



The cyber and technological dimensions of domestic violence against women in Bulgaria

20 recommendations in an
ecosystem perspective



COUNTER
INTUITIVE
INSTITUTE



BULGARIAN
FUND FOR
WOMEN



Co-funded by
the European Union

The cyber and technological dimension of domestic violence (CTDDV) is emerging as **a structural problem** in the Member States of the European Union (EU) and constitutes a violation of fundamental rights, such as the right to human dignity, the right to life and personal integrity, the right to data protection, and the right to non-discrimination, including on the grounds of gender. In Bulgaria, the phenomenon is insufficiently documented: the existing legislative framework does not explicitly cover many of its forms, institutional capacity to respond is limited, and statistical data are scarce. Bulgaria has not ratified the Istanbul Convention, which makes **Directive (EU) 2024/1385** the main instrument for modernising the legal framework, with a transposition deadline of 14 June 2027.

This document presents key findings from the project ***“Invisible Data: Knowledge-based approaches for countering Cyber and Technology Facilitated Gender-based violence against women”***, which analyses gaps in current legislation and proposes twenty specific recommendations for the government, institutions, the media, the private sector and civil society organisations (NGOs).

The Counterintuitive Institute
April 2026
Sofia

**Invisible
DataBase**



With the financial support of the Bulgarian Fund for Women and the European Union. The views and opinions expressed, however, are solely those of the author(s) only and do not necessarily reflect the views of the Bulgarian Fund for Women, the European Union or the European Commission Directorate-General for Justice and Consumers. Neither the Bulgarian Fund for Women, the European Union, the European Commission, nor any of their respective structures or entities can be held responsible for these actions or outcomes.



The concept of **cyber and technology-facilitated violence** (CTFV) encompasses a wide range of behaviours that encompass the use of technology and online spaces as tools to exert control, intimidate, humiliate or harm women and girls. Directive (EU) 2024/1385 explicitly regulates: the non-consensual sharing of intimate or manipulated material (Article 5), cyberstalking (Article 6), cyberbullying (Article 7), and incitement to violence or hatred in cyberspace (Article 8). More specifically, the phenomenon includes doxxing, deepfake sexual content, technology-mediated coercive control, online harassment and threats. The latest EU-wide study on gender-based violence confirms that **1 in 3 women in the EU has experienced violence in her lifetime**. At the same time, new research shows that digital technologies are increasingly being used **to harass, monitor and silence women** – particularly those who are already experiencing other forms of violence, as well as women who are active online or in public life (FRA & EIGE, 2026).



Research by The Counterintuitive Institute carried out between July 2025 and January 2026 shows that:

- **83%** of domestic violence cases have a cyber or technological aspect, with this type of violence being systemic in **64%** of cases.
- The most common forms of cyber and technological violence include:
 - Insults or threats in private online or telephone communications (**91%**)
 - Use of threats, humiliating, or offensive comments about the victim in private communications with other people online (**73%**)
 - The abuser demanding constant updates from the victim over the phone or online (**71%**)
 - Restricting the victim's online and telephone communication with strangers (**33%**)
 - Seizing the victim's passwords for internet platforms and websites (**29%**).
- The gender aspect of this type of violence is highly pronounced: 1) among perpetrators: **86%** are men, **14%** are women; 2) among victims: **91%** are women, **9%** are men. Male perpetrators and female victims are significantly overrepresented. A woman is more likely to be a perpetrator than a man is to be a victim.
- The average victim is slightly younger (**36** years old) than the average perpetrator (**40** years old).
- Violence perpetrated by men against women in intimate relationships is predominant. **95%** of violence in intimate relationships is perpetrated by men. **54%** of cyber and technological intimate partner violence occurs in the context of past relationships (former spouses or partners).
- **30%** of cases of cyber and technological domestic violence are directed at the victim's close friends, relatives and acquaintances (so-called violence 'by proxy').
- Victims experience lasting effects from cyber and technological violence, including:
 - Fear and a sense of helplessness (**82%**)
 - Depression, anxiety, or panic attacks (**77%**)
 - Sleep issues and/or difficulty concentrating (**73%**)
 - Difficulties in personal relationships (**64%**)
 - Problems at work or with career development (**37%**)
 - Financial problems (**30%**)
 - Problems with the law or trouble with the authorities (**13%**).

For more information on the methodology and results of the study, visit [Invisible DataBase](#).

