WAVE FEMPOWER Magazine

published by Women Against Violence Europe 1 2026 No. 37

Technology-Facilitated Violence Against Women and Girls: Feminist Responses in a Digital Age

Imprint Publisher:
WAVE Network, Bacherplatz 10/6, A-1050 Vienna | ZVR: 601608559
Phone: +43-1-5482720 | E-mail: office@wave-network.org
Website: wave-network.org

Editor: Beverly Mtui
With the support of: Sarah Castellanos, Carloruggero Anastasio & Ilaria Nilges
Graphic Design: Monika Medvey
Cover photo: Clay Banks / Unsplash
Uncredited photos are privately owned.
Place and year of publication: Vienna, Austria, 2026

This publication has been produced with the financial support of the Citizens, Equality, Rights and Values Programme of the European Union. The contents of the magazine are the sole responsibility of the authors and Women Against Violence Europe (WAVE) and can in no way be taken to reflect the views of the European Commission or other funders.

Disclaimer: The views and opinions expressed in the magazine are those of the author(s) and do not necessarily reflect the official policy or opinion/position of Women Against Violence Europe (WAVE).

Thank you to our funders:

Federal Chancellery
Republic of Austria

Federal Ministry
Women, Science
and Research
Republic of Austria

Federal Ministry
Labour, Social Affairs, Health,
Care and Consumer Protection
Republic of Austria

Table of contents

4 **Beyond Cyber Violence: Is the Transposition of the EU Directive an Opportunity to Recognise Digital Coercive Control?**
Kristina Kulić, Croatia

7 **Co-Creating Safer Digital Spaces for Women with Disabilities: A Participatory Approach to Preventing Technology-Facilitated Violence**
Olga Damsen and Janne Hofmann, GESINE Intervention, Germany

10 **Not Yours to Take: Latvia Criminalises Non-Consensual Sharing of Intimate Images**
Polina Filipova, MARTA Centre, Latvia

13 **Who Can Log In? Digital Exclusion as a Hidden Driver of Technology-Facilitated Violence Against Migrant Women**
Ana Freire Jácome, Por Ti Mujer, Spain

16 **From Online Deception to Human Trafficking: Frontline Responses to Technology-Facilitated Violence Against Women and Girls in Albania**
Brikena Puka and Oliana Manaj, Psycho-Social Center 'Vatra', Albania

18 **Abuse in the Digital Age: How We Respond to the Emerging Threats Facing Women and Girls**
Kiera Brodie, Refuge, England (UK)

21 **Translating Survivor Knowledge into Political Power: Building Feminist Alliances for Violence-Free Digital Futures**
Elizabeth Ávila González, bff – German Federal Association of Rape Crisis Centres and Women's Counselling Centres, Germany

Editorial

Women Against Violence Europe (WAVE) is the only European network focusing solely on the elimination of violence against women and girls, and represents more than 1,800 women's specialist services[1] through over 190 members based in 46 European countries. In 2024, WAVE marked 30 years of promoting and strengthening the human rights of women and children across Europe. Since its founding, WAVE's mission and dedication have remained resolute: to enable women and their children to live free from violence by building and sustaining a network of women's specialist services, experts and survivors. Over 30 years on, this crucial work continues.

As digital spaces increasingly become sites of harm, surveillance and control, technology-facilitated violence against women and girls demands urgent feminist attention. With platforms evolving and new forms of abuse emerging, women's specialist services, advocates and researchers are working to understand, name and provide a response, while affirming that technology-facilitated violence is a deeply serious rising form of harm.

This edition of the WAVE Fempower Magazine explores how feminist organisations across Europe and beyond are rising to meet this challenge. Spanning seven contributions from WAVE members, this issue moves across an intricate spectrum of technology-facilitated violence: from image-based abuse and digital coercive control to online deception as a gateway to trafficking. It further explores the hidden barriers faced by migrant women and women with cognitive disabilities in digital spaces, and how survivor knowledge can be translated into feminist political power and lasting change. These articles offer advocacy insights, practice-based reflection, research evidence and policy analysis, attesting to the depth of feminist expertise shaping the field of violence prevention and elimination.

We thank all authors for their time, courage and commitment to this work. We hope that the WAVE Fempower Magazine 2026 deepens our collective responsibility to ensure that digital spaces are safe and free from violence against women and girls. ●

Beverly Mtui is WAVE's Communications Coordinator, leading the network's strategic external communications. She has almost a decade of experience in feminist civil society organisations working to end violence against women in Austria and at the European level. She holds a Master's degree in Globalisation and Development Studies from Maastricht University and also works as a freelance journalist focusing on the empowerment of people of African descent.

Support the WAVE Network and donate now:

https://wave-network.org/donate/donate-now/

1 Women's specialist services is a collective term used to define feminist services that support women and their children experiencing gender-based violence. These services include, but are not limited to, women's centres, women's shelters, helplines, rape crisis or sexual violence referral centres, as well as primary prevention services.

Beyond Cyber Violence:

Is the Transposition of the EU Directive an Opportunity to Recognise Digital Coercive Control?

Kristina Kulić,[1] Croatia

The use of technology in intimate partner violence is often difficult to distinguish from the ordinary use of digital services. A perpetrator may track a woman's location, access her accounts, monitor her communications or repeatedly contact her online. In isolation, some of these acts may appear minor or even lawful. Their significance changes, however, when they form part of an ongoing pattern of surveillance and control that may continue after separation. This understanding is consistent with the work of the Council of Europe's Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO), the independent expert body responsible for monitoring the implementation of the Istanbul Convention. In its General Recommendation No. 1 on the digital dimension of violence against women (2021), GREVIO recognised technology-facilitated violence as a continuation of violence against women occurring offline, rather than as a separate phenomenon. It highlighted online and technology-facilitated stalking, sexual harassment and the digital dimension of psychological violence, and called on states to strengthen prevention, protection, prosecution and a coordinated response.[2] This perspective is particularly relevant to the implementation of Directive (EU) 2024/1385 on combating violence against women and domestic violence, which Member States must transpose by 14 June 2027.[3]

In frontline work with women survivors of violence, technology rarely appears as a separate category of abuse. Women may not describe their experience as 'digital violence'. Instead, they describe a partner who knows where they are, demands constant location updates, controls passwords, monitors contacts or continues to reach them after separation. Digital control can also operate through children. A perpetrator may use a child's phone, school communication system or healthcare information to obtain information about the mother. Repeated mobile phone calls and emails to a paediatrician, frequent visits to a school or persistent requests for information about a child through online school groups may appear legitimate when considered separately, but can form part of a wider pattern of harassment and control. This is relevant in Croatia because public digital services can also become a source of information. Through the e-Citizens system, the Health Portal enables parents to access certain health information concerning their minor children, including information about medical visits and appointments.[4] In a situation involving domestic violence, such information could allow a perpetrator to find out where and when a child – and potentially the mother accompanying them – will be present. The issue is not the legitimacy of these services. The Health Portal is intended to facilitate access to healthcare information. The difficulty arises when a legitimate form of access is used within a pattern of surveillance or intimidation.

The same problem occurs with other ordinary channels. In one case encountered in practice, a perpetrator used the description field of child-support payments on online banking platforms to send threatening messages to the woman. In another,

1 Individual WAVE member

2 Group of Experts on Action against Violence against Women and Domestic Violence. (2021). *GREVIO General Recommendation No. 1 on the digital dimension of violence against women.* Council of Europe. https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147

3 Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence. (2024). *Official Journal of the European Union*, L, 2024/1385, Art. 49. https://eur-lex.europa.eu/eli/dir/2024/1385/oj

4 Government of the Republic of Croatia. (n.d.). Health Portal is mobile-friendly. https://gov.hr/?id=2341&lang=en&url=print

a woman received flowers with no sender's name at a new address that was supposed to be known to only a few people. The message was clear: someone was watching, and someone unknown to her knew where she lived. The florist refused to disclose the purchaser's identity, referring to data-protection obligations. Such examples illustrate why it is difficult to regulate digital coercive control through an exhaustive list of technologies or forms of communication. The channel can change: social media platforms, online payment systems, digital contact with schools, online healthcare platforms or a third party may all become means of maintaining contact or obtaining information.

