishes reports evaluating legislative and other measures taken by the parties to give effect to the provisions of the convention. In cases where action is required to prevent a serious, massive or persistent pattern of any acts of violence covered by the convention, GREVIO may initiate a special inquiry procedure. GREVIO may also adopt general recommendations on themes and concepts of the convention. Article 66 of the Istanbul Convention governs GREVIO membership. It provides that GREVIO shall have between 10 and 15 members, depending on the number of parties to the convention. See more at: Council of Europe, *About GREVIO – Group of Experts on Action against Violence against Women and Domestic Violence*, <https://www.coe.int/en/web/istanbul-convention/grevio>.

against women, the first it has adopted, it outlines the problem of both gender-based violence against women committed online and facilitated by technology. Based on the four pillars of the Istanbul Convention - Prevention, Protection, Prosecution and Coordinated Policies - the Recommendation proposes specific actions to be taken. It coins the term “the digital dimension of violence against women” as comprehensive enough to comprise both online acts of violence and those perpetrated through technology, including technology yet to be developed.²¹²

4. Practical Implementation and National Experiences

Cyberviolence against women is an EU-wide phenomenon, as shown by the 2018 European Parliament-commissioned study “Cyberviolence and hate speech against women”.²¹³ Several EU Member States, including France, the UK, Germany, Malta, Ireland, Italy, and Slovenia, have introduced laws criminalising non-consensual image-sharing and online sexual harassment. France has also expanded its definition of online harassment to cover coordinated group attacks. Nonetheless, in many countries, cyberviolence remains insufficiently addressed, often treated merely as an extension of offline offences. Outdated legal tools and limited police capacity hinder enforcement, leaving victims dissatisfied and reluctant to report, with many not recognising such abuse as a criminal act.²¹⁴

At national level, EU Member States collect data on cyberviolence either through surveys or based on crime reported to the authorities. Surveys are not comprehensive and may not include cyber forms of violence at all, or they may mix online and offline violence. Data based on the number of offences reported to the authorities significantly underestimate the extent of the cyberviolence, as only a few victims report it. Moreover, there is no common methodology that would enable data comparison across the EU.²¹⁵

At the EU level, comprehensive data on the various forms of cyberviolence remains lacking. The most notable effort is the European Union Agency for Fundamental Rights (FRA’s) 2012–2014 survey, which addressed online violence — particularly cyberstalking and harassment — as part of broader research on violence against women across all Member States. The FRA’s survey on violence against women in the EU shows for example that:

- 1) 20% of young women (18-29) in the EU have experienced cyber sexual harassment;
- 2) 77% of women who have experienced cyber harassment have also experienced at least one form of sexual or/ and physical violence from an intimate partner;

²¹² See more at: Council of Europe, *GREVIO's General Recommendation: General recommendation No. 1 on the digital dimension of violence against women*, <https://www.coe.int/en/web/istanbul-convention/general-recommendation>.

²¹³ Van Der Wilk, Adriane (2018.), *op. cit.*, pp. 1-80.

²¹⁴ European Commission, Advisory Committee on Equal Opportunities for Women and Men (2020.), “*New notification: cyberviolence against women has been flagged*”: *Opinion on combatting online violence against women*, p. 5. Available at: https://commission.europa.eu/document/download/ea53eb9-ca88-4fc0-8a6e-51e771c96f68_en?filename=opinion_online_violence_against_women_2020_en.pdf (26.05.2025.)

²¹⁵ Examples include the following:

1) The Dutch Central Bureau of Statistics (CBS) has produced several surveys on harassment, both online and offline, in the Netherlands, and on online security and crime, including threats and intimidation. According to data from the 2022 survey on harassment, 0.5 % of respondents experienced cyberharassment, while 0.3 % experienced both online and offline harassment. Data collected by CBS through their cybercrime survey in 2022 show that the percentage of people having experienced online threats, including harassment, stalking and shamesexting, was 4 %, with a slight difference between men and women. The share of those who had suffered shamesexting was 0.7 %;

2) A comprehensive survey on Crime and Safety in Germany, SKID 2020, contains data on certain types of cyberviolence – namely, online insults and threats – but they are not disaggregated by gender;

3) Spain publishes data (Portal estadístico de criminalidad) on computer-related crime reported to the authorities, disaggregated by gender. Women suffered slightly more than half of the 350 000 reported computer-related crimes in 2023. The vast majority of crimes consisted of fraud (computer, bank or credit card fraud), with relatively low levels of crime in other categories – numbers in the thousands in offences such as threats, discovery and revelation of secrets, violation of personal freedom, etc. See more in: Zamfir Ionel, Murphy Colin, *op. cit.*, pp. 5-6.