EU legislative and regulatory practices to tackle cyber violence

- **Austria:** Adopted a National Action Plan to Combat Violence against Women and Girls (2025–2029) (Nationaler Aktionsplan zur Bekämpfung von Gewalt an Frauen und Mädchen 2025-2029), which includes around 350 measures developed by practitioners, academics, representatives of the administration and policymakers, and is aligned with the Istanbul Convention and Directive 2024/1385. The plan is based on the understanding that all women and girls – regardless of origin, age, disability, profession or lifestyle – have the right to self-determination and a life free from violence. The document also provides for coordinated action against online hate and cyber violence, including in the context of domestic violence.
- **Netherlands:** As of 1 July 2024, new legal provisions on sexual offences came into force, significantly expanding the protection of victims – for example, the requirement to prove physical coercion in cases of rape and sexual assault has been removed. Sexual harassment in public spaces, including on social media and online platforms, is explicitly criminalised, and the principle is established that sexual violence online and offline should be punished in the same way.
- **Ireland:** As of July 2025, the Online Safety Code introduces mandatory requirements for certain categories of online platforms, including video-sharing platforms and those hosting adult content or extreme violence. The measures include age verification mechanisms, restrictions on children's access to harmful content, risk management obligations and reporting to the regulator, with significant financial penalties for non-compliance.

20 recommendations in an ecosystem perspective

To the government and the legislature

Formal inclusion of cyber and technological violence as a priority in national strategies and programmes with designated responsible institutions, deadlines, and indicators.

Prioritising this issue as a policy matter is a critical step towards overcoming the persistent tendency for institutions to downplay the importance and impact of the cyber and technological dimensions of gender-based violence and domestic violence.

01

Timely (by June 2027) transposition of Directive (EU) 2024/1385 into Bulgarian law, ensuring consistency with the rest of the applicable European legal framework (e.g., data protection, digital services, artificial intelligence) and taking into account intersectional factors.

Particular attention should be paid to women who are public figures, journalists, or human rights defenders as vulnerable groups, especially in relation to various forms of cyber violence (Art. 11(n)). Accordingly, prevention and protection measures must take into account the specific risks associated with these women's public roles. When transposing Directive (EU) 2024/1385, as well as when drafting strategic documents and policies to prevent and combat cyber and technologically facilitated violence, the intersectional vulnerabilities of the affected groups should be taken into account. It is necessary to account for factors such as digital exclusion, ethnicity, gender identity, migrant status, disability, age, and socioeconomic status, which can increase the risk of violence and limit access to protection and justice.

02

Regular collection of official data on cases of cyber violence at the national and local levels.

A national “system for the collection, processing, compilation, and dissemination of statistical data on violence against women or domestic violence” (Art. 44(1)), must be set up. It should have a clearly designated leading agency, standardised indicators, and mechanisms for data exchange among institutions. The collected statistical data, which does not contain personal data, should be made available to the public in an easily accessible manner (Art. 44 (6)).

03

Criminalisation of all forms of cyber and technologically facilitated violence described in the Directive.

Conduct a comprehensive review of existing criminal legislation and, where necessary, introduce or adapt criminal offences to comply with the requirements of Directive (EU) 2024/1385, including with regard to the non-consensual sharing of intimate or manipulated material, cyberstalking, cyberbullying, and incitement to violence or hatred in cyberspace. The definitions should be sufficiently technology-neutral to address future forms of abuse and ensure effective protection for all victims, while taking into account the specific risks associated with gender-based violence.

04

Expanding the Protection Against Domestic Violence Act by including a technological component in the definition of domestic violence.

Explicit inclusion of cyber and technological violence, harassment, and coercive control in the definition of domestic violence in Article 2 of the Protection Against Domestic Violence Act. The various forms of cyber and technological violence should be considered as independent and sufficient grounds for issuing a protection order as provided in the Act. Clear rules are needed for the collection, evaluation, and admissibility of electronic evidence (e.g., screenshots, logs, metadata), as well as the possibility of immediate measures to restrict access to harmful content.

05



Promoting partnerships between the government, academia, and NGOs to analyse available data and develop evidence-driven policies.

Within the framework of an existing or new cooperation mechanism, the collection, analysis, and interpretation of data on domestic violence should be undertaken, supported, and promoted. It is desirable for the mechanism to include functional and thematic working groups, clear rules for sharing anonymised data, and regular expert meetings and consultations among government institutions, the academic community, and nongovernmental organisations. NGOs should be recognised as key partners, as they possess practical experience, direct access to victims, and valuable empirical information, and should be supported with sustainable and adequate funding to carry out work in this area.

06

To the institutions

Development and publication of an in-depth legal analysis of the Bulgarian regulatory framework and its compliance with the Directive.

An expert working group at the Ministry of Justice is expected to propose the necessary legislative changes for the full transposition of the Directive by 2026. The report prepared by the working group must be made publicly available to enhance transparency and public awareness on the subject.

07

Active participation in national and international initiatives and projects aimed at increasing engagement and the exchange of expertise.