The Directive establishes common standards for several forms of cyber violence, including cyber stalking (Article 6) – repeated or continuous surveillance through information and communication technologies to monitor a person's movements and activities – as well as cyber harassment (Article 7) and cyber incitement to violence or hatred (Article 8).[5] Croatian criminal law already contains provisions relevant to many forms of technology-facilitated violence, including threats and stalking. For instance, in 2021, Croatia introduced Article 144a of the Criminal Code, criminalising the misuse of sexually explicit recordings. It covers sharing with a third party, without consent, a recording that was originally created with the person's consent for personal use, where the perpetrator has abused a relationship of trust and thereby violated the person's privacy. It also covers creating or altering sexually explicit content, including digitally manipulated content, and presenting it as genuine in a way that violates the privacy of the person depicted.[6] A recent analysis examines the Croatian criminal-law framework in relation to the requirements of the Directive and identifies challenges concerning the scope and application of existing provisions.[7] The issue is therefore not simply whether a particular digital act can be subsumed under an existing offence. It is also whether several acts can be understood in their context, where their cumulative effect is to restrict a woman's freedom and maintain the perpetrator's control. This distinction is particularly relevant to stalking. Technology can make surveillance continuous, remote and difficult to detect. Location tracking, access to accounts, monitoring of online activity and repeated unwanted contact may occur simultaneously and across different platforms in the context of abuse.

The implications are particularly important for protection orders. Article 19 of the Directive requires Member States to ensure that, in situations of immediate danger, competent authorities can prohibit an offender from contacting the victim or dependants 'in any way'.[8] The Directive also expressly refers to contact through online interfaces. In practice, whether it is in Croatia or elsewhere in Europe, 'contact' needs to be understood beyond direct messages or telephone calls. A perpetrator who is prohibited from contacting a woman should not be able to circumvent that restriction by using other means to monitor, threaten or abuse her, or to gain access to private information about where she is located. The indirect contact described above – through a child's paediatrician, school or online school groups – can, in some cases, be part of the same pattern of coercive control as direct digital surveillance. The same consideration should apply to digital public services. Where a perpetrator has been assessed as posing a risk to a woman, protection measures should be capable of addressing access to digital systems insofar as that access enables him to monitor her, obtain information about her whereabouts or facilitate unwanted contact.

Data protection raises a related but distinct issue. The fact that information is protected by the General Data Protection Regulation (GDPR) does not, by itself, determine whether it can ever be disclosed to authorities. The more relevant questions are whether there is a lawful basis for access, whether the information is necessary for the investigation or prevention of violence, and whether the disclosure is proportionate to the purpose for which it is sought. The anonymous flower delivery illustrates the problem: the florist cited data protection to refuse disclosure, even though the purchaser's identity may have been directly relevant to the woman's safety. The same principle applies to public digital services. Protecting personal data and ensuring cybersecurity are essential, but the design and operation of digital systems should also take into account the risks faced by survivors of domestic violence. →

5 Directive (EU) 2024/1385. (2024). Arts. 6–8.

6 Republic of Croatia. (2021). *Act on Amendments to the Criminal Code*. Official Gazette, 84/2021, Art. 144a.

7 Munivrana, M., & Brđanović, T. (2025). Criminal law protection of women from gender-based online violence: Challenges in the implementation of Directive (EU) 2024/1385. *Croatian Annual of Criminal Sciences and Practice*, 32(2), 387–418. https://hrcak.srce.hr/en/clanak/494367

8 Directive (EU) 2024/1385. (2024). Art. 19(1) and Recital 45.

→ Where necessary and legally justified, mechanisms should exist to restrict or modify access to information that could expose a woman to further surveillance or harm.

The psychological impact of digital coercive control can be profound. When a woman knows that her whereabouts, communications or activities may be monitored, physical separation does not necessarily produce a sense of safety. Instead, she may continue to feel watched and pursued, constantly anticipating the next attempt at contact or surveillance. This can produce a persistent state of hypervigilance: checking devices repeatedly, changing routines, avoiding places where she might be found and feeling that there is no safe space in which the perpetrator cannot reach her. For some women, the experience develops into a sense of hopelessness that they will never be able to fully escape the perpetrator's reach. This is consistent with the psychological consequences of prolonged exposure to violence, including symptoms associated with post-traumatic stress among women survivors of violence.[9] Recognising the potential severity of these impacts is therefore essential to understanding digital coercive control as part of the continuum of violence experienced by survivors.

The transposition of the Directive offers an opportunity to examine digital coercive control within the wider system of criminal law and victim protection, rather than as a collection of isolated online offences. The Croatian transposition process should therefore address digital forms of control within existing mechanisms for stalking, threats, protection orders and risk assessment. In practice, this would require frontline professionals to ask not only whether a perpetrator has directly contacted the victim, but also whether he has access to her accounts, devices, location data or information held by institutions concerning the children. Such questions could be incorporated into safety planning and risk assessment rather than being treated as a separate category of 'online' abuse. Public digital services should be developed with an awareness that information intended to facilitate citizens' access to services can, in particular circumstances, also be misused by perpetrators. Digital coercive control is difficult to capture precisely because perpetrators do not necessarily rely on illegal technologies, but on something more insidious: everyday tools that all of us use for banking, healthcare, childcare and staying in touch with our communities. The effectiveness of protection therefore depends not only on preventing physical contact, but also on preventing the forms of digital and indirect access through which coercive control can continue.

States cannot realistically anticipate all the ways in which perpetrators may use technology and otherwise legitimate services to continue monitoring and controlling women. The response therefore needs to combine sufficiently broad legal safeguards with the practical capacity to investigate digital forms of abuse. This includes strengthening digital-forensics capacity within law enforcement and ensuring that police, prosecutors and other relevant professionals receive specialised training on technology-facilitated violence. Furthermore, this should cover not only the offences introduced or amended in response to the Directive, but also the practical identification of location tracking, account access, device monitoring and indirect digital contact. Effective implementation of the Directive will depend not only on legislative amendments, but also on whether institutions have the expertise and resources to recognise digital coercive control and preserve the evidence needed to respond to it. ●

Kristina Kulić is a social worker and independent expert on violence against women, with more than 13 years of experience in frontline work, research, advocacy and training. Her professional journey draws on direct work with survivors of gender-based violence and covers structural violence, coercive control, economic and digital violence, trauma-informed care and institutional responses to violence against women. She is a lecturer and trainer with extensive experience in educating professionals who work with survivors of violence. She has contributed to international human rights monitoring and advocacy processes, including presenting before the UN Committee on Economic, Social and Cultural Rights (CESCR) in Geneva and speaking at the UN Commission on the Status of Women (CSW) in New York as a member of official Croatian delegations. She has also contributed to international reports and research on violence against women and collaborates with organisations across Europe on advocacy, research, policy development and professional education.

9 Lauri Korajlija, A., & Kulić, K. (2024, July 25). *Post-traumatic stress disorder in women survivors of domestic violence* [Paper presentation]. 45th International Conference of the Stress, Trauma, Anxiety, and Resilience Society, Charlotte, NC, United States.

Co-Creating Safer Digital Spaces for Women with Disabilities:

A Participatory Approach to Preventing Technology-Facilitated Violence

Olga Damsen and Janne Hofmann, GESINE Intervention,[1] Germany

Women with disabilities[2] experience disproportionately high levels of physical, psychological and sexualised violence throughout their lives,[3] in addition to various forms of discrimination and exclusion. While the digital sphere offers new possibilities for them to access information or support, and to connect with others, these spaces can also expose them to new forms of violence and abuse. Technology-facilitated violence – including cyberbullying, online sexual harassment and the misuse or non-consensual sharing of private images and messages – can be particularly harmful for women with disabilities. Various forms of discrimination, in particular sexism and ableism, intersect to increase both their risk of experiencing digital violence and the barriers they face when seeking help.

Despite this, there is a lack of accessible, tailored training and awareness-raising initiatives that address their specific needs. The result is a double gap: women with disabilities remain under-informed about digital risks and available support, while the professionals around them may be unsure how to respond when violence occurs. GESINE Intervention decided to address this gap at the local level.

Participatory action and innovation

GESINE Intervention is a specialised agency for prevention, information, protection and support regarding violence against women in North Rhine-Westphalia, Germany. Its work includes running a women's shelter and decentralised women's counselling centres, a programme for people who use violence, awareness-raising campaigns, interdisciplinary cooperation, research, training and advocacy activities aimed at creating lasting structural change.

For many years, the organisation has been committed to strengthening the protection and empowerment of women with cognitive disabilities. Twelve years ago, GESINE established 'Courageous and Strong', a group in which women with disabilities learn about different forms of violence, develop strategies for protecting themselves, and are encouraged to empower others. GESINE also works with facilities for people with disabilities to support them in developing and implementing concepts for protection against violence. →

Technology-facilitated violence is becoming a political concern – but who is being heard?

Following several high-profile cases, technology-facilitated violence has become a topic of increasing public and political concern across Europe. In Germany, for example, the Ministry of Justice published a draft bill in April 2026 aimed at strengthening civil and criminal protection against it. Yet the specific experiences and needs of women with disabilities and other marginalised groups remain underrepresented in public discourse.