3) 70% of women who have experienced cyber stalking have also experienced at least one form of physical or/and sexual violence from an intimate partner;

4) 5% of women in the EU have experienced one or more forms of cyber stalking since the age of 15.²¹⁶

The 2019 FRA fundamental rights survey provided data on cyberharassment disaggregated by gender. It found that 13 % of women in the EU had been subjected to cyberharassment in the past 5 years, compared to 15 % of men. For cyberharassment, the highest rate was in the 16-29 age group: 27 % had experienced cyberharassment in the 5 years before the survey.²¹⁷

Italy's 2019 law on gender-based violence serves as a notable example of national legislation addressing cyberviolence. It criminalises the non-consensual distribution of sexually explicit material, with aggravated penalties when committed by a current or former partner, or if the victim is pregnant. The law also introduces specific offences such as identity violations and non-consensual image-sharing, ensures expedited legal procedures in domestic violence cases, and mandates specialised training for police officers.²¹⁸

Cooperation with major tech companies plays an important role in addressing cyberviolence against women. In 2017, Spain's PantallasAmigas launched the "Ten types of digital gender violence" campaign, highlighting early warning signs of abuse and cyberbullying, especially among youth, with active support from Twitter España. On the international level, the 2019 G7 Ministerial Meeting on Gender Equality called for user-friendly reporting tools and closer collaboration between platforms and civil society organisations. The 2016 EU Code of Conduct on illegal hate speech - though focused on racism and xenophobia, not gender-based hate - has proven effective, with companies reviewing around 89% of flagged content within 24 hours by 2018. The Code also promotes transparency, training, and partnerships, encouraging platforms to act more responsibly while improving their public image.²¹⁹ Posting sexually explicit images without consent, known as "nonconsensual pornography" or "revenge porn," is a form of image-based sexual abuse.

Although the GDPR introduced the right to erasure in 2018, allowing users to request removal of harmful personal data, its impact has been limited. By April 2020, the UK's Revenge Porn Helpline reported 250 cases - double the previous year - while in Ireland, 140,000 women's images were leaked. In response, Ireland adopted strict legislation in December, introducing penalties of up to 10 years' imprisonment and unlimited fines. Belgium followed with similar measures, including prison sentences and fines up to €15,000.²²⁰

Member States increasingly recognise the seriousness of cyberviolence against women, with several adopting laws targeting online abuse, such as non-consensual image-sharing and harassment. Italy's 2019 legislation is a notable example of a comprehensive national response. Public-private initiatives and awareness campaigns have also contributed to improving victim support and visibility. Despite this progress, many countries still treat cyberviolence as a mere extension of offline abuse, resulting in weak enforcement and fragmented data collection. The GDPR's right to erasure has had limited effect, prompting some states to adopt stricter laws. A more unified EU strategy, stronger enforcement, and consistent data practices remain crucial for an effective response.

²¹⁶ European Union Agency for Fundamental Rights (2014.), "Violence against women: an EU-wide survey", pp. 1-200. Available at: <http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report> (18.04.2025.)

²¹⁷ Zamfir Ionel, Murphy Colin, *op. cit.*, p. 5.

²¹⁸ European Commission, Advisory Committee on Equal Opportunities for Women and Men (2020.), *op. cit.*, p.

²¹⁹ European Commission, Advisory Committee on Equal Opportunities for Women and Men (2020.), *op. cit.*, p.

²²⁰ Politico, *How Europe's privacy laws are failing victims of sexual abuse*. Available at: <https://www.politico.eu/article/how-europe-privacy-laws-are-failing-victims-of-sexual-abuse/> (28.05.2025.)

