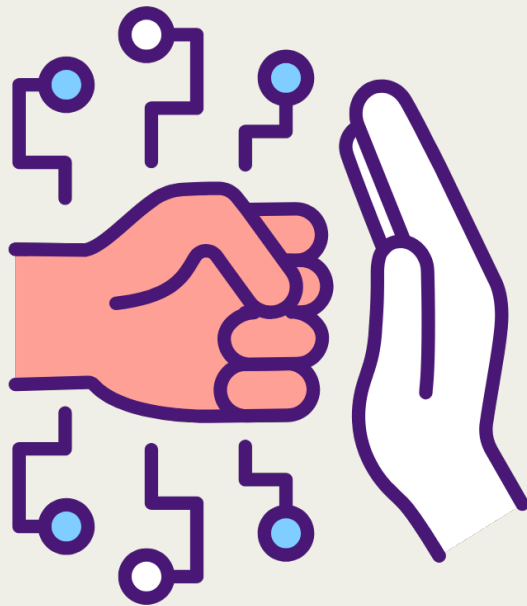


# OVERVIEW OF LEGISLATIONS REGULATING CYBERVIOLENCE



**Authors:**

Baia Patariaia  
Ekaterine Muzashvili  
Mariam Getsadze  
Goga Khatiashvili

# Contents

The scale and consequences of cyberviolence.....	3
Forms of cyberviolence.....	6
<i>Online sexual harassment</i> .....	6
<i>Image-based sexual abuse</i> .....	7
<i>Sextortion</i> .....	11
<i>Cyberbullying</i> .....	11
<i>Cyberstalking</i> .....	12
<i>Sexting</i> .....	12
<i>Doxing</i> .....	13
<i>Impersonation (imitation)</i> .....	13
Council of Europe Conventions.....	14
GREVIO standards.....	17
ECHR resolutions .....	21
Legislations of the European Union Member States .....	26
<i>Online threats</i> .....	26
<i>Online surveillance</i> .....	26
<i>Cyberviolence based on gender</i> .....	28
<i>Image-based sexual abuse</i> .....	28
<i>Blackmail using intimate photos</i> .....	30
<i>Cyberbullying</i> .....	31
<i>Cyber-grooming</i> .....	32
<i>Cyber harassment</i> .....	34
<i>Online hate speech</i> .....	35
<i>Other non-criminal provisions</i> .....	36
<i>Subjective composition of cyberviolence</i> .....	37
Experience of other countries .....	38
In search of a solution .....	42

# The scale and consequences of cyberviolence

Online violence, similar to physical violence, is deeply rooted in power dynamics, economic imbalances and patriarchal attitudes, reinforcing the idea of women's inferiority in relation to men. These damaging beliefs and attitudes are deeply embedded in the fabric of societies and thus require a large-scale societal change. States have an obligation to fight against digital forms of violence against women. This is an integral part of their comprehensive approach to preventing this type of violence, protecting victims, supporting them and prosecuting perpetrators<sup>1</sup>.

Cyberviolence has a grave social and economic impact on women; studies show that women aged 18 to 24 are at the highest risk of stalking, sexual harassment and physical threats<sup>2</sup>. According to the European Union, as recently as 2015, 18% of girls (approximately 9 million women) had experienced serious forms of online violence by the age of 15<sup>3</sup>. According to the same study, in 74% of the 86 countries surveyed, law enforcement agencies and courts were unable to take appropriate measures against cyberviolence<sup>4</sup>. Currently, the legislative framework has improved, however, the trend of prevalence of cyberviolence is much wider, as the scale of using social networks has been increased as never before. Using the Internet on a mobile phone, criminals can easily reach their targets. They can harass many people simultaneously. Also, at this time, it is possible to potentially maintain anonymity, which further complicates the process of regulating crime<sup>5</sup>.

*According to data of 2021, **every second young woman** has experienced cyberviolence<sup>6</sup>.*



---

<sup>1</sup> GREVIO General Recommendation No. 1 on the digital dimension of violence against women, 20 October 2021, 18. para. 35.

<sup>2</sup> Final report of the Broadband Commission Working Group on Gender, September 2015, Combatting Online Violence Against Women & Girls: A Worldwide Wake-up Call, Highlights.

<sup>3</sup> Final report of the Broadband Commission Working Group on Gender, September 2015, Combatting Online Violence Against Women & Girls: A Worldwide Wake-up Call, Highlights.

<sup>4</sup> Final report of the Broadband Commission Working Group on Gender, September 2015, Combatting Online Violence Against Women & Girls: A Worldwide Wake-up Call, Highlights.

<sup>5</sup> Cyber Sexual Harassment: A Summary of Current Measures and Implications for Future Research, Elizabeth Reed, Alice Wong and Anita Raj, 2019, 2.

<sup>6</sup> European Parliamentary Research Service (EPRS), Combating gender-based violence: Cyberviolence, European added value assessment, 2021.

In 2021, the United Nations (hereinafter: UN) declared violence against women and girls as a “shadow pandemic”<sup>7</sup>. The statistics above demonstrate that cyberviolence is a growing crime, requiring adequate efforts from states to address it.

Girls may be targeted for online violence simply because of their gender and young age, and when it comes to their political views, disabilities, skin color, or LGBTIQ+ identity, the level of violence worsens. The extent of harassment due to an opinion can range from humiliation and threats of violence to the forced display of unwanted pornographic images. Similar to harassment in general, online harassment is a continuous, often psychologically damaging process that can result in physical harm as well<sup>8</sup>.

Access to Internet and online safety are fundamental human rights issues. Social media platforms provide spaces for girls and young women to debate on these issues, but the more often girls speak out, the more often they are threatened and humiliated. Harassment should not limit the right of girls and young women to enjoy all the opportunities offered by the social media. Discussions on issues they are curious about, their various activities or their right to express their opinions are hindered by systematic bullying. Neither the platforms nor the perpetrators are responsible for this<sup>9</sup>.

30% of women across the EU fear that their fake intimate images will be shared without their consent; additionally, this is possible through the use of “nude / stripping” apps, which can be accessed by millions of people around the world. The apps allow users to upload non-sexual photos and have them almost instantly transformed into nude photos. Many women and girls may not even know they have become the victims of such violence<sup>10</sup>.

---

<sup>7</sup> UN Women, ‘Measuring the Shadow Pandemic: Violence against Women during COVID-19’ (2021) <<https://data.unwomen.org/sites/default/files/documents/Publications/Measuring-shadow-pandemic.pdf>> Seen: February 19, 2024.

<sup>8</sup> Free to be online? Girls’ and young women’s experiences of online harassment, Plan International, Girls Get Equal, 2020, 8.

<sup>9</sup> Free to be online? Girls’ and young women’s experiences of online harassment, Plan International, Girls Get Equal, 2020, 8.

<sup>10</sup> Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission’s proposal to criminalise image-based sexual abuse, Carlotta Rigotti and Clare McGlynn, 2022, 457-458; “Nudifying” AI Tools Which “Undress” Women in Photos Are Gaining Traction, but What Is Being Done to Stop It, and How Can We Protect Our Images Online?’ Glamour, 7 December 2021, < <https://www.glamourmagazine.co.uk/article/nudification-intimate-image-abuse> >, seen February 19, 2024.

In March 2022, the European Commission published a Proposal for a Directive on combating violence against women and domestic violence<sup>12</sup>.

Lack of awareness about this issue leads to cyberattacks and national authorities' perception of this type of violence as less serious than physical violence. Moreover, law enforcement agencies and the judiciary often lack the necessary technical training to effectively investigate such incidents of violence<sup>11</sup>.

The overall objective of the directive is to “effectively combat violence against women and domestic violence across the European Union” by establishing minimum rules for the definition of criminal offences and penalties, as well as for access to justice, support for victims and crime prevention. The document defines cyberviolence as, inter alia, the manipulation or dissemination of intimate material without consent, cyberstalking and cyberbullying, and notes that cyberviolence, especially against women, is used and encouraged by violent right-wing extremist and terrorist groups. Cyberviolence is particularly used against female politicians, journalists and human rights defenders to silence them<sup>13</sup>.

Cyberviolence is not a legal category that is common to many jurisdictions, therefore it is not easy to determine the extent to which the current laws cover such acts. In part, this is because criminal laws, like laws in general, were not originally designed to eliminate gender-based harm: general criminal categories have long failed to reflect harms done to women and their experiences, and laws criminalize only specific categories of offenses. In addition, legal systems continuously fall behind technological developments<sup>14</sup>.

There are many new forms of violence against women - “**doxing**”, “**sextortion**” and “**trolling**”. Some forms of violence against women have the prefix “online” - online mobbing, online stalking and online harassment. Other forms of violence have also developed, such as the non-consensual distribution of intimate content (so-called “revenge porn”)<sup>15</sup>.

---

<sup>11</sup> GREVIO General Recommendation No. 1 on the digital dimension of violence against women, 20 October 2021, 18. para. 34.

<sup>12</sup> European Commission Proposal for a Directive of the European Parliament and of the Council on combating violence against women and domestic violence', 2022 <<https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX-%3A52022PC0105>>, seen: February 19, 2024.

<sup>13</sup> Ibid.

<sup>14</sup> Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission's proposal to criminalise image-based sexual abuse, Carlotta Rigotti and Clare McGlynn, 2022, 460; 'Regulating New Technologies in Times of Change', Ronald Leenes, (Springer) 9.

<sup>15</sup> Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, General Assembly, 18 June 2018, A/HRC/38/47, para. 33.

In 2021, the European Parliament called on the EU and its Member States to take action to eliminate cyberviolence against women, as cyberviolence is often linked to and is a continuation of violence in the physical space<sup>16</sup>. It also listed a wide range of forms of online violence.

Crimes against women and girls can include “online sexual and psychological harassment, cyber-intimidation, non-consensual disclosure of sexual images, sexist hate speech online and new forms of online harassment such as “Zoom bombing” or “threats in the internet”<sup>17</sup>. In particular, it explicitly identified “image-based sexual abuse,” including cases where “the recording or distribution of a sexual encounter without consent” is “weaponized” against women, as well as the growing problem of “**deep-fake**” pornography, where artificial intelligence is used to exploit, humiliate, and harass women<sup>18</sup>.

This paper aims to review regulations related to cyberviolence in both international instruments and domestic legislation, in order to allow us to clearly see legislative gaps in this area and opportunities for its improvement.

## Forms of cyberviolence

### *Online sexual harassment*

Among the types of cyberviolence, online sexual harassment is one of the most common forms. It is defined as a range of sexually aggressive or harassing images or texts delivered through the use of digital mediums.<sup>19</sup> In their publication, cyber sexual harassment researchers Reed, Wong, and Rai discuss the gendered nature of this crime and the serious social impacts on the behavior and mental health of adolescent girls. According to the researchers, cyber sexual harassment mainly manifests itself in three forms: **(1)** unwanted requests of sexual content; **(2)** unwanted messages/photos of sexual content; **(3)** messages/photos of sexual content shared without the victim’s consent<sup>20</sup>:

---

<sup>16</sup> European Parliament resolution of 14 December 2021 with recommendations to the Commission on combating gender-based violence: cyberviolence (n 6) Recital F; European Parliament resolution of 16 September 2021 with recommendations to the Commission on identifying gender-based violence as a new area of crime listed in Article 83(1) TFEU (n 6) Recital C.

<sup>17</sup> European Parliament resolution of 16 September 2021 with recommendations to the Commission on identifying gender-based violence as a new area of crime listed in Article 83(1) TFEU (n 6) para. 33.

<sup>18</sup> European Parliament resolution of 14 December 2021 with recommendations to the Commission on combating gender-based violence: cyberviolence (n 6) Recitals T-U.