1 GESINE Intervention: https://www.gesine-intervention.de/

2 Disclaimer: When we speak of 'women with disabilities', we mean women with cognitive disabilities in the context of the project presented later in this article. This is because the project activities are tailored to this particular target group. The needs of women with cognitive disabilities differ from those of women with physical disabilities.

3 Federal Ministry for Family Affairs, Senior Citizens, Women and Youth. (2014). *Lebenssituation und Belastungen von Frauen mit Beeinträchtigungen und Behinderungen in Deutschland* [The living conditions and pressures faced by women with impairments and disabilities in Germany]. https://www.bmbfsfj.bund.de/bmbfsfj/service/publikationen/lebenssituation-und-belastungen-von-frauen-mit-beeintraechtigungen-und-behinderungen-in-deutschland-80576

Photo: GESINE

Olga Damsen at one of the project's training sessions, listening to participants and discussing technology-facilitated violence and prevention measures

→ Based on this experience, we are implementing an innovative WAVE-funded project that aims to strengthen the protection of women with disabilities against technology-facilitated violence through inclusive, participatory approaches. Our mission: to empower women with cognitive disabilities to protect themselves against digital violence, and to equip the professionals working with them to provide effective support.

Trauma-informed leadership coaching

Our work with women with cognitive disabilities is guided by a principle we call 'trauma-informed leadership coaching'. It is based on an understanding of trauma that recognises the complex interplay between experiences of violence and discrimination. The everyday lives of many of the women we work with are shaped by factors such as social prejudice and legally restricted self-determination (e.g. statutory guardianship and living in residential care settings).

In this context, trauma-informed leadership coaching means continuously reassessing individual potential, identifying factors that may undermine one's sense of agency and integrating these considerations into every stage of our work. Participation and empowerment, therefore, are more than simply giving someone a voice in a project. Our aim is to create opportunities for women with disabilities to become leaders and multipliers within their networks, while being mindful of the fine line between strengthening a person's sense of capability and making them feel overwhelmed.

From participation to co-creation

In May 2026, the project began with a workshop involving a group of women with cognitive disabilities. Rather than starting with a predefined curriculum, we wanted to hear from the participants themselves: What kind of devices and applications do you use? What do you know about digital violence? Have you experienced it yourself? If so, what support did you receive? What would have helped you more? What information do you need? What should other women with disabilities know about this topic?

Using Easy Language and printed pictures, we created an accessible environment in which participants could share their experiences and ideas. Some key impressions:

1) Women with cognitive disabilities actively participate in digital spaces and use a variety of applications to stay connected with family and friends, access information or share news about their days – often using creative solutions, such as the use of voice assistants, to overcome access barriers.
2) They do experience digital violence – from cyberbullying to sexual harassment and abuse.
3) Participants differed significantly in their use of digital technologies, experiences of digital violence and knowledge of how to protect themselves.

Thus, instead of a one-size-fits-all approach, training concepts need to be flexible and meet women where they are.

The women's input directly informed the development of training concepts and materials. We created accessible printed cards featuring pictures and questions in Easy Language and embedded them in a flexible training concept. This allows participants to influence the content and direction of the sessions, making it possible to tailor the training to their individual skills and needs. In parallel, we developed training concepts and materials for professionals working with women with disabilities, identifying relevant focus areas and recommendations for action based on the insights shared by women.

Pilot training sessions delivered in August 2026 gave us an opportunity to test the materials in practice and

Photo: GESINE

Flipchart sheets used to plan the Easy Language brochure, including the note 'You have to be careful what you send, e.g. nude photos' ('Du musst gut aufpassen, was du verschickst, z. B. Nacktfotos')

Olga Damsen is a project coordinator at GESINE Intervention. After working on several EU research projects, she now focuses on implementing 'KoRA' (Coordinated Risk Assessment) and the WAVE-funded project 'Strengthening Protection for Women with Disabilities Against Digital Violence'. She holds a Master's degree in Empowerment Studies with an emphasis on Human Rights Policy from the University of Applied Sciences in Düsseldorf, Germany. Previously, she spent more than ten years working in psychosocial counselling with refugees and in trauma stabilisation for survivors of domestic and sexual violence.

Janne Hofmann works as a project coordinator at GESINE Intervention. She holds a Master's degree in Human Rights and Humanitarian Action with a specialisation in project management from Sciences Po Paris, France. Prior to joining GESINE, she worked in the humanitarian sector in Germany and abroad for several years.

→ refine them based on feedback from women with disabilities and professionals. The revised concepts will be transformed into a training handbook, which we aim to make available to other organisations that may wish to use it in their own settings. The process has already produced several important lessons:

Start from participants' needs. Digital violence is a complex and rapidly evolving issue. This creates a particular challenge for training: How do you create training materials that are comprehensive enough to be useful, but not so complex that participants become overwhelmed or the content becomes outdated within months? Our approach was to ask women with disabilities and professionals which experiences and subtopics were most relevant to them and to build the training around their answers. We also used a practice-oriented, participant-led approach, and gave participants access to further information and support, so they know where to turn when they encounter a situation that goes beyond what they have learned.

Agency creates leadership. Women with disabilities may face discrimination at the individual and societal level that can lead to experiences of silencing and disempowerment. Hence, training needs to counteract these dynamics by honouring their individual agency. Our pilot showed that this can foster leadership and create multiplier effects. One of our pilot groups, for instance, expressed the desire to teach other women with disabilities about digital violence – an idea we are now putting into practice together by developing an informational brochure in Easy Language and a peer-to-peer training concept that they can deliver themselves.

Simple, but key: digital violence is real for women with disabilities – and needs to be addressed.

All women with disabilities, as well as professionals working in disability services, should be trained on digital violence. Ideally, each facility should designate at least one digital safety advocate who can serve as a first point of contact when concerns and cases arise. This should be integrated into facilities' strategies for protection against violence and, in the longer term, become a legal obligation for facilities.

That said, we are aware that this type of structural change seems far off in many contexts. Yet our project has shown that improvement does not have to wait for systemic reform. Even small-scale action can have an impact when it is participatory, practice-oriented, flexible and grounded in the potential and agency of women with disabilities. The aim should be to create safer digital spaces with women with disabilities, building on their knowledge and leadership. ●

Not Yours to Take:

Latvia Criminalises Non-Consensual Sharing of Intimate Images

Polina Filipova, MARTA Centre,[1] Latvia

Violence against women is no longer confined to physical spaces. Now, more than ever, it follows women into the digital world.

As relationships, conversations and increasingly intimate parts of our lives move into digital spaces, technology has become another tool through which gender-based violence can be perpetrated, amplified and reproduced. Non-consensual sharing of intimate images is one of its most invasive manifestations. It can involve distributing photographs or videos originally created consensually, secretly recorded material, threats to publish intimate content, or manipulated and artificially generated images. What these acts have in common is that they take away the depicted person's control over something profoundly intimate: their body, sexuality and identity. The consequences can be devastating. Intimate images can be copied, downloaded and redistributed within seconds, leaving victims with little control over where the content appears or who sees it. The harm may affect their relationships, employment, mental wellbeing, safety and participation in public life. Importantly, digital violence rarely exists separately from violence offline. European data increasingly shows an online–offline continuum, particularly in cases involving intimate partner violence.[2] For women and girls, this continuum has a clear gendered dimension. Technology may change the tools used by perpetrators, but the underlying dynamics – humiliation, sexualisation, coercion, punishment and control – are the same.

Artificial intelligence has added another layer to this problem.

Today, a perpetrator no longer needs to possess a real intimate image of a victim. Generative AI and so-called nudification tools can create one from an ordinary photograph, while deepfake technology can place a person's face onto sexually explicit material that never existed. The fact that an image is artificial does not make the violence artificial. Figures cited by the European Parliamentary Research Service indicate that 98% of deepfakes available online are pornographic and 99% of those depict women.[3] In May 2025 alone, 31 websites hosting tools capable of creating synthetic intimate imagery received a combined 20.7 million visits worldwide, illustrating the enormous scale and accessibility of this technology.[4] The rapid development of accessible generative AI makes this particularly alarming. Creating sexualised materials no longer necessarily requires sophisticated technical knowledge. A publicly available photo on social media may be enough. This changes the scale of image-based sexual abuse, but not its essence. Whether an intimate image was originally shared privately with a partner or generated by an AI tool without ever existing in reality, the purpose and impact are similar.

European legislation is gradually catching up with this reality.