5. Conclusion and Recommendations

The future of cyberviolence against women is deeply concerning. The potential for abuse in up and coming immersive digital environments, such as the metaverse or virtual reality, is already raising alarms, with perpetrators finding increasingly sophisticated ways to exploit vulnerable individuals. Additionally, the global nature of the internet enables cyberviolence to transcend national borders, complicating efforts to hold perpetrators accountable. Weak or inconsistent legal frameworks further exacerbate the issue, leaving many victims without adequate recourse.²²¹

The European Union has made significant progress in addressing cyberviolence against women through a strengthened legal framework, most notably with Directive 2024/1385 and complementary instruments such as the GDPR and Digital Services Act. These measures mark a critical step forward in recognizing online gender-based violence as a serious legal and human rights issue. However, enforcement remains uneven, and emerging technologies present new risks that outpace existing regulations. To enhance the EU's response to cyberviolence against women, it is essential that Member States ensure the full and timely implementation of Directive 2024/1385, accompanied by adequate training and resources for relevant authorities. The harmonisation of definitions and data collection practices across the Union is also necessary to enable coherent, evidence-based policymaking.

Furthermore, cross-border cooperation must be strengthened to improve the investigation and prosecution of online abuse, which often transcends national jurisdictions. Online platforms should be held accountable for illegal content, with an emphasis on promoting safer design features and more effective reporting mechanisms. Special attention must be given to the specific vulnerabilities of marginalised groups to guarantee equal access to justice and protection. Lastly, educational initiatives and public awareness campaigns should be developed to foster a culture of online respect and to empower women and girls to navigate the digital space safely. A coordinated and proactive EU strategy is crucial to ensure that the digital environment becomes a secure and equitable space for all.

References:

1. Berryhill, Alex & Fuentes, Lorena (2023.), *Technology-facilitated Violence against Women: Taking stock of evidence and data collection*, UN Women and World Health Organization, pp. 1-31.
2. Bosch, Núria Vergés & Gil-Juarez, Adriana (2021.), A situated approach to online gender-based violence and ways to counter them, *Revista Estudos Feministas*, Vol. 29, No. 3. Available at: <https://doi.org/10.1590/1806-9584-2021v29n374588>.
3. Buono, Laviero (2020.), *EU strategy for a more effective fight against child sexual abuse*, ERA Forum, Vol. 21, pp. 361–364.
4. Georgiadou, Ekaterini (2024.), *Gender-based violence: Does the practice meet the law?*, Heinrich Böll Stiftung Greece. Available at: <https://gr.boell.org/en/2024/07/03/legislative-response-gender-based-violence>.
5. Kasım, Ceren (2024.), *Advancing Gender Equality: The EU's Landmark Directive 2024/1385 on Violence Against Women*, EU Law Analysis: Expert insight into EU law developments. Available at: <https://eulawanalysis.blogspot.com/2024/06/advancing-gender-equality-eus-landmark.html>.
6. Kaushal, Rishabh, Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database, in: *ACM Conference on Fairness, Accountability, and Transparency (ACM FAccT '24)*, June 3–6, 2024, Rio de Janeiro, Brazil. ACM, New York, NY, USA, pp. 1121 – 1132.
7. KocharyanI, Hovsep *et al.* (2021.), Critical Views on the Right to Be Forgotten After the Entry Into Force of the GDPR: Is it Able to Effectively Ensure Our Privacy?, *International and Comparative Law Review*, Vol. 21, No. 2., pp. 96-115.
8. Kumbisek, Akerke *et al.* (2025.), *An Analysis of the EU's Directive on Combating Violence Against Women and Domestic Violence*, European Student Think Tank. Available at:

²²¹ United Nations, *Cyberviolence Against Women and Girls: The Growing Threat of the Digital Age*, <https://unric.org/en/cyberviolence-against-women-and-girls-the-growing-threat-of-the-digital-age/> (29.05.2025.)

<https://esthinktank.com/2025/02/24/an-analysis-of-the-eus-directive-on-combating-violence-against-women-and-domestic-violence/>.