<sup>19</sup> Cyber Sexual Harassment: A Summary of Current Measures and Implications for Future Research, Elizabeth Reed, Alice Wong and Anita Raj, 2019, 2.

<sup>20</sup> Cyber Sexual Harassment: A Summary of Current Measures and Implications for Future Research, Elizabeth Reed, Alice Wong and Anita Raj, 2019, 2-9.

- **Unwanted requests of sexual content** include requests that the victim participate in sexual behavior. For example, requests to exchange photos/messages of sexual content, requests for the victim to have sexual intercourse with the perpetrator, and requests to perform sexual behavior in front of a video camera.
- **Receiving unwanted messages/photos of sexual content**, also known as unwanted “sexting,” includes receiving unwanted sexually explicit photos, emails, text messages, or comments.
- **Sexually explicit messages/photos shared without the victim’s consent**, also known as “revenge porn”. Photos and messages of the victim may be spread via private message, shared with a third party, or shared publicly.

It must be distinguished whether a sexual image/message was sent in a private message or via email, collectively. It is also necessary to determine whether the sexual images received belong directly to the sender or were found online, as they can vary depending on the sender’s intention and the impact on the other party to the communication. In addition, the elements of crime need to be better defined, focusing on the unwanted nature of the communication. To summarize, it is necessary to define the elements in order to better assess the context (private or group message), the content (e.g., whether the sender shares their private sexually explicit photo) and the presence of consent from another party to the communication<sup>21</sup>. Online harassment can be carried out by one individual or by a group of individuals (mobbing). As a rule, this is done by online groups of violent men who aim to harass women and minorities<sup>22</sup>.

## ***Image-based sexual abuse***

Image-based sexual abuse is a term that encompasses the creation of intimate photo or video content without the consent of the person(s) shown in the content, all forms of filming or sharing such material, including altered or manipulated media products, and the threat to share such material. It is an “umbrella term” that describes interconnected forms of abuse and is therefore not limited to the non-consensual dissemination of intimate material<sup>23</sup>.

---

<sup>21</sup> Cyber Sexual Harassment: A Summary of Current Measures and Implications for Future Research, Elizabeth Reed, Alice Wong and Anita Raj, 2019, 9.

<sup>22</sup> A Training Handbook for Criminal Justice Practitioners on Cyberviolence Against Women and Girls (CVAWG), UNODC, 2022, 40; VAW Learning Network (2013). Technology-related Violence Against Women. Available online at < [https://gbvlearningnetwork.ca/our-work/issuebased\\_newsletters/](https://gbvlearningnetwork.ca/our-work/issuebased_newsletters/) >.

<sup>23</sup> Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission’s proposal to criminalise image-based sexual abuse, Carlotta Rigotti and Clare McGlynn, 2022, 454-455; Clare McGlynn, Erika Rackley and Ruth Houghton, ‘Beyond “Revenge Porn”: The Continuum of Image-Based Sexual Abuse’, 2017, 25.

The term “image-based sexual abuse” includes both “revenge porn,” when ex-partners spread intimate material without consent, and other actions such as threats to share photos and messages without consent, and the sharing of stolen images. It is noteworthy that the term “image-based sexual abuse” goes beyond sharing and includes the non-consensual creation of intimate images or videos, as well as the use of technology and artificial intelligence to modify non-sexual images into sexual or pornographic images (often referred to as “deep-fakes”).

It also includes taking intimate pictures without the consent of the person depicted, including cases where the victim is photographed secretly, while changing clothes, showering, sleeping, under the influence of drugs or alcohol, as well as with the help of hidden cameras in public places, on public transport, or as a result of coercion. Such forms of violence include “up-skirting”, “sextortion” and the taking and spreading of photographs depicting sexual violence<sup>24</sup>.

The term “image-based sexual abuse” was coined in response to the term “revenge porn,” which is still used around the world but is misleading. Many victims believe that the term implies some responsibility on their part, an act that results in “revenge.” The term is also misleading because it focuses only on one form of abuse and motivation, failing to reflect the interests or experiences of victims<sup>25</sup>.

In the 1980s, the first court case concerned a magazine that published nude photos of women, along with their personal details. In 2008, a new online website, IsAnyoneUp.com, was launched, and we saw the devastating effects of cyber harrasment and revenge porn. The website allowed users to upload intimate photos of their former partners, along with their personal details. In just one month, the website had a staggering 30 million users. It was shut down in 2012<sup>26</sup>.

The number of cases of image-based sexual abuse is also alarming. In her 2022 study, Carlotta Rigotti reviews statistics from different countries and presents a grim picture<sup>27</sup>: for example, in 2020, more than 100,000 images of Irish women and girls were spread online, which ultimately led to the criminalization of all forms of image-based sexual abuse. Similar experiences have been reported in other countries, such as Italy, where websites were recently discovered with thousands of users sharing sexual images without the consent of the individuals depicted.

---

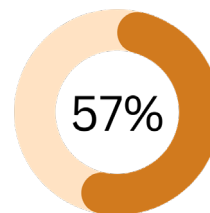
<sup>24</sup> Ibid.

<sup>25</sup> Ibid.

<sup>26</sup> The Criminalisation of Revenge Pornography, Elaine Degiorgio, *Elsa Malta Law Review*, 113: Lajuan and Billy Wood vs. Hustler Magazine, Inc. 736 F.2d 1084 (5th Cir. 1984) U.S. Court of Appeals for The Fifth Circuit - 736 F.2d 1084 (5th Cir. 1984) (July 23, 1984).

<sup>27</sup> Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission's proposal to criminalise image-based sexual abuse, Carlotta Rigotti and Clare McGlynn, 2022, 456; ‘Gardaí, Looking into Allegations That Large Number of Images of Women Were Shared Online without Their Consent’ 19 November 2020 < <https://www.thejournal.ie/images-of-irish-women-shared-without-consent-5271799-Nov2020/> > seen: February 19, 2024.

*According to a 2021 study conducted in 51 countries, including many European countries, 57% of women have been victims of image-based sexual abuse.*



Research in New Zealand and the UK showed that one in three adults is a victim of image-based sexual abuse. In addition, recent statistics from Ireland show that threats to share intimate images increased by 85% in the past year; thousands of fake pornographic images of women are being created for internet sales. The study also shows that victims are mostly young, representatives of sexual and ethnic minorities, persons with disabilities and people of color<sup>28</sup>.

Israeli lawmaker Yifat Kariv calls this crime “virtual rape,” suggesting that stricter laws are needed to reduce the rate of such crimes. Under the new Israeli law, the perpetrator could face up to five years in prison. In addition, as a civil offense, the victim can be awarded compensation of NIS 50,000, without proof of damage. Moreover, higher compensation can be awarded if actual damage is proven. Accordingly, in Israel, there is no need to prove damage, but the loss is sufficient to receive compensation<sup>29</sup>.

Most criminal law frameworks define sexual nature in terms of the nudity of the person depicted and/or their involvement in sexual activity. Some states’ lawmakers have specified intimate areas that are specifically protected from view and have named specific body parts that must be covered. In this way, it is likely that the law also applies to non-consensual nude photographs taken in changing rooms, restrooms, and other public spaces. Another approach is to allocate the area by referring to “intimate” images. Terminologically, this can be expressed as a synonym for the word “sexual”, included as an additional definition, or its frames can be expanded<sup>30</sup>.

It is also noteworthy that the terminology of “intimate” images can be interpreted more broadly, considering cultural specificities. In particular, it can extend to images that are considered sexual and/or intimate in some minority communities (for example, the absence of a headscarf or other religious attire in the photo) <sup>31</sup>.

---

of Nonconsensual Porn: Understanding and Addressing a Growing Form of Sexual Violence’, Asia A. Eaton and Clare McGlynn, Policy Insights from the Behavioral and Brain Sciences, 2020, 190.

<sup>28</sup> Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission’s proposal to criminalise image-based sexual abuse, Carlotta Rigotti and Clare McGlynn, 2022, 457; ‘The Psychology

<sup>29</sup> The Criminalisation of Revenge Pornography, Elaine Degiorgio, Elsa Malta Law Review, 121; Yifa Yaakov, ‘Israeli Law Makes Revenge Porn a Sex Crime’ The Times Of Israel, 6 January 2014, < <https://www.timesofisrael.com/israeli-law-labels-revenge-porn-a-sex-crime/> >, seen February 19, 2024.

<sup>30</sup> Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission’s proposal to criminalise image-based sexual abuse, Carlotta Rigotti and Clare McGlynn, 2022, 463.

<sup>31</sup> Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission’s proposal to criminalise image-based sexual abuse, Carlotta Rigotti and Clare McGlynn, 2022, 463; English Law Commission (n 46) 84-86.

There are also broader definitions. For example, Swedish laws on “intrusive photography” include photographs taken secretly in a person’s private space. Belgian criminal law provisions on “voyeurism” are focused on the disclosure of a specific part of the body and concentrate on whether a person would have covered that part of the body if they knew someone was taking pictures of them<sup>32</sup>. It is a separate issue whether the laws exclude images that were originally taken or shared with consent. Such distinctions are introduced by fault elements, whereby the victim is responsible for their own harm because they initially shared the image, although without consent to further sharing.

There should be no such distinctions, as the focus should be on any subsequent non-consensual photo-taking or spreading, regardless of whether the image was originally taken and shared with or without consent<sup>33</sup>.

There are different requirements for qualification as a crime in different countries, such as, for example, the repetition of the act (to underscore the repeated doing of the unwanted act, the stalking of the victim and their harassment in this way, or the explicit pornographic content of the shared photo, especially explicit or obscene images). Although the above definitions do not impose liability for a single act and emphasize the need for additional circumstances for qualification as a crime, it can still be assumed that there is a consensus around the criminalization of using some forms of intimate images without right<sup>34</sup>.

There is a separate regulation for intimate footage obtained without consent. For example, the law criminalizes the filming of intimate parts of the body that a person has protected from public view (including “up-skirting” and “down-blousing”, or a situation where a person is in a residential home or room specifically shielded from public view).

Image-based sexual abuse draws on the myths about motives and victims. The reality is that image-based sexual abuse is motivated by control. Many victims suffer devastating harm due to the double sexual standards and social and political context of online violence against women. The lack of support leaves them in isolation<sup>35</sup>.

---

<sup>32</sup> Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission’s proposal to criminalise image-based sexual abuse, Carlotta Rigotti and Clare McGlynn, 2022, 463; Chapter 4 Section 6a. Swedish Criminal Code; Article 417/8 Belgian Criminal Code.

<sup>33</sup> Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission’s proposal to criminalise image-based sexual abuse, Carlotta Rigotti and Clare McGlynn, 2022, 464;

<sup>34</sup> Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission’s proposal to criminalise image-based sexual abuse, Carlotta Rigotti and Clare McGlynn, 2022, 465.

<sup>35</sup> Shattering Lives and Myths: A Report on Image-Based Sexual Abuse. Australian Research Council (ARC), McGlynn, C. et al, 2019, 1.

## **Sextortion**

Sextortion is defined as “the abuse of power to obtain sexual favors or advantage”<sup>36</sup>. Online abusers use fake profiles to communicate and deceive victims on social media. After gaining the victims’ trust, they convince them to engage in video calls or send them intimate photos. As a result, online abusers take and record these videos and images, which are then used to harass and extort money from the victims.

In some cases, when the victim refuses to comply with the online abuser’s request, the images are posted on social media or sent to the victim’s friends<sup>37</sup>. Both children and men become victims of this crime.