Directive (EU) 2024/1385, the EU's first directive on violence against women

1 Centrs MARTA: https://www.marta.lv/

2 European Institute for Gender Equality. (2026). *Protecting women in the digital age: Strengthening EU action against cyber violence.* https://eige.europa.eu/gender-statistics/dgs/data-talks/protecting-women-digital-age-strengthening-eu-action-against-cyber-violence?language_content_entity=en

3 Bentzen, N. (2026). *Women in the age of AI-enabled disinformation* [Briefing]. European Parliamentary Research Service. https://www.europarl.europa.eu/RegData/etudes/BRIE/2026/782670/EPRS_BRI(2026)782670_EN.pdf

4 Puglielli, C., & Craanen, A. (2025, October 23). *The ecosystem of nonconsensual intimate deepfake tools online.* Institute for Strategic Dialogue. https://www.isdglobal.org/digital-dispatch/the-ecosystem-of-nonconsensual-intimate-deepfake-tools-online/

and domestic violence, requires Member States to criminalise the non-consensual sharing of intimate images by June 2027. It explicitly covers manipulated material: creating or altering images, including through artificial intelligence, to make it appear that a person is engaged in sexually explicit activities, where the material is then made accessible without their consent and is likely to cause serious harm.[5]

This represents a significant change in the European approach to digital violence. In the European Commission's 2022 assessment, only ten EU Member States (Belgium, France, Ireland, Italy, Malta, the Netherlands, Poland, Portugal, Spain, Sweden) were identified as having specifically criminalised the non-consensual dissemination, publication or disclosure of intimate images.[6] By 2027, protection against this form of abuse should no longer depend on which EU country a victim happens to live in.

The Istanbul Convention provides another important framework. The Convention – which the Latvian Parliament voted to leave in 2025 (see below) – also applies online: GREVIO's General Recommendation No. 1 confirms that its provisions cover violence committed through technology, including technologies yet to be developed.[7]

Latvia has now taken an important step towards recognising this reality.

On 19 March 2026, the Latvian Parliament adopted amendments to the Criminal Law introducing criminal liability for distributing intimate material without the consent of the person depicted. The amendments entered into force on 16 April 2026.[8]

The new Section 145[1] covers images, videos and similar material depicting another person's sexual activities or intimate body parts. The amendments also strengthen the protection of victims of human trafficking by introducing stricter criminal liability in cases where a victim of human trafficking is involved in the production of pornography.[9]

Crucially, the provision applies not only to authentic materials, but also to materials that have been created or altered using technical or other means. As the Latvian Parliament explained when adopting the amendments, this includes materials artificially created or modified using image-processing software or artificial intelligence tools.[10]

Publishing such material or transmitting it to another person without the depicted person's consent can now result in imprisonment for up to one year, short-term imprisonment, probation supervision, community service or a fine. The same penalties apply to threats to distribute such material when they are used to force a person to do, accept or refrain from doing something. Where substantial harm is caused, imprisonment of up to three years may be imposed.[11]

The wording is important for another reason. Latvia's provision is not limited to publishing material openly on the internet. As mentioned above, liability may also arise from sharing or transmitting such material to another person. This matters because, in practice, intimate-image abuse does not always begin with thousands of strangers seeing an image. Sometimes it begins with sending it to one colleague, one family member, one new partner or one group chat, and consent has already been violated at that moment.

Criminalising this behaviour sends a message that extends beyond individual criminal cases: consent to creating intimate material is not consent to distributing it. Consent to sending an image to one person is not consent for that person to send it on. And with AI-generated images, there is often no consent at any stage: neither to the image being created nor to it being shared. →

5 Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combating violence against women and domestic violence. (2024). *Official Journal of the European Union*, L, 2024/1385, Arts. 5–8 and 49. https://eur-lex.europa.eu/eli/dir/2024/1385/oj

6 European Commission. (2022). *Impact assessment accompanying the proposal for a directive of the European Parliament and of the Council on combating violence against women and domestic violence* (SWD(2022) 62 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52022SC0062

7 Group of Experts on Action against Violence against Women and Domestic Violence. (2021). *GREVIO General Recommendation No. 1 on the digital dimension of violence against women.* Council of Europe. https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147

8 Republic of Latvia. (2026). Amendments to the Criminal Law [Grozījumi Krimināllikumā]. Latvijas Vēstnesis [Official Gazette], 2026/65.1. https://www.vestnesis.lv/op/2026/65.1

9 Parliament of the Republic of Latvia. (2026). *Stronger measures to combat deep fakes and non-consensual distribution of intimate images* [Press release]. https://www.saeima.lv/en/news/saeima-news/29027-saeima-adopts-administrative-territorial-r/35624-stronger-measures-to-combat-deep-fakes-and-non-consensual-distribution-of-intimate-images

10 Parliament of the Republic of Latvia. (2026). *Stronger measures to combat deep fakes and non-consensual distribution of intimate images* [Press release]. https://www.saeima.lv/en/news/saeima-news/29027-saeima-adopts-administrative-territorial-r/35624-stronger-measures-to-combat-deep-fakes-and-non-consensual-distribution-of-intimate-images

11 Parliament of the Republic of Latvia. (2026). Stronger measures to combat deep fakes and non-consensual distribution of intimate images [Press release]. https://www.saeima.lv/en/news/saeima-news/29027-saeima-adopts-administrative-territorial-r/35624-stronger-measures-to-combat-deep-fakes-and-non-consensual-distribution-of-intimate-images

→ This is fundamentally a question of dignity and bodily autonomy.

For too long, conversations about intimate-image abuse have focused on the victim's choices rather than the perpetrator's actions: *Why did she take the photo? Why did she send it? Why did she trust him?* But none of these questions address the actual violation. The question we should be asking is: *Why did someone choose to share an intimate image without her consent?*

Moving the focus from the victim's behaviour to the perpetrator's actions is essential.

Criminal law alone will not eliminate technology-facilitated violence, particularly when images can cross platforms and borders almost instantly. Effective implementation, accessible reporting mechanisms, rapid removal of materials, informed law-enforcement responses and specialised victim support will remain crucial. But naming the behaviour as a criminal offence establishes an essential baseline: responsibility lies with the person who violated consent.

The significance of this development becomes even clearer when placed within Latvia's current political climate.

Women's rights and gender equality have become increasingly contested in public and political debate. In October 2025, the Latvian Parliament voted to withdraw from the Istanbul Convention, the international treaty specifically designed to prevent and combat violence against women and domestic violence. Following widespread public mobilisation, the President returned the law to Parliament for reconsideration by the newly elected legislature. Its further consideration has been postponed, with a deadline for parliamentary proposals set for 1 November 2026.[12]

The debate has been accompanied by broader anti-gender narratives and recurring political discussions around women's reproductive autonomy and the meaning of gender equality itself. In such an environment, progress cannot be taken for granted.

At a moment when some protections for women are being questioned, Latvia has simultaneously recognised a form of violence that barely existed in public consciousness a decade ago. It has acknowledged that women's right to safety and dignity does not disappear when violence moves online, and that legislation must develop alongside technology.

The new law will not prevent every intimate image from being shared, nor every AI-generated sexual image from being created. Its real impact will depend on whether victims know their rights, whether police and prosecutors understand the gendered dynamics of violence and image-based abuse, whether cases are investigated effectively and whether perpetrators are actually held accountable.

Nevertheless, the law establishes an important and much-needed principle. Technology may evolve and the platforms through which violence is perpetrated may change. The images themselves may be real, manipulated or entirely AI-generated. The methods of abuse may become more sophisticated and increasingly difficult to recognise. But the fundamental principle of consent does not change – it remains the line between what is freely shared and what becomes a violation. ●

Polina Filipova is Head of Communications at MARTA Centre, Latvia's leading women's rights organisation. She holds a Master's degree in Strategic Communication Management and focuses on using strategic communication to address gender-based violence, discrimination and inequality. In her role, Polina focuses on making complex and often stigmatised issues accessible to wider audiences. She believes that communication is a powerful tool to challenge harmful stereotypes, reshape public narratives and contribute to lasting social change towards a safer and more equal society.
MARTA Centre provides professional social, legal and psychological support to adult victims of violence and human trafficking, while also advancing policy and legislation, developing violence-prevention programmes, training professionals and implementing international projects.

12 Parliament of the Republic of Latvia. (2025, November 5). *Atkārtotai izskatīšanai Ārlietu komisijā nodots likumprojekts par Latvijas izstāšanos no Stambulas konvencijas* [Draft law on Latvia's withdrawal from the Istanbul Convention submitted to the Foreign Affairs Committee for reconsideration]. https://www.saeima.lv/aktualitates/saeimas-zinas/35189-parlamenta-atkartoti-vertes-likumprojektu-par-latvijas-izstasanos-no-stambulas-konvencijas

Who Can Log In?