9. Medvedska, Viktoriia V. (2022.), Theoretical and Legal Aspect of Cyberviolence Against Women, *Law. Human. Environment.*, Vol. 13, No. 2, pp. 25-31.
10. Parti, Katalin & Szabó, Judit (2024.), The Legal Challenges of Realistic and AI-Driven Child Sexual Abuse Material: Regulatory and Enforcement Perspectives in Europe, *Laws*, Vol. 13, No. 7, pp. 1-19.
11. Polyzoidou, Vagia (2024.), Digital Violence Against Women: Is There a Real Need for Special Criminalization?, *Int J Semiot Law*, Vol. 37, pp. 1777-1797.
12. Rodríguez-Darias, Alberto Jonay & Aguilera-Ávila, Laura (2018.), *Gender-based harassment in cyberspace. The case of Pikara magazine*, Women's Studies International Forum, Vol. 66, pp. 63-69. Available at: <https://doi.org/10.1016/j.wsif.2017.10.004>.
13. Rigotti, Carlotta, McGlynn, Clare & Benning, Franziska (2024.), Image-Based Sexual Abuse and EU Law: A Critical Analysis, *German Law Journal*, Vol. 25, pp. 1472-1493.
14. Rigotti, Carlotta & McGlynn, Clare, Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission's proposal to criminalise image-based sexual abuse, *New Journal of European Criminal Law*, Vol. 13, No. 4, pp. 452-477.
15. Solove, Daniel J. (2022.), The Limitations of Privacy Rights, *Notre Dame Law Review*, Vol. 98, No. 3, pp. 975-1036.
16. Van Der Wilk, Adriane (2018.), *Cyber violence and hate speech online against wome: WOMEN'S RIGHTS & GENDER EQUALITY*, European Parliament's Policy, Study for the FEMM Committee, Department for Citizens' Rights and Constitutional Affairs, Directorate General for Internal Policies of the Union, pp. 1-80.
17. Zamfir Ionel, Murphy Colin (2024.), *Cyberviolence against women in the EU*, European Parliamentary Research Service, pp. 1-11. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2024/767146/EPRS_BRI%282024%29767146_EN.pdf.

Case law of ECJ:

1. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317
2. Case C-1/19, Istanbul Convention, ECLI:EU:C:2021:832
3. Case C-18/16, K, L v Staatssecretaris van Justitie en Veiligheid, ECLI:EU:C:2017:680
4. Case C-621/21, WS v Bulgaria, ECLI:EU:C:2024:47

Legal Sources, opinions and other acts:

1. Charter of Fundamental Rights of the European Union. OJ C 326, 26.10.2012, str. 391-407.
2. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions a Union of Equality: Gender Equality Strategy 2020-2025, COM/2020/152 final.
3. GREVIO General Recommendation No. 1 on the digital dimension of violence against women (2021.), Council of Europe. Available at: <https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147>.
4. Consolidated version of the Treaty on European Union, OJ C 326, 26.10.2012, p. 13-390.
5. Consolidated version of the Treaty on the Functioning of the European Union. OJ C 326, 26.10.2012, pp. 47-390.
6. Council framework Decision 2004/68/JHA of 22 December 2003 on combating the sexual exploitation of children and child pornography, OJ L 13, 20.1.2004, pp. 44-48.
7. Council of Europe Convention on preventing and combating violence against women and domestic violence, Council of Europe Treaty Series - No. 210, Istanbul, 11.05.2011.
8. Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence, OJ L, 2024/1385, 24.5.2024.
9. Directive 2011/93/EU of the European Parliament and of the Council of 13 December 2011 on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA, OJ L 335, 17.12.2011, pp. 1-14.
10. European Commission, Advisory Committee on Equal Opportunities for Women and Men (2020.), "New notification: cyberviolence against women has been flagged": *Opinion on combatting online violence against women*, pp. 1-8. Available at: https://commission.europa.eu/document/download/eae53eb9-ca88-4fc0-8a6e-51e771_c96f_68_en?filename=opinion_online_violence_against_women_2020_en.pdf.

11. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ L 119, 4.5.2016, pp. 1–88.
12. 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), OJ L 277, 27.10.2022, pp. 1–102.