## **Cyberbullying**

Cyberbullying can occur through digital devices such as mobile phones, computers and tablets, through texting, apps, online social media, forums or games, that is, anywhere where people can exchange content and communicate. Cyberbullying involves sending, publishing or sharing negative, harmful, false or pointless content about another person. It may involve sharing another person’s private information, causing the victim to feel embarrassed or humiliated. Cyberbullies may also send threatening or brutal messages, or impersonate another person in order to send messages that are embarrassing or annoying to the victim. An online bully is also called an internet troll - a person who deliberately tries to offend, cause trouble, or directly attack people<sup>38</sup>. Cyberbullying is usually considered a crime committed among or against minors (under 18 years of age). The bully often has a sense of anonymity, as minors are often reluctant to report online bullying to adults.

Cyberbullying most often occurs through social media, including Facebook, Instagram, Snapchat, and TikTok.<sup>39</sup>

Cyberbullying is:<sup>40</sup>

---

<sup>36</sup> A Training Handbook for Criminal Justice Practitioners on Cyberviolence Against Women And Girls (CVAWG), UNODC, 2022, 39; International Association of Women Judges (IAWJ): Naming, Shaming, and Ending Sextortion – A Toolkit (2012) < [https://www.unodc.org/res/ji/import/guide/naming\\_shaming\\_ending\\_sextortion/naming\\_shaming\\_ending\\_sextortion.pdf](https://www.unodc.org/res/ji/import/guide/naming_shaming_ending_sextortion/naming_shaming_ending_sextortion.pdf) > seen February24, 2024.

<sup>37</sup> A Training Handbook for Criminal Justice Practitioners on Cyberviolence Against Women and Girls (CVAWG), UNODC, 2022, 39; MAUCORS (The Mauritian Cybercrime Online Reporting System): Sextortion, <[https://maucors.govmu.org/maucors/?page\\_id=1073](https://maucors.govmu.org/maucors/?page_id=1073) >.

<sup>38</sup> A Training Handbook for Criminal Justice Practitioners on Cyberviolence Against Women and Girls (CVAWG), UNODC, 2022, 39. Internet trolling: A definition. <<https://www.endsleigh.co.uk/blog/post/what-is-internet-trolling/> >.

<sup>39</sup> A Training Handbook for Criminal Justice Practitioners on Cyberviolence Against Women and Girls (CVAWG), UNODC, 2022, 39.

<sup>40</sup> A Training Handbook for Criminal Justice Practitioners on Cyberviolence Against Women and Girls (CVAWG), UNODC, 2022, 40.

- Persistent – digital devices make it possible to communicate instantly and continuously 24 hours a day. As a result, children who are victims of cyberbullying may find it difficult to escape;
- Permanent – Most information communicated electronically is permanent and public if not reported or removed. A negative online reputation, including intimidation can impact a person’s education, college or university admissions, employment, and other areas of life.
- Hard to notice – Because teachers and parents of minors may not overhear or see cyberbullying, it is harder to recognize.

## ***Cyberstalking***

A concept related to cyberbullying - cyberstalking, is more often used against adults than minors. However, people of any age can be victims of cyberstalking. Cyberstalking can be defined as the use of the Internet to threaten or cause unwanted consequences for another person. Cyberstalking can be described as “the use of technology to stalk and monitor someone’s activities and behavior, in real time or historically”<sup>41</sup>.

## ***Sexting***

Sexting is a combination of the words “sex” and “text”. It can be defined as the exchange of sexually explicit messages, nude or semi-nude images of oneself via mobile phone or the Internet, using social media platforms such as instant messaging on Facebook, Twitter, email, etc.”<sup>42</sup> The images and photos used in sexting are usually voluntarily created by the person themselves, although the creation of such content may also be involuntary and may occur under coercion or pressure, especially in case of minors<sup>43</sup>. The distribution of sexting may or may not be voluntary.

---

<sup>41</sup> A Training Handbook for Criminal Justice Practitioners on Cyberviolence Against Women and Girls (CVAWG), UNODC, 2022, 40; UNFPA-Technology-Facilitated GBV (TFGBV) -Making All Spaces Safe, 2021, <[https://asiapacific.unfpa.org/sites/default/files/pub-pdf/unfpa-tfgbv-making\\_all\\_spaces\\_safe.pdf](https://asiapacific.unfpa.org/sites/default/files/pub-pdf/unfpa-tfgbv-making_all_spaces_safe.pdf) >.

<sup>42</sup> A Training Handbook for Criminal Justice Practitioners on Cyberviolence Against Women and Girls (CVAWG), UNODC, 2022, 41; Special Issue on Sexting: Current Research Gaps and Legislative Issues, Ngo, F., Jaishankar, K., Agustina, J.R., International Journal of Cyber Criminology (IJCC), 2017, July to December, Volume 11, Issue 2.

<sup>43</sup> Gender-based interpersonal cybercrime, UNODC, available: <https://www.unodc.org/e4j/en/cybercrime/module-12/key-issues/gender-based-interpersonal-cybercrime.html>

## ***Doxing***

Doxing is the non-consensual disclosure of personal information. It involves posting of an individual's personal information publicly – home and email addresses, phone numbers, employer and family contact information, or other types of personal information. Doxing is a form of online harassment that rarely occurs in isolation. More often, it is accompanied by other forms of harassment, such as image-based violence; minority groups, especially women of color and LGBTQIA+ people, become the victims of doxing<sup>44</sup> most often.

There are three types of doxing:<sup>45</sup>

- De-anonymization - the disclosure of someone's identity without right;
- Targeting – intentionally disclosing someone's personal information, which can reveal the victim's location. For most women, this can have serious safety implications;
- De-legitimization – spreading personal information in order to damage the victim's credibility or reputation, to shame, and humiliate them.

Doxing often leads to further online and physical harassment, such as receiving a large number of insulting messages and threats via email, social media, phone, or mail.

## ***Impersonation (imitation)***

Impersonation is the act of stealing someone else's identity for the purpose of threatening or intimidating them, as well as damaging their reputation. Perpetrators may create fake online accounts and websites to spread false information and damage the victim's reputation, destroying their personal or professional relationships. Often they place women's information in advertisements for sex work or on dating apps, and sometimes even incite others to commit violence against them<sup>46</sup>.

---

<sup>44</sup> A Training Handbook for Criminal Justice Practitioners on Cyberviolence Against Women and Girls (CVAWG), UNODC, 2022, 42; Doxing. *The International Encyclopedia of Gender, Media, and Communication*, Eckert, S and Metzger-Riftkin, J., 2020.

<sup>45</sup> A Training Handbook for Criminal Justice Practitioners on Cyberviolence Against Women and Girls (CVAWG), UNODC, 2022, 42; Douglas, D. 'Doxing: a conceptual analysis', *Ethics and Information Technology*, vol. 18, (2016), pp. 199–210.

<sup>46</sup> A Training Handbook for Criminal Justice Practitioners on Cyberviolence Against Women and Girls (CVAWG), UNODC, 2022, 42.

# Council of Europe Conventions

International instruments oblige signatory states to respond to gender-based crimes committed in cyberspace. Among these conventions, it is important to point out the Istanbul, Budapest and Lanzarote Conventions. These international instruments impose on signatory states the obligation to adopt the necessary legislative or other measures to ensure the effective investigation of the crimes covered by these conventions and the imposition of liability for the perpetrator, proportionate to their gravity, in each signatory state. The practice of the International Court of Human Rights has also developed in this direction, having repeatedly established a violation of Article 8 of the Convention by the state, since, in the cases under consideration, the state did not have the relevant legislation to combat cybercrime and failed to ensure an effective investigation of the crime<sup>47</sup>.

The Convention on Cybercrime, developed by the Council of Europe in Budapest in 2001, was the first international document to reflect the need to criminalize acts using the Internet and computer systems to commit crimes. In particular, the crimes provided for in the Convention were already regulated by the signatory states, however, the criminal codes did not consider computer systems and the Internet as a means of committing crimes: “This Convention is necessary to deter action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalization of such conduct, as described in this Convention, and the adoption of powers sufficient for effectively combating such criminal offences, by facilitating their detection, investigation and prosecution at both the domestic and international levels<sup>48</sup>.”

The text of the Convention emphasizes fraud committed through computer systems, cybersecurity, copyright protection, protection of personal data, and, in addition, contains general provisions on crimes committed through the Internet, the scope of which is wide and can be interpreted as norms regulating cybercrime. In this regard, Articles 4 (“Data interference”) and 5 (“System interference”) of the Convention are particularly important<sup>49</sup>.

---

<sup>47</sup> Volodina V Russia (Application No 40419/19), K.U V Finland (Application No 2872/02), Buturugă v Romania (Application No 56867/15).

<sup>48</sup> Preamble to the Convention.

<sup>49</sup> EIGE, Combating Cyber Violence against Women and Girls, 2022, P. 22

The Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, developed by the Council of Europe in 2007, was ratified by Georgia in 2014. Article 23 of the mentioned Convention directly obliges the signatory states to criminalize the so-called “grooming”, which refers to the intentional offer made by an adult using information and technology to commit a sexual or pornography-related crime with a child, if this offer was accompanied by material promises, which resulted in a meeting<sup>50</sup>.

In 2011, the Council of Europe developed the Convention on Preventing and Combating Violence against Women and Domestic Violence, which Georgia joined in 2017. The Convention does not contain a special stipulation regarding cyberviolence, however, in 2021, GREVIO clarified in its General Recommendation #1 that the crimes provided for in the Convention need to be combated in both the physical and virtual spaces, and that signatory states are obliged to combat violence against women, inter alia by preventing cybercrime. In this regard, Articles 33 (psychological violence), 34 (stalking) and 40 (sexual violence) of the Convention are particularly important<sup>51</sup>. GREVIO standards are additionally discussed in a separate sub- chapter.

Article 5, paragraph 2, of the Istanbul Convention obliges Member States to take the necessary legislative and other measures to prevent, investigate, punish and ensure accountability for acts of violence covered by the scope of this Convention that are perpetrated by non-State actors. This well-established concept, adopted in international and regional human rights instruments, policy documents and jurisprudence, is an obligation to adopt measures, not the results.

It obliges Member States to establish the necessary legal and policy frameworks to prevent and effectively investigate all forms of violence against women, with the purpose of imposing liability on perpetrators and providing victims with compensation. This is a provision of the Istanbul Convention that is central to ending impunity regarding gender-based violence against women and ensuring access to justice for women and girls who are victims of such violence.

---

<sup>50</sup> Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, <https://matsne.gov.ge/ka/document/view/2684715?publication=0>

<sup>51</sup> EIGE, Combating Cyber Violence against Women and Girls, 2022, P. 22

GREVIO considers that this obligation covers all forms of violence against women, including digital expressions and violence committed with the help of or through technology<sup>52</sup>. One of the foundations of the Istanbul Convention is to ensure a holistic response to all forms of violence against women and domestic violence at the state level, by proposing effective, comprehensive and coordinated policies that include a range of tools (Article 7).

A number of articles of the European Convention on Human Rights are relevant in cases of cyberviolence against women. In particular: Article 3 - Prohibition of torture, inhuman and degrading treatment; Article 8 - Right to private life; Article 10 - Freedom of expression; Article 14 - Prohibition of discrimination. It is noteworthy that the complaints referring to the above mentioned articles are already being submitted to the European Court of Human Rights. The relevant decisions are reviewed in a separate sub-chapter.