Digital Exclusion as a Hidden Driver of Technology-Facilitated Violence Against Migrant Women

Ana Freire Jácome, Por Ti Mujer,[1] Spain

In Spain, the rapid digitalisation of everyday life and public services has coincided with growing institutional attention to technology-facilitated violence against women. Yet access to digital tools and the skills to use them remain unevenly distributed. Public policy is moving towards increasingly digitalised responses, while paying less attention to how digital exclusion restricts migrant women's independent access to information, services and protection. For those of us working at the intersection of gender-based violence, migration and rights, this raises a fundamental question: What happens when digitalised protection systems fail to account for those facing the greatest barriers in the digital environment?

Looking beyond technology

Technology-facilitated violence against women has become a central concern on international human rights and gender-equality agendas. Far from being an isolated phenomenon, it forms part of a continuum with other forms of gender-based violence, amplifying harassment, coercive control and threats.[2] Significant gaps in the evidence nevertheless remain, particularly concerning how it manifests itself and how it affects different groups of women.[3]

These developments have produced legal frameworks and responses designed to strengthen protection, improve access to justice and foster safer digital environments. Their effectiveness, however, depends on women being able to access the available tools and to use them meaningfully. Inequalities in access to devices, connectivity and digital skills disproportionately affect certain groups, including migrant women, while also restricting their access to online information and public services.[4] At its sixty-seventh session (CSW67) in 2023, the Commission on the Status of Women recognised that while technology can improve migration procedures and access to services, these benefits cannot be fully realised without addressing the digital divides affecting migrant women and girls.[5]

When access to information, safety resources or protection services depends on the ability to navigate digital environments, digital exclusion can become an additional barrier to exercising rights. The question, then, is not simply how technology facilitates or intensifies violence, but whether prevention and protection systems are equipped to respond to those unable to access or navigate the digital environment independently.

Our argument is not that the digital divide is, in itself, a form of violence, nor that all migrant women experience technology in the same way. Rather, we suggest that the interaction between gender, migration, language barriers, socioeconomic inequality, immigration status and digital exclusion can create specific conditions that hinder effective access to information, support and protection mechanisms. →

1 Asociación Por Ti Mujer: https://asociacionportimujer.org/

2 Group of Experts on Action against Violence against Women and Domestic Violence. (2021). *GREVIO General Recommendation No. 1 on the digital dimension of violence against women.* Council of Europe. https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147

3 UN Women. (2023). *Technology-facilitated violence against women: Taking stock of evidence and data collection.* https://knowledge.unwomen.org/sites/default/files/2023-04/Technology-facilitated-violence-against-women-Taking-stock-of-evidence-and-data-collection-en.pdf

4 Group of Experts on Action against Violence against Women and Domestic Violence. (2021). *GREVIO General Recommendation No. 1 on the digital dimension of violence against women.* Council of Europe. https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147

5 Commission on the Status of Women. (2023, March 20). *Innovation and technological change, and education in the digital age for achieving gender equality and the empowerment of all women and girls: Agreed conclusions* (E/CN.6/2023/L.3). United Nations. https://docs.un.org/en/E/CN.6/2023/L.3

→ This question emerges from our work at Por Ti Mujer, where we provide feminist legal support to migrant women in Spain. For many, the difficulty lies not only in the risks posed by the digital environment, but also in the barriers to using it independently as a route to information, services and the exercise of rights.

This reflection is particularly significant from an intersectional perspective. As Kimberlé Crenshaw argued, experiences of inequality cannot be understood by examining categories such as gender, origin or immigration status in isolation; they must be understood through their interaction.[6] International and European standards have repeatedly stressed the need to address the specific barriers faced by women exposed to multiple forms of discrimination, including migrant, refugee and asylum-seeking women.

What we learned by listening to women

This reflection is grounded in direct practice and in the situated knowledge generated through feminist legal support and participatory focus groups we have conducted with migrant women.

We designed the focus groups to explore participants' everyday lives and their access to rights. It was there that digital exclusion surfaced repeatedly, particularly in migration procedures, which the Spanish administration has moved almost entirely online. Participants described difficulties completing online procedures, locating reliable information, using institutional platforms and navigating increasingly digitalised processes independently. Many said they felt insecure when using digital tools and relied on third parties for procedures requiring a form of digital identification they themselves did not fully understand or control. That dependence can place their own digital identity at risk.

The findings point to something both simple and urgent: when designing information, prevention and protection measures, or pathways to access rights and services, we cannot assume that all women have the digital access, skills and confidence needed to use them independently.

This observation is especially relevant in Spain. A 2025 study by the Government Delegation Against Gender-Based Violence on digital violence against women and minors confirms the phenomenon's complexity and the need for legal, educational and technological responses.[7] Our experience contributes a practice-based perspective, drawing attention to the challenges faced by women who cannot independently navigate increasingly digitalised pathways to information, support and protection.

The women we have spoken to describe everyday, less visible forms of exclusion rather than the spyware and sophisticated digital surveillance that tend to dominate public debate. This may be the hardest form of vulnerability to see, and precisely for that reason, the most urgent to name. We use this evidence to show how a lack of digital autonomy becomes, in practice, a cross-cutting barrier to exercising rights.

When protection also depends on access

Digital exclusion is often analysed in terms of access to devices, connectivity or digital skills. These dimensions matter, but in the context of gender-based violence they are not enough.

The European debate recognises the need for protection systems that are tailored to different experiences and remain accessible to women facing intersectional discrimination. GREVIO, the Council of Europe's expert body, warns in its General Recommendation No. 1 that legal and policy responses must account for the heightened effects of intersecting forms of discrimination, including the specific barriers faced by migrant, asylum-seeking and refugee women.[8] In March 2026, the Council of Europe went further with Recommendation CM/Rec(2026)2, which emphasises the need for effective, accessible justice systems that remove complex procedures and other barriers to access.[9] The conversation is therefore shifting from recognising technology-facilitated violence

6 Crenshaw, K. (1989). Demarginalizing the intersection of race and sex: A Black feminist critique of antidiscrimination doctrine, feminist theory and antiracist politics. *University of Chicago Legal Forum*, 1989(1), 139–167.

7 Delegación del Gobierno contra la Violencia de Género. (2025). *Violencia contra mujeres, niñas, niños y adolescentes en el ámbito digital* [Violence against women, girls, boys and adolescents in the digital sphere]. Ministerio de Igualdad. https://violenciagenero.igualdad.gob.es/violenciaencifras/estudios/investigaciones/violencia-contra-mujeres-ninas-ninos-y-adolescentes-en-el-ambito-digital/

8 Group of Experts on Action against Violence against Women and Domestic Violence. (2021). *GREVIO General Recommendation No. 1 on the digital dimension of violence against women.* Council of Europe. https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women-1680a49147

9 Council of Europe. (2026). *Recommendation CM/Rec(2026)2 on accountability for technology-facilitated violence against women and girls.* https://edoc.coe.int/en/violence-against-women-12590-accountability-for-technology-facilitated-violence-against-women-and-girls.html

Photo: Por Ti Mujer

Focus group conducted by Por Ti Mujer as part of a project on digital gender-based violence against migrant women in Spain, funded by the Spanish Ministry of Equality.

→ to assessing whether responses work in practice.

Drawing on our experience, we argue that this question cannot be answered by speaking only of technological participation. What is at stake is access to information, support, protection and justice. Every procedure, form or reporting mechanism moved online assumes a level of access, understanding and confidence that not all women possess. When that starting point is ignored, digitalisation does not remove barriers; it relocates them and, at times, multiplies them for those who were already disadvantaged.

For migrant women, these barriers intersect with language, administrative uncertainty, socioeconomic inequality and previous experiences of discrimination. An intersectional approach requires us to avoid generalisations – not all migrant women are digitally excluded, and migration alone does not determine vulnerability – while also recognising that particular combinations of inequality create specific obstacles that universal systems do not always detect.

This has direct implications for professional practice. Legal and specialist support in response to gender-based violence remains essential, but digital transformation requires us to ask what additional assistance women need to exercise their rights: accessible information, help navigating digital procedures and non-digital alternatives where necessary.

Our thesis is deliberately straightforward: the digital transformation of protection systems may outpace the ability of the women who depend on them most to use them independently. Unless this gap is acknowledged, tools designed to expand protection risk unintentionally reproducing the inequalities they were meant to address.