Bulgarian state and municipal institutions should actively participate in European and national projects related to the prevention and combating of violence against women, as well as cyber and technological violence. This facilitates the exchange of best practices, capacity building, and the implementation of innovative technological solutions, often developed at the European level. Efforts must be made to overcome these institutions' reluctance to participate in such initiatives and projects.

08

Consistent, sustainable, and transparent operation of the National Council for the Prevention and Protection against Domestic Violence.

The sustainable operation of the National Council for the Prevention and Protection against Domestic Violence should be ensured through a clearly defined mandate, budget, public disclosure of its activities, and the participation of experts from state institutions and non-governmental organisations, as well as subject matter experts on cyber and technologically facilitated violence.

- It is recommended that a mechanism be established to consult with non-governmental organisations that receive state funding, in order to include stakeholders with significant expertise that work directly with victims.
- Minutes from the meetings of the National Council for the Prevention and Protection against Domestic Violence, as well as supporting materials (analyses, studies, statistics), should be published on the Council of Ministers' website.
- The National Council's mandate should explicitly mention cyber and technologically facilitated violence as a form of domestic violence.
- It is recommended that the National Council include a representative from civil society or the academic community with in-depth knowledge of gender-based cyber and technologically facilitated violence.

09

Sustained, active focus on prevention and raising public awareness of cyber and technologically facilitated violence.

The responsible institutions must place a strong emphasis on prevention, including "targeted awareness-raising campaigns or programs aimed at the general public from an early age." It is important that they also promote understanding of the various forms and root causes of violence against women and domestic violence (Article 34(2) of the Directive). Effective prevention is underpinned by educational measures starting at an early age, including initiatives that encourage men and boys to serve as positive role models in support of societal behavioural changes related to respect for personal integrity, gender equality, and mutual respect (Art. 34 (5)).

10

Building capacity among institutions involved in preventing and combating cyber and technologically facilitated violence.

There is a need for the systematic development of knowledge, skills, and coordination among the relevant authorities to ensure timely and adequate protection for victims, for example:

- Conducting specialised training for professionals in the police forces, the prosecution service, the judiciary, and local authorities on the forms, mechanisms, and evidence of cyber and technologically facilitated violence, including the prevention of secondary and repeat victimisation when working with and communicating with victims (Art. 21(f)). This is particularly important in cases of cyber violence, characterised by its scale (e.g., sharing videos of the victim on platforms, social media, or websites with pornographic content).
- Development of practical guidelines and standardised procedures for handling cases of cyber and technologically facilitated violence for all relevant institutions. These should outline the development of procedures for the collection, storage, and verification of electronic evidence in accordance with procedural requirements, as well as the explicit inclusion of CTFV in the risk assessment methods applied.
- Identifying specialised experts and building capacity within existing institutions, units, and directorates (e.g., operational units within the General Directorate of National Police with jurisdiction over cybercrime cases for the storage and analysis of electronic evidence, and specialised prosecutors for cyber violence in district prosecutor's offices, with priority given to areas with a higher caseload).
- Promoting inter-institutional cooperation and the exchange of best practices, including through joint training sessions and coordination mechanisms such as specialised training for practitioners working with victims and/or perpetrators, to help those experiencing domestic violence recognise its cyber and technological forms.
- Explicit recognition of the importance and prevalence of the economic dimension of CTFV, which includes restricting access to online banking and digital financial services, unauthorised use of personal data to take out loans or make purchases, control over electronic payments and accounts, and the use of technological means to sabotage victims' employment and career advancement opportunities.

Support for EU efforts to effectively moderate and report content related to cyber and technologically facilitated violence.

Bulgarian institutions should actively support and promote efforts at the European level to more effectively prevent, report, and remove content related to cyber and technologically facilitated violence by implementing the European regulatory framework and participating in common coordination mechanisms..

- Under the Digital Services Act, competent national authorities should apply and utilise the mechanisms provided for in the European regulatory framework (including cooperation with the national digital services coordinator) to ensure effective reporting and removal of content.
- National competent authorities should promote enhanced monitoring, transparency regarding the measures taken, assessment of systemic risks, and effective cooperation between platforms, government institutions, and the civil sector in order to better protect those affected.

12

To the media

Editorial Standards for reporting on cyber and technologically facilitated violence against women.

Given the growing prevalence of cyber violence against women, it is essential that the Bulgarian media take on an active and responsible role in both reporting on and preventing it. This requires the development and implementation of clear editorial standards to ensure ethical, balanced, and victim-sensitive media content, including the avoidance of sensationalism, victim-blaming, and the dissemination of harmful stereotypes. In this regard, it is appropriate to strengthen the role of the Council for Electronic Media and the Commission on Journalistic Ethics in developing and promoting guidelines and self-regulatory mechanisms for reporting cases of CTFV.