The Budapest Convention on Cybercrime together with Additional Protocol, adopted in 2001, was the first treaty to focus on Internet-related crimes, in particular computer fraud, copyright infringement, child pornography and network security breaches. The main goal of the Budapest Convention is to protect society from cybercrime by ensuring a common criminal justice policy, through appropriate legislation and international cooperation. Some of the articles of the Convention can be applied to cases of gender-based cyberviolence - Articles 4 and 5. they refer to interference with data and systems in a way that is likely to cause death or physical or psychological harm<sup>53</sup>. Three articles of the Budapest Convention are relevant to cyberviolence, namely<sup>54</sup>:

Article 4 – Data Interference. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

Article 5 - Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

---

<sup>52</sup> GREVIO General Recommendation No. 1 on the digital dimension of violence against women, 20 October 2021, 17. para. 34.

<sup>53</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 98.

<sup>54</sup> Convention on Cybercrime, 2001, Budapest. Available at: <https://rm.coe.int/16802fa423>

Article 9 – Offences related to child pornography. Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct: a) producing child pornography for the purpose of its distribution through a computer system; b) offering or making available child pornography through a computer system; c) distributing or transmitting child pornography through a computer system; d) procuring child pornography through a computer system for oneself or for another person; e) possessing child pornography in a computer system or on a computer-data storage medium.

Other substantive articles criminalize actions that may be involved in cyberbullying, but the connection is less direct. Such actions may contribute to violence and may be subject to criminal prosecution, but these articles do not criminalize violence itself.

The Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse criminalizes all forms of violence against children, including forms of cyberviolence, which refer to online sexual exploitation and sexual abuse - crimes related to child prostitution, child pornography, child corruption, and solicitation of a child for sexual purposes. These criminalized acts of cyberviolence are set out in Articles 18 to 23<sup>55</sup>.

## GREVIO standards

### *Online sexual harassment*

According to Article 40 of the Istanbul Convention, sexual harassment is “any form of unwanted verbal, non-verbal or physical conduct of a sexual nature with the purpose or effect of violating the dignity of a person, in particular when it creates an intimidating, hostile, degrading, humiliating or offensive environment<sup>56</sup>.”

In this sub-chapter, we will examine in detail GREVIO’s first general recommendation, which addresses the digital dimension of violence against women and identifies the following behaviors through online or digital means: **(1)** non-consensual sharing of images or videos; **(2)** non-consensual taking, production or obtaining of intimate images or videos; **(3)** exploitation, coercion and threats; **(4)** sexual bullying; and **(5)** cyber-flashing<sup>57</sup>.

---

<sup>55</sup> Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, 2007, Lanzarote \*available at: <https://rm.coe.int/168046e1cf>

<sup>56</sup> GREVIO General Recommendation No. 1 on the digital dimension of violence against women, 20 October 2021, 18. para. 37.

<sup>57</sup> GREVIO General Recommendation No. 1 on the digital dimension of violence against women, 20 October 2021, 18. para. 38.

- **The non-consensual sharing or threats to share a person’s nude or sexual photos or videos of a person** is image-based sexual abuse (also known as “revenge pornography”)<sup>58</sup>.
- **The non-consensual taking, production, or obtaining of intimate images or videos** includes “*up-skirting*” and other types of photographing in public, as well as the production of digitally altered images in which a person’s face or body is depicted in a pornographic photo or video. This practice is known as “fake pornography” (“deep-fake,” the creation of synthetic images using artificial intelligence)<sup>59</sup>.
- **Exploitation, coercion and threats** - fall within the scope of Article 40 of the Convention and include forms of violence such as forced sexting, sexual extortion, rape threats, sexual/gender doxing, impersonation and the disclosure of a person’s gender identity or sexual orientation without right (“outing”)<sup>60</sup>.
- **Sexual bullying** includes behaviors such as spreading rumors about a victim’s alleged sexual behavior, posting sexual comments under the victim’s posts or photos, impersonating the victim, sharing sexually explicit material with them, or sexually harassing them which affects the person’s reputation or livelihood, as well as “outing” a person without their consent for the purpose of intimidation, threats, and body shaming.
- **Cyber-flashing** entails sending unwanted sexual images using dating or messaging apps, texts, or other technologies (e.g., using Airdrop, Bluetooth).

Some of the above-mentioned behaviors are commonly known as **sexist hate speech**. As recognized in the Council of Europe Recommendation on preventing and combating sexism, these actions are often degrading and contribute to a social climate where women are humiliated, their self-respect is undermined, and their activities and choices are restricted, including work, private life, public or online space. Sexist behavior – sexist hate speech – is often a first step towards physical violence. It can escalate into or encourage overtly insulting acts and threats, including sexual assault, violence or rape, which fall within the scope of Article 40 of the Istanbul Convention<sup>61</sup>.

---

<sup>58</sup> GREVIO General Recommendation No. 1 on the digital dimension of violence against women, 20 October 2021, 18. para. 38(a).

<sup>59</sup> GREVIO General Recommendation No. 1 on the digital dimension of violence against women, 20 October 2021, 18. para. 38(b).

<sup>60</sup> GREVIO General Recommendation No. 1 on the digital dimension of violence against women, 20 October 2021, 18. para. 38(c).

<sup>61</sup> GREVIO General Recommendation No. 1 on the digital dimension of violence against women, 20 October 2021, 18. para. 39.

## ***Online and technology-facilitated stalking***

Article 34 of the Istanbul Convention defines stalking as “intentional conduct of repeatedly engaging in threatening conduct directed at another person, causing them to fear for their safety.” The Explanatory Report expands this definition further, clarifying that stalking committed through the use of information and communication technologies falls within the scope of Article 34: The threatening behavior may consist of repeatedly following another person, engaging in unwanted communication with another person or letting another person know that he or she is being observed. This includes physically going after the victim, appearing at her or his place of work, sports or education facilities, as well as following the victim in the virtual world (chat rooms, social networking sites, etc.).

Engaging in unwanted communication entails the pursuit of any active contact with the victim through any available means of communication, including modern communication tools and ICT devices<sup>62</sup>.

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

## ***Digital dimension of psychological violence***

In Article 33, the Istanbul Convention describes psychological violence as “the intentional conduct of seriously impairing a person’s psychological integrity through coercion or threats”. The Explanatory Report to the Convention specifies further: The extent of the offence is limited to intentional conduct which seriously impairs and damages a person’s psychological integrity which can be done by various means and methods. The Convention does not define what is meant by serious impairment. This provision refers to a course of conduct rather than a single event. It is intended to capture the criminal nature of an abusive pattern of behavior occurring over time<sup>63</sup>.

---

<sup>62</sup> GREVIO General Recommendation No. 1 on the digital dimension of violence against women, 20 October 2021, 19. para. 40.

<sup>63</sup> GREVIO General Recommendation No. 1 on the digital dimension of violence against women, 20 October 2021, 19-20. para. 42.

All forms of violence against women perpetrated in the digital space have a psychological impact and could be categorized as psychological violence perpetrated online and with the use of technology. The specific features of such violence against women increase the impact of the violence on victims. In addition, forms of psychological violence perpetrated in the context of domestic violence take radical forms when coupled with new technologies. For example, with the aid of the digital domain this can take a new dimension where current or former partners are in possession of victim's intimate images. Abusers can similarly misuse technology to track the whereabouts of their victims. Such forms of violence have a devastating mental and physical toll on women and girls<sup>64</sup>.

Economic abuse is closely related to psychological violence, which is defined as controlling a woman's ability to acquire, use, and maintain economic resources. Economic abuse usually occurs within the context of intimate-partner violence and has a negative impact on the physical and mental health of victims. In digital forums, economic abuse can manifest itself as controlling the bank accounts and financial activities of the victim through internet banking, damaging the victim's credit rating by using credit cards without permission or filing all financial contracts (leases, loans, utilities, etc.) in the name of the victim and failing to make payments on time or at all (in particular alimony payments)<sup>65</sup>.

In order to combat cyberviolence, GREVIO calls for the recognition of the gendered nature of online and technology-facilitated violence, which requires a response. GREVIO recommends that States Parties take the following measures in the areas of prevention, protection, prosecution and coordinated policies<sup>66</sup>:

- It is important to review legislation and adopt new legislation for **prevention**; taking into account the Recommendation CM/Rec(2019)1 of the Committee of Ministers of the Council of Europe on preventing and combating sexism, initiatives should be implemented that are aimed at combating gender stereotypes, discrimination and sexist attitudes.
- For **protection**, it is important that the legal framework related to violence against women extends to all forms of violence committed in the digital dimension.

---

<sup>64</sup> GREVIO General Recommendation No. 1 on the digital dimension of violence against women, 20 October 2021, 20. para. 43.

<sup>65</sup> GREVIO General Recommendation No. 1 on the digital dimension of violence against women, 20 October 2021, 21. para. 48.

<sup>66</sup> GREVIO General Recommendation No. 1 on the digital dimension of violence against women, 20 October 2021, 23. para. 49-57.

- For **prosecution**, it is important that the State equips law enforcement agencies with the necessary (human, financial and technical) resources to effectively investigate the digital dimension of violence against women, in line with the obligations under Article 5. This may include establishing specialized units/expertise and facilitating the coordination and cooperation of such units/experts with existing cybercrime units/experts; Specialists should be trained on how to obtain electronic evidence without secondary victimization and re-traumatization of victims. International cooperation and mutual legal assistance opportunities among criminal justice actors on issues related to the digital dimension of violence against women should also be increased to ensure easier access to evidence for service providers.
- **Coordinated policy** implies integrating the above issues into national state strategies, programs and action plans, as required by Article 7 of the Istanbul Convention.

## ECHR resolutions

This subchapter reviews the resolutions of the European Court of Human Rights that refer to various forms of cyberviolence.

### **K.U. v. Finland**<sup>67</sup>

On 15 March 1999, an unidentified person or persons placed an advertisement on an Internet dating site in the name of the applicant, who was 12 years old at the time, without her consent. The advertisement stated her age and year of birth, described her physical characteristics in detail, and provided a link to the applicant's website, which contained her photographs and telephone number. The advertisement stated that she wanted to have an intimate relationship with a boy of her age or older. The applicant learned about the advertisement on the Internet when she received an e-mail from a man offering to meet her.

---

<sup>67</sup> K.U. v. Finland, Application no. 2872/02, 02/03/2009.

In order to file a complaint, the applicant's father asked the police to identify the person who had placed the advertisement against his daughter, but the service provider refused to reveal his identity, as the law required protection of confidentiality. The police subsequently asked the Helsinki District Court (käräjäoikeus, tingsrätten) to order the service provider to disclose the information in question, in accordance with the criminal investigation, but all three instances refused to do so, as this would have been a violation of the Telecommunications Act on the Protection of Confidentiality and Data Security. Despite this regulation, the police was authorized to extract telecommunications identification data in connection with certain offences, although the law did not cover the offence in question<sup>68</sup>, the Court found a violation of Article 8 of the Convention. The aim of Article 8 is essentially to protect the individual against interference by public authorities without right, however it encompasses not only negative but also positive obligations, which entail effective protection of private or family life (see *Airey v. Ireland*, 9 October 1979, § 32, Series A no. 32)<sup>69</sup>.

The Court explained that it was undisputed that Article 8 of the Convention was applicable in the present case. The facts underlying the application refer to the issue of "private life", a concept which encompasses the physical and moral integrity of a person (see *X and Y v. the Netherlands*, cited above, § 22). Although the present case is a "misrepresentation" of a person under domestic law, the Court preferred to focus on these specific aspects of the concept of private life, namely the physical and mental well-being of the applicant, which was threatened by the present situation, which was all the more dangerous given her vulnerability, namely her young age.