Looking beyond the screen means shifting our attention from technology to the conditions that determine who can use it, who benefits from it and who is left at the margins. It also means recognising that digital autonomy is not a prerequisite we can simply take for granted, but a condition that public policy must help secure if protection and justice are to be genuinely accessible. ●

Ana Freire Jácome is a lawyer and human rights professional with specialised training in artificial intelligence and LegalTech, and Master's degrees in Human Rights, Democracy and International Justice and in Law and Gender-Based Violence. At Por Ti Mujer, she is part of the Legal Advisory Team. With over eight years of experience at the intersection of law, gender and humanitarian action, she has worked in Ecuador and Spain in public institutions, feminist civil society and complex humanitarian contexts. Her experience includes providing legal assistance to people affected by forced displacement, armed conflict, human trafficking and gender-based violence at the Ecuador–Colombia border, as well as leading large-scale migrant regularisation processes. Having worked with international organisations including the Norwegian Refugee Council (NRC) and Cooperative for Assistance and Relief Everywhere (CARE), she now explores how technology is reshaping access to rights – and creating new forms of violence and inequality for women and girls.

From Online Deception to Human Trafficking:

Frontline Responses to Technology-Facilitated Violence Against Women and Girls in Albania

Brikena Puka and Oliana Manaj, Psycho-Social Center 'Vatra',[1] Albania

A job offer received through social media. A relationship initiated through a messaging application. A promise of travel, accommodation and well-paid employment. Behind an ordinary online interaction, a process of recruitment and exploitation may already have begun.

For the Psycho-Social Center 'Vatra', which has worked for more than two decades with victims of human trafficking and violence in Albania, this has become an increasingly important dimension of frontline work. Technology is changing not only how victims are recruited and controlled, but also how trafficking is identified, investigated and addressed. The Organization for Security and Co-operation in Europe (OSCE) has highlighted the increasing use of technology throughout the trafficking process,[2] while the latest evaluation of Albania by the Council of Europe's Group of Experts on Action against Trafficking in Human Beings (GRETA) specifically identifies the growing role of information and communication technologies in trafficking.[3]

A changing trafficking trend

Vatra's data shows how rapidly the profile of trafficking is changing. In 2024, Vatra supported 76 newly identified victims and potential victims of trafficking. Nationally, 178 victims were identified. Women and girls represented 72% of Vatra's new cases, while 45 of the 76 cases (59%) involved sexual exploitation.

In 2025, Vatra supported 166 victims and potential victims of trafficking and 54 children. 102 people received assistance for the first time. The proportion of foreign nationals among new cases increased from approximately 51% in 2024 to around 70% in 2025, while sexual exploitation increased from 59% to approximately 73% among newly identified cases. Significantly, Vatra's monitoring showed that in more than half of sexual exploitation cases identified in 2025, online and physical forms of exploitation intersected.

This trend is continuing in 2026. Between January and July, Vatra identified 67 victims and potential victims for the first time, 44 of whom were foreign nationals. Alongside sexual exploitation, there were 17 cases of labour exploitation, 12 of forced begging and one involving forced or early marriage. Thirteen of those identified were minors.

These trends must also be understood within the broader framework of violence against women and girls. For Vatra, trafficking for sexual exploitation is not separate from other forms of gender-based violence. The cases encountered in frontline practice frequently involve overlapping forms of violence, including deception, psychological manipulation, threats, coercive control, sexual violence and economic dependency. Technology can facilitate or intensify these forms of abuse, allowing control to begin before physical contact and, in some cases, to continue even after a survivor has left the exploitative situation. The rise in sexual exploitation needs to be understood not only as a trafficking trend, but also as a significant manifestation of violence against women and girls.

1 Qendra Psiko-Sociale 'Vatra': https://qendravatra.org.al/

2 OSCE Office of the Special Representative and Co-ordinator for Combating Trafficking in Human Beings. (2024, October 24). *Policy action to address technology-facilitated trafficking in human beings. Organization for Security and Co-operation in Europe.* https://www.osce.org/cthb/579190

3 Group of Experts on Action against Trafficking in Human Beings. (2025). *Evaluation report: Albania – Fourth evaluation round* (GRETA(2025)05). Council of Europe. https://rm.coe.int/greta-evaluation-report-on-the-implementation-of-the-council-of-europe/1680b65f41

When recruitment starts online

Technology-facilitated trafficking extends far beyond 'online exploitation'. Recruitment may begin through social media, messaging applications, online relationships or apparently legitimate employment opportunities. Digital tools can later be used to communicate instructions, advertise services, monitor victims or maintain control.

GRETA has documented these dynamics specifically in Albania, including the use of social media and mobile applications to establish deceptive relationships with young women before sexual exploitation, false online employment offers, and the use of technology to monitor victims.[4] The UN Office on Drugs and Crime (UNODC) has similarly documented deceptive job advertisements distributed through social media and messaging applications, promising salaries, accommodation and travel before victims are placed in exploitative situations.[5]

For foreign-national victims, this can create a complex cross-border trajectory: recruitment may take place in one country and exploitation in Albania, while recruiters or facilitators operate elsewhere, and digital evidence may be held in yet another jurisdiction.

This reality is reflected in Vatra's increasingly diverse caseload, which includes survivors from Latin America, Asia, Eastern Europe and Africa.

Frontline identification and emerging challenges

Victims rarely approach services saying, 'I am a victim of trafficking.' Instead, they describe experiences:

Recognising what lies behind these statements requires trained professionals and proactive outreach. In 2025, Vatra's Mobile Units identified 43 potential victims of trafficking; during the first seven months of 2026, they identified another 43.

The growing number of foreign-national victims has also transformed the services needed. A survivor may simultaneously need accommodation, medical and psychological assistance, legal counselling, interpretation, residence documentation and coordination with police, prosecutors, migration authorities, embassies and organisations abroad.

Access to qualified interpreters remains one of Vatra's most persistent challenges. For languages rarely available in Albania, difficulties in securing interpretation can delay identification, psychological assessment, legal assistance and communication with authorities. Language is therefore not merely an operational barrier; it directly affects access to rights.

Mental-health needs have also become increasingly complex, with some cases in 2026 requiring urgent psychiatric assessment or hospitalisation alongside trafficking protection. At the same time, lengthy or postponed legal proceedings can increase anxiety and uncertainty and undermine survivors' trust in institutions.

Digital evidence and the response ahead

Technology also changes what evidence looks like. Messages, online advertisements, social-media accounts, screenshots, telephone numbers and payment records can help reconstruct recruitment and exploitation. Yet this evidence can disappear rapidly.

For frontline organisations, this creates an important challenge: how should a social worker, psychologist or Mobile Unit professional respond when a survivor's phone contains potentially important evidence?

Vatra's experience points to several priorities: stronger digital literacy among frontline professionals, reliable interpretation services, specialised mental-health support, clear procedures concerning digital evidence and faster cross-border cooperation. →

4 Group of Experts on Action against Trafficking in Human Beings. (2025). *Evaluation report: Albania – Fourth evaluation round* (GRETA(2025)05). Council of Europe. https://rm.coe.int/greta-evaluation-report-on-the-implementation-of-the-council-of-europe/1680b65f41

5 United Nations Office on Drugs and Crime. (2024). *Global report on trafficking in persons 2024*. United Nations. https://www.unodc.org/documents/data-and-analysis/glotip/2024/GLOTIP2024_BOOK.pdf

Illustration: Semanche / shutterstock

→ Vatra's caseload over the past three years reflects an increasingly complex reality in which trafficking, migration, technology and violence intersect. For women's specialist services, this means that responses to technology-facilitated trafficking cannot be separated from the broader response to violence against women and girls. Anti-trafficking services and services for women survivors of violence need to work across these traditional boundaries, recognising the continuum of violence experienced by survivors and ensuring that digital, physical, sexual, psychological and economic forms of abuse are addressed together. We also need to ask ourselves: Are our protection systems adapting as quickly as the methods used by traffickers?

Technology may change the methods of recruitment and control, but the principle guiding our response remains unchanged: survivors need accessible, specialised and survivor-centred support. Behind every message, online advertisement or digital profile connected to trafficking is a person whose trust has been exploited. ●

Brikena Puka is the Executive Director of the Psycho-Social Center 'Vatra' in Albania. She has extensive experience in combating trafficking in human beings and violence against women and girls, as well as in survivor protection, reintegration and advocacy.

Oliana Manaj works at the Psycho-Social Center 'Vatra', contributing to its specialised assistance and reintegration programme for victims of trafficking and survivors of gender-based violence.

Abuse in the Digital Age:

How We Respond to the Emerging Threats Facing Women and Girls

Kiera Brodie, Refuge,[1] England (UK)

Like many countries across the globe, the UK is currently facing alarming rates of violence against women and girls. At a time when almost every aspect of our lives is mediated by online spaces – from the way we socialise to our dating lives – it is no surprise that much of this horrific abuse is now facilitated by technology. From non-consensual intimate image abuse and AI chatbots that enable abuse to stalking and harassment on social media, the scale of the problem is vast and unrelenting. In a domestic abuse context, perpetrators are increasingly using technology to extend the web of coercive control they exercise over survivors. While Refuge played a key role in securing stronger protections for survivors through the Online Safety Act and Ofcom's violence against women and girls guidance, significant gaps in legislation and enforcement mean that survivors continue to experience abuse on an unprecedented scale. This is why specialist support services are vital, and why practice and regulation must keep pace with incredibly fast-evolving harms.