Reports:

1. European Institute for Gender Equality (2022.), *Report: Gender-based violence: Combating Cyber Violence against Women and Girls*, pp. 1-110. Available at: https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf?utm_source=chatgpt.com.
2. European Union Agency for Fundamental Rights (2014.), *“Violence against women: an EU-wide survey”*, pp. 1-200. Available at: <http://fra.europa.eu/en/publication/2014/violence-against-women-eu-wide-survey-main-results-report>

Web sources:

1. Council of Europe, *About GREVIO – Group of Experts on Action against Violence against Women and Domestic Violence*, <https://www.coe.int/en/web/istanbul-convention/grevio>.
2. Council of Europe, *Cyberviolence against women*, <https://www.coe.int/en/web/cyberviolence/cyberviolence-against-women>.
3. Council of Europe, *GREVIO's General Recommendation: General recommendation No. 1 on the digital dimension of violence against women*, <https://www.coe.int/en/web/istanbul-convention/general-recommendation>.
4. GDPR.EU, *Everything you need to know about the “Right to be forgotten”*, <https://gdpr.eu/right-to-be-forgotten/>.
5. Politico, *How Europe's privacy laws are failing victims of sexual abuse*. Available at: <https://www.politico.eu/article/how-europe-privacy-laws-are-failing-victims-of-sexual-abuse/>.
6. United Nations, *Cyberviolence Against Women and Girls: The Growing Threat of the Digital Age*, <https://unric.org/en/cyberviolence-against-women-and-girls-the-growing-threat-of-the-digital-age/>.

NOVA PRAVILA U BORBI PROTIV CYBER NASILJA NAD ŽENAMA: PRAVNE REGULATIVE I POLITIKE EVROPSKE UNIJE

Ajna JODANOVIĆ,

redovni profesor, Pravni fakultet, Univerziteta u Bihacu i Fakultet za Međunarodne odnose i diplomatiju, Sarajevska škola za nauku i tehnologiju (Sarajevo School of Science and Technology - SSST)

Vladimir M. SIMOVIĆ,

tužilac Tužilaštva BiH i redovni profesor Fakulteta za bezbjednost i zaštitu, Nezavisni univerzitet u Banjoj Luci

Sažetak: Kao posljedica sve veće upotrebe naprednih tehnologija i interneta u svakodnevnom životu i djelovanju, nasilje nad ženama u digitalnom svijetu postaje sve ozbiljniji pravni i društveni problem na nivou Evropske unije. U nastojanju da pruži adekvatan odgovor na ovaj rastući izazov, Unija posljednjih godina uvodi sveobuhvatne pravne mjere i politike s jedinstvenim ciljem zaštite žena od različitih oblika digitalnog nasilja, od kojih se u posljednje vrijeme najviše izdvajaju cyber uznemiravanje, digitalno uhođenje, rodno zasnovani govor mržnje, te neovlašteno dijeljenje intimnih sadržaja. Ovaj rad analizira posljednju pravnu regulativu koja je Evropska unija usvojila u nastojaju da unaprijedi zaštitu žena u digitalnom prostoru, s posebnim naglaskom na Direktivu o borbi protiv nasilja nad ženama i nasilja u porodici, koja predstavlja prvi zakonodavni akt na unijskom nivou koji

prepoznaje cyber nasilje kao oblik rodno zasnovanog nasilja, te postavlja obavezu državama članicama da kriminalizuju određene oblike digitalnog nasilja, osiguraju efikasne mehanizme zaštite žrtava, kao i da omoguće pristup pravnim lijekovima. Pri analizi pravnog okvira Evropske unije u odnosu na borbu protiv cyber nasilja nad ženama, posebna pažnja u radu će se posvetiti načinu na koji Opšta uredba o zaštiti podataka (GDPR) doprinosi zaštiti privatnosti i sigurnosti žena na internetu, kao i Digital Services Act (DSA), koji uvodi strožije obaveze u odnosu na digitalne platforme s ciljem uklanjanja nezakonitog sadržaja i preduzimanja preventivnih mjera protiv cyber nasilja.

Cilj ovog rada je da prikaže pravne regulative i politike Evropske unije kao značajan pomak u kontekstu borbe protiv nasilja nad ženama u digitalnom prostoru, ali i da ukaže na izazove u njihovoj primjeni. Kroz analizu trenutnih politika i njihovog uticaja, kao i iskustava država članica Evropske unije u području implementacije zakonodavnih mjera, rad ističe važnost daljeg razvoja integrisanih strategija koje će osigurati sveobuhvatnu zaštitu žena u digitalnom prostoru na unijskom nivou.

Ključne riječi: *Evropska unija, digitalno nasilje, žene, pravni okvir i politike EU.*