13

Media campaigns to raise public awareness.

The media should promote, implement, and participate in targeted campaigns to raise public awareness about the various forms of CTFV, the risks to victims, and the options for protection and support. Such campaigns can be carried out in partnership with government institutions, non-governmental organisations, and educational institutions (schools, universities, community centres). It is recommended to use modern, up-to-date, and diverse communication channels in order to reach different age and social groups.

14

Cooperation with online platforms and social media to identify CTFV and uphold standards for reporting on harmful content.

It is important to strengthen cooperation between the media and online platforms and social networks, including Meta Platforms, Google, and TikTok, to more effectively identify and remove harmful content. This cooperation may include the exchange of best practices, the development of common standards, and participation in self-regulatory initiatives consistent with the Bulgarian legal framework and the European requirements.

15

To the private sector

Prevention and counteraction of technologically facilitated financial violence.

Banks and non-bank financial institutions should develop internal policies and procedures to identify risk patterns, in accordance with regulatory requirements and customer rights (including suspicious patterns of account control, forced sharing of access, or abuse of digital banking).

- This can be achieved through employee training, the creation of specialised protocols for reporting and protecting victims, and the development of “secure” banking services (e.g., discreet communication channels and temporary access restrictions).
- These activities should comply with the requirements of the General Data Protection Regulation (GDPR), ensuring the protection of personal data and information security.

16



Safety-by-design AI to tackle technologically facilitated violence.

Companies developing and offering services using artificial intelligence (AI) and connected devices (IoT / smart devices) should integrate “safety-by-design” and “privacy-by-design” approaches, including through risk assessments, mechanisms for detecting abuse (sexual deepfakes, digital tracking, and control via technology) and transparency, in accordance with the applicable European regulatory framework.

- This includes implementing mechanisms to detect and limit manipulated content, safeguards against unauthorised access to devices, and clear user controls.
- Compliance with the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), and the EU AI Act should be combined with regular risk assessments and transparency regarding the functioning of algorithms and consumer protection measures.

17

To the civil society organisations

Comprehensive and well-informed legal and psychological support for victims.

Civil society organisations should provide coordinated and comprehensive support to victims of cyber and technologically facilitated violence, covering both legal and psychological aspects:

- Establishing multidisciplinary teams (lawyers, psychologists, social workers, and healthcare professionals).
- Providing free or affordable legal assistance, including in cases of online violence and harassment.
- Providing psychological support tailored to the specific needs of victims of cyber and technologically facilitated violence.
- Developing coordination mechanisms for referral to relevant institutions and services.

18

Digital safety: training for frontline practitioners.

Improving the digital literacy and skills of frontline professionals is essential for recognising and responding appropriately to cases of cyber and technologically facilitated violence. Training should be practical and tailored to the real-world challenges faced by victims:

- Organising regular training sessions on digital safety and cyber risks led by organisations with expertise in the field.
- Developing practical guidelines and tools for handling cases of cyber and technologically facilitated violence through cross-sectoral initiatives and collaboration.
- Training on protecting personal data, devices, and online profiles led by organisations with expertise in the field.
- Building risk assessment skills and directing individuals to appropriate assistance through cross-sectoral and cross-organisational knowledge sharing.

19

Monitoring, data collection, and advocacy.

Civil society organisations must continue to play a vital role in collecting data and monitoring trends in relation to cyber and technologically facilitated violence, supplementing official information and identifying gaps in the system. These data serve as the foundation for effective advocacy and evidence-based policy formulation. Activities should include:

- Systematic collection and analysis of data from cases handled by organisations.
- Publication of reports, analyses, and recommendations to institutions.
- Participation in public consultations and legislative processes.
- Building partnerships with institutions, academia, and other NGOs for joint advocacy.

20



Effectively combating cyber and technologically facilitated violence requires a comprehensive, cross-sectoral, and coordinated approach that brings together the efforts of government institutions, lawmakers and policymakers, the private sector, the media, and civil society. There is a need to modernise the legal framework, fully transpose European requirements, and consistently recognise new forms of digital violence as real and serious risks to the security, rights, and dignity of victims. At the same time, sustainable mechanisms for prevention, training, data collection, and inter-institutional cooperation should be developed to ensure not only a response to incidents of violence but also the long-term prevention of CTFV.

The cyber and technological dimensions of violence require improved ecosystem capacity: specialised units, digitally literate professionals, standards for working with victims of CTFV, accessible services, and enhanced cross-sectoral cooperation.



invisible Data



COUNTER
INTUITIVE INSTITUTE