As the UK's largest domestic abuse charity, Refuge has been pioneering efforts to tackle technology-facilitated abuse since 2017, when it launched the only specialist service dedicated to supporting survivors experiencing complex technology-facilitated and economic abuse. Since then, Refuge's specialist team has continued to evolve in direct response to the emerging and increasingly complex harms faced by survivors.

Demand for this specialist support has grown year on year. Earlier in 2026, Refuge released data showing a staggering 78% increase in referrals for technology-facilitated and economic abuse.[2] Between April 2025 and March 2026, there were 967 referrals to Refuge's specialist Technology-Facilitated Abuse and Economic Empowerment (TFAEE) team, compared with 542 between April 2024 and March 2025, marking a substantial jump.

In part, this increase reflects growing awareness of technology-facilitated abuse among survivors, professionals and the wider public. High-profile public advocacy, including Refuge's successful campaign around the

1 Refuge: https://refuge.org.uk/

2 Refuge. (2026). Refuge data reveals 78% rise in tech and economic abuse referrals, including rising cases involving car finance. https://refuge.org.uk/news/refuge-data-reveals-78-rise-in-tech-and-economic-abuse-referrals-including-rising-cases-involving-car-finance/

Phone displaying Refuge's freephone, 24-hour National Domestic Abuse Helpline (+44) 0808 2000 247

Photo: Refuge

→ Online Safety Act,[3] has played an important role in raising awareness – alongside the invaluable work of survivors, organisations across the sector, and dedicated policymakers and journalists. The TFAEE team also trained over 4,000 people in the last financial year alone. At the same time, what the data shows us is just the tip of the iceberg. We know first-hand that many cases of abuse continue to go unidentified and unreported.[4]

In our experience, almost all cases of domestic abuse now involve some component of tech abuse, and many involve several forms – all of which contribute to the perpetrator's wider web of power and control. As technology becomes exponentially more sophisticated, and increasingly embedded in our everyday lives, we frequently hear from survivors who are being subjected to extensive systems of surveillance, both in the home and beyond.

Drawing directly on insights from our frontline services, Refuge continues to highlight how emerging technologies can be weaponised by perpetrators. In January 2025, our organisation sounded the alarm about the growing use of wearable technology and AI to facilitate abuse, including perpetrators tracking survivors through smartwatches and covertly filming without consent using smart glasses.[5]

Later that year, we also raised concerns about the rise of 'spycam' surveillance, which typically involves perpetrators using hidden cameras disguised as everyday household objects to secretly film and photograph survivors.[6] Again, this rarely happens in isolation. Hidden camera surveillance – like other forms of tech abuse – is nearly always part of a wider pattern of coercive control, with devastating consequences. If a perpetrator sees that a survivor has left the house, for example, they may then demand to know where exactly the survivor has been, and coerce them into not leaving to see other people. In other cases, abusers have threatened to share the footage they have taken.

It is this wider context that makes specialist support so important. Through direct referrals from the Refuge operated National Domestic Abuse Helpline (which increased by over 300% in the last financial year), and referral pathways through our community services, survivors can access specialist advice tailored to the technology-facilitated abuse they are experiencing. Our expert staff are here to empower survivors through safety planning, knowledge-sharing and practical guidance, helping survivors to identify hidden technology and to secure their devices and accounts.

Although press attention around tech-facilitated abuse often focuses on headline-grabbing issues such as deepfakes and AI, at Refuge we know that it is just as critical to focus on tech abuse in all its forms. This is why our expert service providers are equipped to understand not only emerging forms of abuse, but also the impact of compromised iCloud or email accounts, social media hacking and other forms of digital intrusion and harm.

Refuge's TFAEE team also prides itself on operating with the aim of empowering survivors. Technologically disempowering narratives have for too long been the default for support services, with survivors often advised to delete their social media accounts, change their phone number or disconnect from online spaces. Instead, our approach focuses on empowering survivors with the knowledge and tools to use technology safely and stay connected online, placing them at the centre of the process of rebuilding →

3 Online Safety Act 2023, c. 50. https://www.legislation.gov.uk/ukpga/2023/50/contents

4 Refuge. (n.d.). *Survey reveals gaps in nations' awareness of red flags of domestic abuse.* https://refuge.org.uk/news/survey-reveals-gaps-in-nations-awareness-of-red-flags-of-domestic-abuse/

5 Refuge. (2025). *Refuge exposes alarming new patterns of abuse involving wearable technology* [Press release]. https://refuge.org.uk/news/refuge-exposes-alarming-new-patterns-of-abuse-involving-wearable-technology/

6 Refuge. (2025). *Refuge reveals rise in tech abuse including spycam surveillance ahead of UN's 16 Days of Activism.* https://refuge.org.uk/news/refuge-reveals-rise-in-tech-abuse-including-spycam-surveillance-ahead-of-uns-16-days-of-activism/

→ their lives free from abuse. We are also clear that while technology may facilitate abuse, it is a perpetrator's choice to abuse, and accountability must always lie with them.

Another critical part of Refuge's service provision is an embedded commitment to intersectional approaches. Time and again, we see how certain marginalised groups experience harms that are compounded by other aspects of their identity and discrimination. For example, in the context of intimate image abuse, for someone who is Muslim, an 'intimate' image might include an image of them without a headscarf or showing their shoulders.[7] Yet UK legislation does not always recognise this, even though the impact of this violation can be just as severe for survivors. Recognising this is essential to understanding the full extent of harm and ensuring that survivors receive care and support that is responsive to the different forms of discrimination and inequality they may face.[8]

Research also suggests that Black women experience disproportionately high rates of online abuse.[9] Despite this, pervasive racism and the adultification of young Black girls can mean that the abuse they experience is taken less seriously. Survivors in the LGBTQ+ community are also uniquely impacted by image-based abuse, and the associated harms can include being outed without consent. Technology-facilitated stalking can also be heightened in cases of so-called 'honour'-based abuse. These situations often involve multiple perpetrators, meaning survivors can be subjected to particularly high levels of surveillance, increasing the risks they face.

Together, these examples demonstrate why an intersectional approach is essential to understanding and responding effectively to technology-facilitated abuse.

Access to culturally competent specialist support for technology-facilitated abuse can be life-saving. This is why Refuge continues to campaign for increased funding for specialist services,[10] while also working with organisations across the sector and parts of the criminal justice system to share core knowledge through expert-led training based on survivor insights. Through just one Home Office funded Tech Partnership Initiative, the TFAEE team trained over 500 staff across five key sector organisations, including Galop, SignHealth and Karma Nirvana. But specialist support and training are only one part of the picture. We also need to ensure that survivor voices and experiences are used to shape the wider systems, policies and technologies that determine their safety.

Recently, insights from survivors and specialist services such as Refuge fed into an online safety coalition that launched a new Safety by Design Code of Practice,[11] which sets out clear, practical steps that online services can take to protect their users from the outset. Refuge also strives to stay ahead of emerging threats by proactively researching the digital landscape and hosting focus groups on everything from the manosphere and online gaming to AI chatbots. This helps ensure that the experiences and expertise of survivors, their communities and their families remain at the heart of how we understand emerging harms and develop responses to them.

Ultimately, meaningful progress in tackling tech-facilitated abuse depends on joined-up action. The expertise and pioneering approaches of specialist services must be matched by a clear Government strategy for tackling technology-facilitated abuse, backed by survivor-centred, enforceable regulation and a commitment to tackling online violence against women and girls proactively. Without this coordinated approach, women and girls will continue to bear the cost of a digital world that was never designed with their safety in mind. ●

Kiera Brodie joined Refuge in 2024 as Tech Abuse Training Lead for its Technology-Facilitated Abuse and Economic Empowerment (TFAEE) team. In her role, she delivers accredited training packages for charitable and for-profit organisations to improve recognition of 'tech and economic abuse' nationally. With a background in the homelessness and violence against women sectors, she specialises in sexual exploitation, harm reduction, and trauma-informed practice, drawing on years of frontline experience to educate and empower professionals to better understand emerging harms.