The court did not specifically define cyber violence in this case, however, it noted that through this criminal offense, the defendant became a target of pedophiles<sup>70</sup>, and noted further that sexual violence is a serious crime, especially against children<sup>71</sup>. Accordingly, the court indirectly confirmed that this type of cyber violence is a form of sexual violence. While the choice of the means to secure compliance with Article 8 in the sphere of protection against acts of individuals is within the State's margin of appreciation, where essential aspects of private life are at stake, the availability of effective criminal law provisions is essential (see *X and Y v. the Netherlands*, cited above, §§ 23-24 and 27; *August v. the United Kingdom* (dec.), no. 36505/02, 21 January 2003; and *M.C. v. Bulgaria*, no. 39272/98, § 150, ECHR 2003-XII)<sup>72</sup>.

---

<sup>68</sup> Ibid, §§6-14. <sup>69</sup> Ibid, §42.

<sup>70</sup> Ibid, §41.

<sup>71</sup> Ibid, §§45; 48.

<sup>72</sup> Ibid, §43.

Although a criminal law provision existed in the present case, the Court held that it was not sufficient because, if there was no way of identifying the real perpetrator and bringing them to justice, the law had a limited effect. For the Court, States had a positive obligation inherent in Article 8 of the Convention to criminalize offences against the person, including attempted offences, and to use it effectively in practice, through effective investigation and prosecution (see, *M.C. v. Bulgaria*, no. 39272/98, ECHR 2003-XII §153)<sup>73</sup>.

### **Volodina v Russia**<sup>74</sup>

In November 2014, the applicant began a relationship with an Azerbaijani national, Mr S. After the breakup in 2015, S. threatened her with death and bodily harm, kidnapped her on several occasions and even assaulted her. In June 2016, the applicant learned from her brother that her account on the Russian social media platform, VKontakte, had been hacked. Her fictitious name had been changed to her real name, and her personal details, a passport photo and intimate photos had been uploaded to the account. In her account she had added her twelve-year-old son's classmates and teachers as friends. The applicant tried to log in to her account and discovered that the password had been changed. The police took a statement from the applicant's brother, according to which he spoke to S. and he admitted that he had hacked the applicant's email account and sent obscene messages to her contacts<sup>75</sup>.

Online, or cyberviolence, is closely linked to offline, or "real-life" violence and is considered as one more type of the complex phenomenon of domestic violence (*Buturugă*, §§ 74 and 78). States have a positive obligation to establish and effectively operate a system that punishes all forms of domestic violence and to provide sufficient guarantees for victims (see *Opuz v. Turkey*, no. 33401/02, § 145, ECHR 2009, and *Bălșan v. Romania*, no. 49645/09, § 57, 23 May 2017). The positive obligation applies to all forms of domestic violence, whether in real life or online. The Court held that this positive obligation – in some cases under Articles 2 or 3 and in other cases under Article 8, either alone or in conjunction with Article 3 of the Convention – includes specifically: (a) the obligation to establish and apply an adequate legal framework ensuring the protection of individuals against violence; (b) the obligation to take reasonable steps to prevent a real and imminent risk of repeated violence of which the authorities knew or ought to have known; and (c) the obligation to conduct effective investigations into acts of violence (*Buturugă*, §§ 60-62). The Court reiterates that the State's positive obligations under Article 8 to protect the physical or psychological integrity of an individual may extend to issues relating to the effectiveness of criminal investigations.

---

<sup>73</sup> *Ibid*, §46.

<sup>74</sup> *Volodina v. Russia*, Application No. 40419/19, 14/12/2021.

<sup>75</sup> *Ibid*, §§5-6.

The Court established a violation of the obligation to conduct an effective investigation in cases where the proceedings were continued without grounds or the perpetrators were given the opportunity to escape liability (P.M. v. Bulgaria, No. 49669. /07, §§ 64-66). The principle of effectiveness means that the authorities must under no circumstances leave the infliction of physical or psychological suffering unpunished<sup>76</sup>.

### **Høiness v. Norway** <sup>77</sup>

The applicant was a well-known lawyer who worked mainly on criminal and child custody cases. The case concerned the refusal of the domestic courts to impose civil liability on the host of an internet forum after vulgar comments about Ms. Høiness had been posted on the forum. The European Court found that regarding private life, there had been no violation of Article 8 of the Convention and that the applicant had not suffered serious harm because the website had moderators who were deleting such comments. In that case, there was no specific reference to the State's obligations, nor was there any violence or investigation, but rather a focus on criminalization.

### **Buturuga v. Romania** <sup>78</sup>

The applicant, Ms. Buturuga, was a victim of domestic violence. Her partner physically abused her and threatened to kill her. In addition, the applicant alleged that her partner had downloaded her private messages and photographs from her social media accounts without her consent. In order to prove this, she requested an investigation. The police refused, as they considered that the act was not related to domestic violence. Additionally, the prosecutor discontinued the criminal proceedings, despite the threats of violence and murder, because, they considered, the acts were not serious enough<sup>79</sup>. The Court found a violation of Articles 3 and 8 due to the failure to adequately investigate and take appropriate measures to address the complaints of domestic violence.

The Court emphasizes that special diligence is required in the examination of cases of domestic violence and considers that the specific nature of domestic violence, as recognized in the preamble to the Istanbul Convention, must be taken into account in the context of domestic proceedings (see M.G v. Turkey, § 93)<sup>80</sup>.

---

<sup>76</sup> Ibid, §67.

<sup>77</sup> Høiness v. Norway, Application no. 43624/14, 19/06/2019.

<sup>78</sup> Buturuga v. Romania, Application no. 56867/15, 11/06/2020.

<sup>79</sup> Ibid, §§7-21.

<sup>80</sup> Ibid, §67.

Under both domestic and international law, the phenomenon of domestic violence is not limited to the act of physical violence but is considered to include, among other aspects, psychological violence and factors of surveillance (C.M v. the Republic of Moldova, no. 26608/11, § 47, 28 January 2014)<sup>81</sup>. Furthermore, cyberbullying is now recognized as a form of violence against women and girls and can take many forms, including cyber-invasion, hacking into the victim’s computer and the collection, sharing and manipulation of data and images, including personal data. In the context of domestic violence, cyber-surveillance is often done by a person’s intimate partner<sup>82</sup>. The State argued that there was no evidence of violence from the applicant’s partner. The court noted that the investigators had not attempted to establish who had inflicted the injuries to the victim. They had only questioned three of the victim’s relatives, when they could have taken additional measures, such as interviewing neighbors, etc. <sup>83</sup>

It is noteworthy that following the February 10, 2020 resolution of the European Court of Human Rights, *Buturga v. Romania*, Romania amended its legislation. In July 2020, the latest amendment to the Law on Domestic Violence included cyberviolence as a form of domestic violence. Article 4, paragraph 1h, defines cyberviolence as: “Online harassment, online messages that incite hatred on the basis of gender, online stalking, online threats, non-consensual publication of information and intimate graphic content, unlawful access to communications and personal data and any other form of misuse of information and communication technologies through computers, smartphones or other similar devices that use telecommunications or can connect to the Internet and can be transmitted and used on social platforms or email platforms, with the aim of embarrassing, humiliating, intimidating, threatening or silencing the victim.” <sup>84</sup>.

The National Strategy for Combating and Preventing Sexual Violence, “SINERGY” 2020-2030, aims to reduce and prevent cases of sexual violence. The measures envisaged by the strategy include, inter alia, training of all relevant professionals in the prevention and fight against sexual violence; awareness-raising activities for journalists, bloggers and vloggers; analysis of the current legislative framework to strengthen safety in the online environment and combat pornography, “revenge pornography” and harassment/blackmail related to the dissemination of sexual material; psychological support for victims of sexual violence; collection of data on sexual violence crimes (including sexual harassment in the street and online crimes) and the creation of specialized units in prosecutors’ offices and law enforcement agencies. In addition, forensic medical services will be introduced for women victims of rape and sexual violence<sup>85</sup>.

---

<sup>81</sup> Ibid, §74.

<sup>82</sup> Ibid.

<sup>83</sup> Ibid, §68.

<sup>84</sup> GREVIO Baseline Evaluation Report, Romania, 2022, para. 7.

<sup>85</sup> GREVIO Baseline Evaluation Report, Romania, 2022, para. 41.

# Legislations of EU Member States

Forms of cyberviolence are usually distributed under different crimes in the domestic legislation of countries. In some cases, the definition of the crime indicates that the mentioned act can be committed online or in any other form. Only in some countries are forms of cyberviolence separated in separate crimes and their gender dimension is emphasized. In this sub chapter, we are interested in the legislation that recognizes different forms of cyberviolence as separate crimes.

## **Online threats**

Under **Greek** law, threats of violence or persistent stalking of a victim, carried out using telecommunications or electronic means, and causing terror or anxiety to the victim, are punishable<sup>86</sup>. According to the law of Cyprus, for a person who:

**a)** sends a message via a public communication network that is clearly offensive and/or obscene or threatening, or

**b)** sends a message via a public communication network with the intention of annoying, harassing and/or causing reasonable concern to another person, knowing that it is false and/or who is constantly using a public communication network<sup>87</sup>, the mentioned act is punishable by criminal law and, if convicted, the offender faces a fine of 1,700 euros<sup>88</sup>.

## **Online surveillance**

**Spanish** law envisages liability for the following acts:

---

<sup>86</sup> EIGE, Combating Cyber Violence against Women and Girls, 2022, P. 27; EIGE, Combating Cyber Violence against Women and Girls, 2022, Annex 5. Legal notes to Chapter 3, vi: <https://www.lawspot.gr/nomikes-plirofories/nomothesia/pk/arthro-333-poinikos-kodikas-apeili>

<sup>87</sup> EIGE, Combating Cyber Violence against Women and Girls, 2022, P. 27; EIGE, Combating Cyber Violence against Women and Girls, 2022, Annex 5. Legal notes to Chapter 3, x.

<sup>88</sup> Ibid.

- a) stalking;
- b) contacting or attempting to contact a person by any means;
- c) publishing any statement or other material by any means: 1. relating to, or seeming to relate to, a person, or 2. Seeming to be the work of that person;
- d) monitoring a person's use of the Internet, e-mail, or any other form of electronic communication;
- e) suspicious activity in a public or private space;
- f) interfering with any property in the person's possession;
- g) surveillance<sup>89</sup>.

**Slovak** law punishes a person who, through repeated observation, stalking or abusive behavior, tracks another person or intimidates them or their relatives by direct contact or electronic means<sup>90</sup>.

According to **Czech** law, dangerous stalking of a person is punishable, which is manifested in the following actions:

- a) threatens to inflict bodily harm or harms them or their close relative;
- b) seeks out or follows them;
- c) constantly contacts them using electronic communications, in writing or in any other form;
- d) abuses their personal data for the purpose of obtaining personal or other contact, which may cause the victim to have a well-founded fear of harm to their life or health or that of their close relative<sup>91</sup>.

According to Article 226 of the **Hungarian** Criminal Code, defamation is a crime and punishable if a person declares, disseminates or uses facts that are likely to harm the reputation of that person. The liability is aggravated if the defamation is committed: **a)** for any purpose or reason; **b)** in front of a large audience; **c)** which significantly harms the interests of the person; **d)** has caused significant harm to the interests of the person<sup>92</sup>.

---

<sup>89</sup> Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, Última actualización publicada el 28/04/2023, Artículo 172 ter, <https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444>

<sup>90</sup> Slovakia - Stalking, <https://www.coe.int/en/web/cyberviolence/-/slovakia-criminal-code-provisions-applied-to-cyber-violence>

<sup>91</sup> Czech Republic - Stalking, [https://eige.europa.eu/gender-based-violence/regulatory-and-legal-framework/legal-definitions-in-the-eu/czech-republic-stalking?language\\_content\\_entity=en](https://eige.europa.eu/gender-based-violence/regulatory-and-legal-framework/legal-definitions-in-the-eu/czech-republic-stalking?language_content_entity=en)

<sup>92</sup> EIGE, Combating Cyber Violence against Women and Girls, 2022, P. 28; EIGE, Combating Cyber Violence against Women and Girls, 2022, Annex 5. Legal notes to Chapter 3, xxxiii.

## ***Cyberviolence based on gender***

As noted above, not all countries consider the gender component during cyberviolence, which complicates data collection and analysis. Romania stands out in this regard. Romania recently recognized cyberviolence as a form of domestic violence under a new legislative amendment. Domestic violence now includes a provision specifically for “cyberviolence,” which aims to “humiliate, intimidate, silence, or threaten the victim”<sup>93</sup>. This includes online threats or messages, or when a partner shares intimate graphic content without the consent of the person depicted. The law also covers illegal access to communications and personal data through computers, smartphones, or devices that can connect to the internet<sup>94</sup>.

On August 3, 2018, France passed a law that also covers cyber-harassment (Article 222-33-2 of the French Criminal Code, on moral harassment). Cyber-harassment is defined as repeated comments, insults or threats made online (on a social network, in a forum, in a multiplayer video game, on a blog, etc.), with the aim of worsening the victim’s living conditions or with the result that could lead to a deterioration of the victim’s condition, physical or mental health. Victims of cyber harassment can request the removal of the content (comments, videos, images, messages, etc.) from their author or from the electronic network. Cyber harassment is punishable by a fine or imprisonment. It is an aggravating circumstance if the victim is under 15 years of age<sup>95</sup>.

## ***Image-based sexual violence***

The European Parliament calls on the Member States to update their national laws and include “image-based sexual violence” in the list of sexual crimes<sup>96</sup>.

---

<sup>93</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 103; Romania criminalises cyber harassment as a form of domestic violence, <<https://www.euronews.com/my-europe/2020/07/09/romania-criminalises-cyber-harassment-as-a-form-of-domestic-violence>>

<sup>94</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 103; Romania criminalises cyber harassment as a form of domestic violence, <<https://www.euronews.com/my-europe/2020/07/09/romania-criminalises-cyber-harassment-as-a-form-of-domestic-violence>>

<sup>95</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 103.

<sup>96</sup> European Parliament resolution of 14 December 2021 with recommendations to the Commission on combating gender-based violence: cyberviolence (n 6) Recital 17.

**Belgium** has a specific provision in its Criminal Code on online non-consensual pornography or image-based sexual violence (“voyeurism-revenge porn”). Article 371/1 sets a prison sentence of between six months and five years for anyone who makes available, without consent, visual images or audio recordings of a naked person or a person engaged in explicit sexual activity, even if that person consents to the recording. The same punishment applies to anyone who stalks or records a person naked or engaged in explicit sexual activity, even if it is not spread. Therefore, in Belgium, the spreading of content is not a prerequisite for punishment. The punishment increases if the victim is a minor<sup>97</sup>.

In the **Czech Republic**, the Criminal Code defines “non-consensual pornography” as any act committed using the Internet without the victim’s knowledge, including the posting of erotic photos along with erotic advertisements and contact details, resulting in the victim being insulted or harassed. Cyberstalking and cyber-harassment are also recognized and defined in the Czech Criminal Code<sup>98</sup>.

The **Spanish** Criminal Code provides for punishments for image-based sexual violence or non-consensual pornography. It punishes the distribution and sharing of images or audiovisual recordings obtained by a third party in the private space of a person, without the person’s consent. The sanction may be aggravated if the perpetrator is or was the intimate partner of the victim. Although Spain protects victims of domestic violence, it does not apply a gender perspective<sup>99</sup>.

**France** passed the Digital Republic Law in 2016, which punishes those found guilty of image-based sexual violence or non-consensual pornography with up to two years in prison and a fine of up to €60,000. It is noteworthy that all Member States criminalize image-based sexual violence if the victim is a child, as it is considered child pornography.

---

<sup>97</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 103.

<sup>98</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 104; Cyber violence and hate speech against women. European Parliament, Van der Wilk, A., 2018.

<sup>99</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 104.

**Romania** has adopted this approach. A new criminal law has been enacted against certain forms of image-based sexual violence, as a form of sexual violence, as part of the transposition of the Istanbul Convention<sup>100</sup>.

**Swedish** law covers many forms of image-based sexual violence, both as acts of “intrusive photography” and invasion of privacy, as well as part of the “freedom” and “peace” laws<sup>101</sup>.

## ***Blackmail by using intimate photos***

Article 197 of the Spanish Criminal Code considers it a crime if a natural person, without the consent of the person concerned, distributes or gives to third parties images or audiovisual recordings of the person concerned, taken with the person’s consent, in the person’s home or in any other place. The liability is aggravated if the act is committed by a person’s spouse or intimate partner<sup>102</sup>.

Maltese law punishes anyone who, with the intent to cause emotional harm, spreads a photo or video of sexual content without consent<sup>103</sup>.

Certain articles of the Belgian Criminal Code punish some forms of sexual violence, which are classified as crimes against sexual integrity, sexual self-exploration and public morality<sup>104</sup>.

Under French law, it is punishable to intentionally violate the private life and intimate relationships of other persons by any means, including:

**a)** listening to, recording or communicating words spoken in confidential or private circumstances without the person’s consent;

---

<sup>100</sup> GREVIO, ‘Baseline Evaluation Report on Legislative and Other Measures Giving Effect to the Provisions of the Council of Europe Convention on Preventing and Combating Violence against Women and Domestic Violence (Istanbul Convention) Romania’, 2022, 12, □□□□□□□□: < <https://rm.coe.int/final-report-on-romania/1680a6e439> >.

<sup>101</sup> Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission’s proposal to criminalise image-based sexual abuse, Carlotta Rigotti and Clare McGlynn, 2022, 462; Chapter 4, section 6a (intrusive photography) and Chapter 4, Section 6c (unlawful breach of privacy), Chapter 4 section 7 on molestation and Chapter 6 Section 10 on sexual molestation.

<sup>102</sup> Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, Última actualización publicada el 28/04/2023, Artículo 197, <https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444>

<sup>103</sup> EIGE, Combating Cyber Violence against Women and Girls, 2022, P. 28.

<sup>104</sup> Legal Provisions, Belgium, Article 371/1, [https://resourcehub.bakermckenzie.com/en/resources/fighting-domestic-violence/europe/belgium/topics/1legal-provisions#:~:text=Voyeurism%20\(Article%20371%2F1%20of,%2C%20making%20accessible%20or%20broadcastin%20g\).](https://resourcehub.bakermckenzie.com/en/resources/fighting-domestic-violence/europe/belgium/topics/1legal-provisions#:~:text=Voyeurism%20(Article%20371%2F1%20of,%2C%20making%20accessible%20or%20broadcastin%20g).)

b) Taking, recording or giving a private photo of a person without their consent<sup>105</sup>.

According to the Swedish law, a person is punished who illegally, using technical means, secretly records an image of a person who is in a house, bathroom, dressing room or other similar space<sup>106</sup>.

Under Polish law, recording a nude image without consent is punishable<sup>107</sup>, while under German law, photographing intimate parts of the body is punishable<sup>108</sup>.

## Cyberbullying

Italy has a specific legislation on cyberbullying, but it only protects minors. The law, 71/2017 entitled “Regulation for the safeguarding of minors and the prevention and tackling of cyberbullying”, defines cyberbullying as “whatever form of psychological pressure, aggression, harassment, blackmail, injury, insult, denigration, defamation, identity theft, alteration, illicit acquisition, manipulation, unlawful processing of personal data of minors and/or dissemination made through electronic means, including the distribution of online content depicting also one or more components of the minor’s family whose intentional and predominant purpose is to isolate a minor or a group of minors by putting into effect a serious abuse, a malicious attack or a widespread and organized ridicule.”<sup>109</sup>

In the case of other types of cyberbullying or crimes against adult victims, some provisions of the Italian Criminal Code may also apply to the online space, although, unlike stalking, it is not specifically mentioned (article / paragraph 612-bis)<sup>110</sup>.

---

<sup>105</sup> French Penal Code, Article 226-1, Section 6a, [https://www.equalrightstrust.org/ertdocumentbank/french\\_penal\\_code\\_33.pdf](https://www.equalrightstrust.org/ertdocumentbank/french_penal_code_33.pdf)

<sup>106</sup> Swedish Criminal Code, Chapter 4, <https://www.government.se/contentassets/7a2dcae0787e465e9a-2431554b5eab03/the-swedish-criminal-code.pdf>

<sup>107</sup> Polish Criminal Code, Article 191a, <https://supertrans2014.files.wordpress.com/2014/06/the-criminal-code.pdf>

<sup>108</sup> German Criminal Code, Section 201a, [https://www.gesetze-im-internet.de/englisch\\_stgb/englisch\\_stgb.html#p1935](https://www.gesetze-im-internet.de/englisch_stgb/englisch_stgb.html#p1935)

<sup>109</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 104.

<sup>110</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 104; < <https://www.coe.int/en/web/cyberviolence/italy#:~:text=Article%20%20of%20the%20law,illicit%20acquisition%2C%20manipulation%2C%20unlawful%20processing> >.

In addition, there is the 2019 Law on Gender-based Violence. Article 10 refers to the illegal dissemination of images or videos of sexual nature and establishes a framework for punishment: whoever publishes this content without the consent of the persons represented therein faces a prison sentence of one to six years and a fine of between 5,000 and 15,000 euros. This penalty also applies to secondary actors<sup>111</sup>.

## **Cyber-grooming**

According to the legislation of Romania, child pornography is punishable, particularly:

- a) production, publication or distribution, purchase, storage, screening – popularization or provision of public access to child pornography by any means<sup>112</sup>;
- b) liability is aggravated if the above-mentioned action is committed using a computer system or other means of data storage<sup>113</sup>.

Regulation for the safeguarding of minors and the prevention and tackling of cyberbullying” whatever form of psychological pressure, aggression, harassment, blackmail, injury, insult, denigration, defamation, identity theft, alteration, illicit acquisition, manipulation, unlawful processing of personal data of minors and/or dissemination made through electronic means, including the distribution of online content depicting also one or more components of the minor’s family whose intentional and predominant purpose is to isolate a minor or a group of minors by putting into effect a serious abuse, a malicious attack or a widespread and organized ridicule.”

An attempt to commit the above-mentioned action is also punishable<sup>114</sup>.

The law also defines what constitutes child pornography. Specifically, child pornography means any material showing a minor engaging in sexually explicit behavior or which, even with the participation of an unreal person, convincingly simulates the behavior of a minor<sup>115</sup>.

---

<sup>111</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 104.

<sup>112</sup> Romania, Sexual Offences Against Children, Criminal Code, Article 374(1), <https://www.icmec.org/wp-content/uploads/2018/08/ICMEC-Romania-National-Legislation.pdf>

<sup>113</sup> Ibid, Article 374(2).

<sup>114</sup> Ibid, Article 374(5).

<sup>115</sup> Ibid, Article 374(4).

According to Article 337(3) of the Greek Criminal Code, any adult who communicates with a person under the age of 15 using the Internet or any other means of communication using obscene gestures or proposals is punishable<sup>116</sup>.

Article 183 of the Spanish Criminal Code punishes contact with a minor under the age of 16 using the Internet, telephone or any other information and communication technology, with the aim of deceiving that person by sending them pornographic material or showing them pornographic images of minors<sup>117</sup>.

The Slovenian Criminal Code establishes liability for the manipulation of persons under the age of 15 for sexual purposes<sup>118</sup>.