7 Waheed, A. (2025). For Muslim women, images of us without our hijabs can be as damaging as nude photos. Glamour UK. https://www.glamourmagazine.co.uk/article/muslim-women-image-based-abuse-hijab

8 Glitch. (n.d.). Non-criminal redress for intimate image abuse victim-survivors. https://glitchcharity.co.uk/our-work/non-criminal-redress

9 Glitch. (2023). Digital misogynoir report. https://glitchcharity.co.uk/our-work/research-digital-misogynoir-report

10 Refuge. (2026). Refuge takes 'Home Is Where the Hurt Is' campaign to the Houses of Parliament. https://refuge.org.uk/news/refuge-takes-home-is-where-the-hurt-is-campaign-to-the-houses-of-parliament/

11 Online Safety Act Network. (2026). Safety by design Code of practice. https://www.onlinesafetyact.net/documents/1684/Safety_by_Design_-_Code_of_Practice.pdf

Translating Survivor Knowledge into Political Power:

Building Feminist Alliances for Violence-Free Digital Futures

Elizabeth Ávila González, bff – German Federal Association of Rape Crisis Centres and Women's Counselling Centres,[1] Germany

Technology-facilitated gender-based violence has entered mainstream public debate in Germany, amplified by the case of German presenter and public figure Collien Fernandes and growing attention to deepfakes, platform responsibility and legal gaps.[2] This attention matters. But it also raises a fundamental question: What does digital safety mean – and whose knowledge shapes it?

Much of the debate focuses on technical and legal fixes. These measures are relevant, but they are not sufficient. From a feminist perspective, technology-facilitated gender-based violence is a continuation and extension of gender-based violence into digital spaces. Technologies change how violence is perpetrated, multiplied and sustained – from monitoring (ex-) partners and distributing intimate images to impersonation and access to private data. But the underlying power relations remain deeply rooted in existing social inequalities.

This means that digital safety cannot be defined by tech companies alone. Our four years of project work and platform monitoring[3] show how narrowly digital safety is often defined by Big Tech: what can be technically detected, categorised and moderated at scale takes priority over the social, relational, and gendered contexts in which violence occurs. Seemingly ordinary digital practices can become tools of coercive control, stalking, or sexualised violence, depending on context.

So, whose knowledge is needed to answer what digital safety should actually mean? Women's specialist services have spent decades understanding violence as patterns embedded in social structures. They know why small digital interventions can have major consequences for safety, and why removing content does not necessarily end the violence. Yet this is still too rarely recognised as expertise in tech governance. Feminist organisations are often expected to perform the invisible labour of digital safety: documenting abuse, supporting survivors, identifying platform failures, and translating lived experiences into policy.

But asking this question also reveals the limits of our own fields. Technology-facilitated gender-based violence is not only a gender equality issue. It is also a question of digital rights, platform regulation, cybersecurity, law and fair digitisation. No single sector holds all the answers. If we want different digital futures, we have to ask these questions together.

This became the starting point for the *Digital Futures Gathering – Thriving Futures for All*,[4] where activists, researchers, digital rights organisations, and women's organisations from across Europe imagined violence-free digital futures. Asking 'what kind of digital future do we want to build together?' was not an exercise in optimism. For feminist movements, imagining alternatives is political work: it challenges the assumption that existing systems are inevitable and opens space for new alliances and forms of accountability. →

1 Bundesverband Frauenberatungsstellen und Frauennotrufe: https://www.frauen-gegen-gewalt.de/de/aktuelles.html

2 Deutsche Welle. (2026, March 20). *Germany to target pornographic deepfakes amid celebrity case.* DW. https://www.dw.com/en/germany-to-target-pornographic-deepfakes-amid-celebrity-case/a-76457460

3 bff. (2026). *Platform regulation must prioritise protection against violence: Platform monitoring with a focus on Articles 12, 16, 34 and 35 of the DSA* [Policy paper]. https://www.frauen-gegen-gewalt.de/de/studien-und-positionspapiere/policy-paper-on-the-digital-services-act-and-digital-gender-based-violence.html

4 SUPERRR Lab. (2025, October 16). *A throwback to two days of inspiration, care, joy, gratitude, and hope.* https://superrr.net/en/blog/digital-futures-gathering-thriving-futures-for-all

Group picture of the Digital Futures Gathering

Photo: Jacqueline Mayen

→ In the workshop *'Translating Hope into Policy'*, we explored what it takes to move from shared visions to political strategy. One answer was clear: collaboration is not an addition to political work; it is part of the strategy itself. Bringing together different forms of expertise can reveal where responsibility lies, which questions have not yet been asked, and where collective action can create change.

This approach led to a new alliance between CDT Europe,[5] the Women's NGOs Cooperation Network of Latvia,[6] and the bff. By combining digital rights, feminist advocacy and specialist support expertise, we are mapping relevant policy actors in the field of technology-facilitated gender-based violence – not simply to create an inventory, but to understand where power lies and where alliances can be built to enable political change. The tool is planned for public presentation in spring 2027.

The same approach informs the bff's work on the Digital Services Act (DSA). During the Digital Futures Gathering, we hosted a workshop on Article 16 DSA and platform reporting mechanisms. Instead of asking only how reporting interfaces should function, participants asked what access to justice requires: Who can use these mechanisms? What barriers do they create? Whose experiences are recognised and whose are rendered invisible?

Together with international experts, we developed feminist recommendations for reporting mechanisms that use plain language, minimise barriers, provide multiple channels, and avoid unnecessary data collection. They should incorporate trauma-informed communication and be developed with survivors and violence prevention experts. Survivors and specialist organisations should not simply use digital safety systems; they should help shape them. The recommendations are also included in our DSA policy paper.[7]

Our cooperation with HateAid[8] has similarly shown how individual experiences can become a basis for collective action. Together, we filed complaints against seven major platforms with Germany's Digital Services Coordinator,[9] focusing on the absence of Single Points of Contact (SPOCs) required under Article 12 DSA. Rather than treating these as isolated failures, we used the complaints to document a systemic problem and demand accountability.

Our work points to a broader lesson: building violence-free futures begins with asking better questions – and recognising that we cannot answer them alone. Feminist expertise is essential, but so are digital rights, cybersecurity, legal and technical expertise, and, above all, the knowledge of those experiencing violence.

5 Center for Democracy and Technology Europe: https://cdt.org/eu/

6 Women's NGOs Cooperation Network of Latvia: https://sadarbibastikls.lv/

7 bff. (2026). *Platform regulation must prioritise protection against violence: Platform monitoring with a focus on Articles 12, 16, 34 and 35 of the DSA* [Policy paper]. https://www.frauen-gegen-gewalt.de/de/studien-und-positionspapiere/policy-paper-on-the-digital-services-act-and-digital-gender-based-violence.html

8 HateAid: https://hateaid.org/

9 bff. (2026, February 17). *Digitale Gewalt gegen Frauen: bff und HateAid reichen Beschwerde gegen Plattformen ein* [Digital violence against women: bff and HateAid file complaint against platforms] [Press release]. https://www.frauen-gegen-gewalt.de/de/ueber-uns/presse/pressemitteilungen/pm/pressemitteilung-bff-hateaid-ggmbh.html

Collective imagination becomes political power when it creates the relationships needed to act: when different movements share knowledge, challenge platforms together and bring survivor expertise into spaces where digital governance is shaped. A violence-free digital future will not emerge from making existing systems slightly safer. It requires building new infrastructures and systems grounded in autonomy, equality and freedom from violence.

And this very future will not be built for us. It has to be built by us – *together.*

Elizabeth Ávila González is a jurist specialising in international and European law. She works on the project 'Aktiv gegen digitale Gewalt' ('active against digital violence') at the bff, the German Federal Association of Rape Crisis Centres and Women's Counselling Centres (Bundesverband Frauenberatungsstellen und Frauennotrufe). The bff is the German umbrella organisation for women's counselling centres and rape crisis centres. It advocates for the rights and safety of women and girls affected by gender-based violence, supports specialist counselling services, and works to improve prevention, legislation and public awareness. Through this project, the bff also addresses emerging forms of violence, including technology-facilitated gender-based violence, and brings the expertise of specialist support services into policy and technology debates.
Elizabeth's work focuses on technology-facilitated gender-based violence, platform regulation, digital self-determination, and intersectional queer-feminist approaches to tech governance.

Research for **Feminist Advocacy**

Use WAVE's expert publications to strengthen women's organisations and advance a Europe free from violence against women and girls

- **Advocate** for sustainable funding for women's specialist services
- **Hold** governments and EU institutions **accountable** to Istanbul Convention standards
- **Challenge** gender-neutral approaches that weaken specialist support
- **Strengthen** feminist, survivor-centred policy responses

Scan to access WAVE's publications

The WAVE Network currently comprises over 190 members (autumn 2026) in 46 European countries. For an updated list go to
https://wave-network.org/members-network/members-list/

wave-network.org

facebook.com/womenagainstviolenceeurope

instagram.com/womenagainstviolenceeurope

linkedin.com/company/women-against-violence-europe

bsky.app/profile/wave-network.bsky.social