According to Article 377 of the Belgian Criminal Code, an adult who, through information and communication technologies, offers a meeting to a minor under the age of 16, with the aim of committing an offence referred to in Chapters VI and VII of the same Code, is punishable<sup>119</sup>.

According to the Bulgarian Criminal Code, a person, using information or communication technologies or other means, gives or collects information about a person under the age of 18 in order to establish contact for the purpose of sexual intercourse, prostitution, or the creation of pornographic material, is punishable by imprisonment for a term of one to six years and a fine of five thousand to ten thousand Lev<sup>120</sup>.

The French Law punishes an adult who makes sexual proposals to a minor under the age of 15 or to a person who presents themselves as such, through electronic means of communication, such as the Internet<sup>121</sup>.

---

<sup>116</sup> Greek Cybercrime Center: Grooming, <https://www.cybercc.gr/en/legislation/grooming/>

<sup>117</sup> Ley Orgánica 10/1995, de 23 de noviembre, del Código Penal, Última actualización publicada el 28/04/2023, Artículo 183, <https://www.boe.es/buscar/act.php?id=BOE-A-1995-25444>

<sup>118</sup> EIGE, Combating Cyber Violence against Women and Girls, 2022, P. 28; EIGE, Combating Cyber Violence against Women and Girls, 2022, Annex 5. Legal notes to Chapter 3, xxxi.

<sup>119</sup> EIGE, Combating Cyber Violence against Women and Girls, 2022, P. 28; EIGE, Combating Cyber Violence against Women and Girls, 2022, Annex 5. Legal notes to Chapter 3, xx.

<sup>120</sup> EIGE, Combating Cyber Violence against Women and Girls, 2022, P. 28; EIGE, Combating Cyber Violence against Women and Girls, 2022, Annex 5. Legal notes to Chapter 3, xxi.

<sup>121</sup> EIGE, Combating Cyber Violence against Women and Girls, 2022, P. 28; EIGE, Combating Cyber Violence against Women and Girls, 2022, Annex 5. Legal notes to Chapter 3, xxv.

**Latvian** law prohibits the solicitation of minors to engage in sexual acts. In particular, it is a crime for an adult to ask a minor under the age of 16 to engage in sexual acts, or to meet with a minor for the purpose of engaging in a sexual act or initiating a sexual relationship, using information or communication technologies or other means of communication<sup>122</sup>.

Under **Luxembourg** law, it is a punishable act when an adult sends a sexual proposal to a minor under 16 years of age or a person who presents themselves as such, using an electronic means of communication<sup>123</sup>.

## **Cyber harassment**

According to Article 208 of the Romanian Criminal Code, it is punishable to make telephone calls or communicate in any other way using remote communication devices that, due to the frequency and content, causes fear<sup>124</sup>.

**Austrian** law punishes an act of a person, who, using telecommunications or computer system in a way that could cause unreasonable impact on a person's life for a long period of time,

1. Insults the dignity of a person in a manner that is perceptible to a large number of people, or
2. Makes facts or photographs about the most private areas of a person's life, without their consent, perceptible to a large number of people<sup>125</sup>.

According to **Slovak** law, it is a punishable act when a person intentionally humiliates another person through electronic means of communication, a computer system or a computer network:

**a)** By acting on the person's behalf without right, with the aim of long-term hatred, intimidation or other similar long-term harassment;

**b)** by publishing without right a personal video, audio or video-audio recording of a person, obtained with their consent or by providing access to it to another person, which may endanger the person's reputation or cause other serious harm<sup>126</sup>.

---

<sup>122</sup> EIGE, Combating Cyber Violence against Women and Girls, 2022, P. 28; EIGE, Combating Cyber Violence against Women and Girls, 2022, Annex 5. Legal notes to Chapter 3, xxvi.

<sup>123</sup> EIGE, Combating Cyber Violence against Women and Girls, 2022, P. 28; EIGE, Combating Cyber Violence against Women and Girls, 2022, Annex 5. Legal notes to Chapter 3, xxviii.

<sup>124</sup> EIGE, Combating Cyber Violence against Women and Girls, 2022, P. 27; EIGE, Combating Cyber Violence against Women and Girls, 2022, Annex 5. Legal notes to Chapter 3, iv.

<sup>125</sup> Austria: Criminalising cyber harassment: <https://www.coe.int/en/web/cyberviolence/-/austria-criminalising-cyberharassment>

<sup>126</sup> EIGE, Combating Cyber Violence against Women and Girls, 2022, Annex 5. Legal notes to Chapter 3, viii.

Austria criminalizes “continuous harassment related to a telecommunications or computer system” (§107c, Criminal Code). A person can be sentenced to up to one year in prison if they “use a telecommunications or computer system in such a way as to cause unjustified interference with the way of life of another person, over a continuous period of time: (1) insult another person in front of a large number of people, or (2) share details of another person’s private sphere or visual material with a large number of people without their consent.” If the crime leads to the victim’s suicide or attempted suicide, the sentence can be increased to up to three years in prison<sup>127</sup>.

## ***Online hate speech***

Hate speech is not punishable in all countries, but in several Member States - Spain, the Netherlands, Bulgaria, Greece, Croatia, Portugal and Malta - online hate speech is clearly punishable. However, hate speech does not always extend to sex or gender<sup>128</sup>. Some Member States, in order to regulate this, refer to other provisions in the Criminal Code to criminalize the act. The following countries take into account the gender aspect when regulating hate speech: Estonia, Spain, Latvia, Lithuania, Hungary, Malta, Austria, Portugal<sup>129</sup>.

Germany uses many legal provisions to address this issue, that are not specific to cyberviolence, legal provisions in the Criminal Code on stalking, harassment, threats or insults that can occur in an online space. In addition to criminal law, relevant provisions and rules can be found in civil law, such as compensation and deletion. This is also covered by labor law (warning notice and administrative law, including police law and regulations for service providers)<sup>130</sup>.

The provisions about harassment or stalking in the Spanish Criminal Code can be applied to the online world, as it punishes all forms of harassment or stalking<sup>131</sup>.

---

<sup>127</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 104.

<sup>128</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 104.

<sup>129</sup> Combating Cyber Violence against Women and Girls, EIGE, 2022, view:

[https://eige.europa.eu/sites/default/files/documents/combating\\_cyber\\_violence\\_against\\_women\\_and\\_girls.pdf](https://eige.europa.eu/sites/default/files/documents/combating_cyber_violence_against_women_and_girls.pdf)

<sup>130</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 105.

<sup>131</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 105.

According to the legislation of Cyprus, the intentional dissemination of sexist information via the Internet is punishable<sup>132</sup>.

## ***Other non-criminal provisions***

In 2017, Germany passed a law to improve law enforcement on social network, requiring social networks with more than 2 million registered users to ensure effective complaint management and to remove or block content that is illegal under certain provisions of the German Criminal Code, including Section 201a of the Code, which deals with the violation of intimate confidentiality. Another law worth mentioning is the civil law on the prevention of acts of violence and stalking (“Gewaltschutzgesetz”), which allows the court to take necessary measures to prevent further misconduct<sup>133</sup>.

In Lithuania, NGOs actively assist victims of gender-based violence. These centers support victims of violence, inform victims about the types and places of assistance, can receive and represent them in other institutions, provide psychological and legal assistance, and help restore interpersonal relationships with family members<sup>134</sup>. Through these centers, victims of gender-based cyberviolence can receive assistance. Lithuania has also implemented the European Commission’s Safer Internet Plus Programme, established the Safer Internet Consortium, which consists of four partners: two government bodies, an NGO and an association. In addition, Lithuania published a new media self-regulation Code in 2016, which prohibits the mockery of a person based gender, along with other forms of identity, and the publication of the surname of a victim of sexual assault<sup>135</sup>. In the legislation, Article 23 of the Law on Education creates a structure through which citizens can report cyberbullying on the website of the Communications Regulatory Authority<sup>136</sup>.

---

<sup>132</sup> EIGE, Combating Cyber Violence against Women and Girls, 2022, P. 27; EIGE, Combating Cyber Violence against Women and Girls, 2022, Annex 5. Legal notes to Chapter 3, xiii.

<sup>133</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 105.

<sup>134</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 105.

<sup>135</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 105; Republic of Lithuania national-level review on the Implementation of the Beijing Declaration and Platform for Action (1995), For the Period from 2014 to 2019 < [https://unece.org/fileadmin/DAM/RCM\\_Website/Lithuania.pdf](https://unece.org/fileadmin/DAM/RCM_Website/Lithuania.pdf) >

<sup>136</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 105; Lietuvos Respublikos švietimo įstatymas < <https://www.e-tar.lt/portal/lt/legalAct/TAR.9A3AD08EA5D0/rjabACXQY> >

In the Netherlands, there is an important initiative in place for gender-based cyber violence. The Expertise centrum online omsluit kinderen (Expertise Centre for Online Sexual violence against Children - INHOPE - local branch of the hotline) operates a hotline as well as a website with information and related chat or other contact methods called “Help”. This website is mainly aimed at combating sextortion and the publication of unwanted fake porn<sup>137</sup>.

Gender equality issues are a priority for the government in Sweden. The country has specifically recognized cyber-harassment as an equality issue that needs to be addressed. “Gender-based cyber-harassment takes many forms. It often involves sharing sexually explicit photos of girls and making derogatory comments about their sexual habits. For women, this often involves making offensive comments or insulting remarks, online and via text messages, phone calls or face-to-face meetings”.<sup>138</sup>

## ***Subjective composition of cyber violence***

As for the mental elements, in EU Member States, criminal law provisions require proof of the perpetrator’s intent, although, for example, Ireland extends this to negligence in specific cases. Other elements of intent are essentially different. For example, the main difference is between provisions focusing on lack of consent and provisions requiring additional proof regarding the perpetrator’s motives. Maltese law, for example, requires proof in all cases that the perpetrator intended to harm the victim<sup>139</sup>. Irish law provides for an offence that focuses on the lack of consent and requires only proof of the intentional recording or dissemination of an intimate image. However, it must also be proven that such acts have either caused or are likely to seriously disrupt the peace and privacy of the victim<sup>140</sup>.

---

<sup>137</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 105; < <https://www.coe.int/en/web/cybercrime/-/netherlands-centre-for-expertise-on-online-child-sexual-abuse> > (□□□□□ □□ □□□□□□□□)

<sup>138</sup> Combating gender-based violence: Cyber violence, N. Lomba, C. Navarra and M. Fernandes, European Parliamentary Research Service, 2021, 105; < <https://www.government.se/opinion-pieces/2016/04/challenging-cyber-harassment-for-women-and-girls-worldwide/> > (□□□□□ □□ □□□□□□□□)

<sup>139</sup> Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission’s proposal to criminalise image-based sexual abuse, Carlotta Rigotti and Clare McGlynn, 2022, 466; Section 208E of the Maltese Criminal Code, as discussed in Sara De Vido and Lorena Sosa.

<sup>140</sup> Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission’s proposal to criminalise image-based sexual abuse, Carlotta Rigotti and Clare McGlynn, 2022, 466.

According to Chapter 4 of Section 6c, of the Swedish Criminal Code, a violation of privacy depends on the serious harm caused to the person. Similarly, Article 197, Section 7 of the Spanish Criminal Code requires disclosure in order for the right to privacy to be considered violated<sup>141</sup>.

There are also other differences among the laws of countries. For example, Italian law does not require intent to cause harm when photos are stolen or taken without consent, but if obtained with consent, their distribution requires intent to cause harm<sup>142</sup>. In other countries, intent to cause harm is an aggravating circumstance in relation to the sentence (for example, Article 160b(3) of the Criminal Code), or an element of a more serious crime (for example, Article 417/10 of the Belgian Criminal Code and the Irish “Harassment, Harmful Communications and Related Offences Act”, 2020)<sup>143</sup>.

## Experience of other countries

### Albania

Albanian law does not directly regulate online gender-based violence, but Article 108/a of the Criminal Code states that the commission of sexual acts that violate the dignity of a person, by any means or form, or create a hostile, degrading or offensive environment, is considered a criminal offense and is punishable by imprisonment for a term of one to five years<sup>144</sup>. Gender constitutes an aggravating circumstance (Article 50, paragraph “J”, of the Criminal Code of Albania, 1995/revised)<sup>145</sup>.

---

<sup>141</sup> Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission’s proposal to criminalise image-based sexual abuse, Carlotta Rigotti and Clare McGlynn, 2022, 466.

<sup>142</sup> Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission’s proposal to criminalise image-based sexual abuse, Carlotta Rigotti and Clare McGlynn, 2022, 466.

<sup>143</sup> Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission’s proposal to criminalise image-based sexual abuse, Carlotta Rigotti and Clare McGlynn, 2022, 466.

<sup>144</sup> Cyber Violence against Women and Girls in the Western Balkans: Selected Case Studies and a Cybersecurity Governance Approach, E. Dorokhova, H. vale, V. Laçi, A. Mahmutovic, Geneva Centre for Security Sector Governance, 2021, 18; Kodi Penal I Republikës Së Shqipërisë, Added Article 108/a with Law No. 144, dated 2.5.2013, Article 24, 2016, <[www.pp.gov.al/web/kodi\\_penal\\_2016\\_1033.pdf](http://www.pp.gov.al/web/kodi_penal_2016_1033.pdf)>

<sup>145</sup> Cyber Violence against Women and Girls in the Western Balkans: Selected Case Studies and a Cybersecurity Governance Approach, E. Dorokhova, H. vale, V. Laçi, A. Mahmutovic, Geneva Centre for Security Sector Governance, 2021, 18.

Also, recent amendments to the Law on Protection from Discrimination have added sexual harassment as a form of discrimination<sup>146</sup>. This law defines sexual harassment as unwanted verbal or non-verbal conduct of a sexual nature that has the purpose or effect of violating the dignity of a person, creates an intimidating, hostile, degrading, humiliating or offensive environment<sup>147</sup>.

## Mexico

Mexico is one of the countries in Latin America and the Caribbean that has implemented the most legislative reforms against gender-based online violence since 2021, such as placing image-based sexual violence under the existing laws on violence against women. The Olympia Law (named after the 2011 victim of image-based violence, Olympia Coral Melo) was important in recognizing the gravity of online violence at the national level, leading to the reform of the Criminal Code to include new forms of crime and laying the foundation for the coordination and implementation of the prevention, response and eradication of online violence in Mexico. To date, this has resulted in 35 legal reforms in 28 local legislative amendments. This includes criminalizing extortion, threats, cyber-harassment, sexual harassment, and sharing non-consensual images<sup>148</sup>.

## Korea

The Digital Sex Crime Victim Support Center in Korea offers comprehensive support and protection to people who have been victims of digital sex crimes. This includes counseling, legal assistance, and medical care. It also provides services such as digital content deletion and investigative cooperation with foreign IT companies. Efforts are also focused on technological solutions such as preventive deletion support, which detects digital violence before it becomes public<sup>149</sup>.

---

<sup>146</sup> Cyber Violence against Women and Girls in the Western Balkans: Selected Case Studies and a Cyber-security Governance Approach, E. Dorokhova, H. vale, V. Laçi, A. Mahmutovic, Geneva Centre for Security Sector Governance, 2021, 18; Albanian Parliament, official website, Ligjnr. 124/2020 Për Disa Shtesa Dhe Ndryshime Në Ligjin Nr. 10221, Datë 4.2.2010 “Për Mbrojtjen Nga Diskriminimi” (additions and amendments in the Law on Protection from Discrimination No. 10221, dated 4.2.2010 ), 2020.

<sup>147</sup> Cyber Violence against Women and Girls in the Western Balkans: Selected Case Studies and a Cyber-security Governance Approach, E. Dorokhova, H. vale, V. Laçi, A. Mahmutovic, Geneva Centre for Security Sector Governance, 2021, 18.

<sup>148</sup> Accelerating Efforts to Tackle Online and Technology Facilitated Violence Against Women and Girls (VAWG), UN women, 8; OEA/ONU Mujeres 2022 Informe | Ciberviolencia y Ciberacoso contra las mujeres y niñas en el marco de la Convención Belém Do Pará.

<sup>149</sup> Accelerating Efforts to Tackle Online and Technology Facilitated Violence Against Women and Girls (VAWG), UN women, 9.

## England, Wales, Scotland, Northern Ireland

Since 2015, it has been a criminal offence in England and Wales to share private, sexually explicit images without consent, but only if it can be proven that the perpetrator did so with the intention of harming the victim. This legislation does not cover:

- Sharing a photo for sexual gratification, financial gain, or “fun”;
- Threats;
- Fake images, such as “deep-fakes,” fake porn<sup>150</sup>.

There is a better law in Scotland - it includes threats, altered images, fake porn, and allows for convictions even when the offender acted recklessly. As for Northern Ireland, it largely follows English and Welsh laws<sup>151</sup>.

Under criminal law, it is a crime in England and Wales to surveil or film a person engaged in sexual activity or in a private setting, but only if the offender does so for the purpose of sexual gratification. For example, taking a picture of someone in a changing room of a gym without their consent is only an offence if it is done for the purpose of sexual gratification<sup>152</sup>.

It is also a criminal offence in England and Wales to “up-skirt” (lift up a woman’s dress), but only if the person does it for sexual gratification or to cause distress. If an image taken while “up-skirting” is shared, for example on a pornographic website, it is only a crime if it is done with the intent of causing distress to the victim<sup>153</sup>.

The law does not apply to photos sent to friends, for financial gain, or for “mockery”<sup>154</sup>. Similarly, the law in Scotland is limited to certain motives, while the law in Northern Ireland does not cover “up-skirting”<sup>155</sup>.

---

<sup>150</sup> Shattering Lives and Myths: A Report on Image-Based Sexual Abuse. Australian Research Council (ARC), McGlynn, C. et al, 2019, 12.

<sup>151</sup> Shattering Lives and Myths: A Report on Image-Based Sexual Abuse. Australian Research Council (ARC), McGlynn, C. et al, 2019, 12.

<sup>152</sup> Ibid.

<sup>153</sup> Ibid.

<sup>154</sup> Ibid.

<sup>155</sup> Ibid.

The UK's "Revenge Porn Helpline" (Rape Porn Help, RPH) was established in 2015 and helps individuals avoid becoming victims of non-consensual intimate image-based abuse. Since its inception, RPH has helped thousands of victims, with a removal rate of over 90% of criminal material from the internet. It has successfully removed over 200,000 individual non-consensual intimate images from the internet. Recently, RPH partnered with Meta to launch StopNCII.org – a free tool that uses innovative technology to support victims and potential victims of non-consensual intimate image abuse by creating a digital fingerprint of the image, which can then be proactively identified and removed to prevent specific images from being shared<sup>156</sup>.

## ***Experience of Arab countries***

Several Arab countries have amended their criminal codes to cover online sexual violence under the laws on sexual harassment and domestic violence. Tunisian Law 58 of 2017 addresses "physical, moral, sexual or economic harm to women, whether in the private or public space"; Article 33 of Tunisian Law No. 58 of 2017 also allows victims of online violence to seek restraining orders against perpetrators, but only if there is physical harm<sup>157</sup>.

Egypt, Lebanon, Saudi Arabia and Morocco have also made similar changes. Legal texts in Egypt, Lebanon and Saudi Arabia specifically punish online violence and harassment that occurs through social media platforms and modern technologies. The Moroccan Criminal Code addresses various forms of online violence, including the acquisition, creation, distribution of written messages, recordings and images of a sexual nature for sexual purposes, received by telephone or other electronic device, the distribution of messages and photographs of a person without prior consent, and the spreading of false accusations aimed at harming a person's privacy or defaming them, by any means, including digital tools<sup>158</sup>.

Countries such as Jordan, Morocco and Tunisia have also established specialized agencies to combat online violence, while fifteen out of twenty-two Arab countries have introduced helplines for victims of online violence, and some countries have introduced online portals, forms or emails for reporting such incidents<sup>159</sup>.

---

<sup>156</sup> Accelerating Efforts to Tackle Online and Technology Facilitated Violence Against Women and Girls (VAWG), UN women, 9; < <https://stopncii.org/> >

<sup>157</sup> Violence against women in the online space, Insights from a multi-country study in the Arab States, Summary report, UN women, 6-8; EuroMed Rights (Rep.), Lannazzone, S., Clough, L., & Griffon, L. 2021, <<https://euromedrights.org/wp-content/uploads/2021/06/Online-gender-violence-in-MENA-region.pdf> >

<sup>158</sup> Ibid.

<sup>159</sup> Ibid.

## In search of a solution

To effectively combat various forms of cyberviolence, states must implement comprehensive legal reforms. Firstly, image-based sexual violence should be recognized as a sexual crime. The criminal code must prohibit all forms of image-based sexual violence, including “deep-fakes” and fake porn.

It is important that when determining laws regulating cyber violence, the motivation of the perpetrator must not be decisive, as it is in the case of other sexual and criminal offenses<sup>160</sup>. It is important that these crimes have appropriate punishments that will have a deterrent effect. Currently, the average maximum punishment for non-consensual distribution of intimate images is usually one to two years of imprisonment (Germany, Portugal), while in some countries it can be up to 5-7 years (Belgium, Italy, Ireland). In some cases, imprisonment can be replaced by a fine (Netherlands, Spain). However, in some cases, a fine is or may be a mandatory part of the sentence (in France, for non-consensual distribution of sexual images, the offender is fined up to 60,000 euros, while in Italy the range is from 5,000 to 15,000 euros). This diversity of sanctions reflects the differences in national approaches to punishment and deprivation of liberty, which are identified across all criminal offenses<sup>161</sup>.

For effective investigation of cyber violence, it is necessary to strengthen cooperation between countries and with the online platforms that are used to commit these crimes. Currently, some social networks and applications cooperate with law enforcement agencies and themselves adhere to internal rules, however, this does not apply to all companies. This cooperation is also hampered by the existence of different regulations in different countries. Therefore, it is necessary to introduce common standards and approaches, which should be implemented primarily through the activity of international organizations, within the frames of the international conventions and instruments that were reviewed in this paper.

---

<sup>160</sup> Shattering Lives and Myths: A Report on Image-Based Sexual Abuse. Australian Research Council (ARC), McGlynn, C. et al, 2019, 1.

It is particularly important for states to prevent cyber violence and implement appropriate policies. Cybersecurity and cyberviolence issues should be taught in schools, and police and other professionals who come into contact with victims of cyberviolence should be trained.

It is important to have support programs for victims of sexual violence, both in the government and non- government sectors. These services should be based on international best practices, such as the Australian Office of the eSafety Commissioner, New Zealand's Netsafe, and South Korea's Advocacy Center for Victims of Online Sexual Violence<sup>162</sup>.

---

<sup>161</sup> Towards an EU criminal law on violence against women: The ambitions and limitations of the Commission's proposal to criminalise image-based sexual abuse, Carlotta Rigotti and Clare McGlynn, 2022, 467.

<sup>162</sup> Shattering Lives and Myths: A Report on Image-Based Sexual Abuse. Australian Research Council (ARC), McGlynn, C. et al, 2019, 16.