COLLECTING DATA ON TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN: CHALLENGES AND WAYS FORWARD

Council of Europe project
"Combating digital and sexual violence against women in Bosnia and Herzegovina II"

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Cover design and layout:
art studio DK

Picture
© Shutterstock

Council of Europe
F-67075 Strasbourg Cedex
www.coe.int

COLLECTING DATA ON TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN: CHALLENGES AND WAYS FORWARD

Prepared by
Rosanna Amato

November 2025

Council of Europe

Table of contents

GLOSSARY AND ACRONYMS

BDVD	Domestic Violence Database
BDVMVD	Database on Violence Against Women and Domestic Violence
CCTV	Closed-Circuit Television
CIG	Comissão para a Cidadania e a Igualdade de Género
EIGE	European Institute for Gender Equality
EU	European Union
FGM	Female Genital Mutilation
GBV	Gender-Based Violence
GPS	Global Positioning System
GREVIO	Group of Experts on Action against Violence against Women and Domestic Violence
HiNBG	Hass-im-Netz-Bekämpfungsgesetz
KoPI-G	*Kommunikationsplattformen-Gesetz*
ICT	Information Communication Technology
LBTI	Lesbian, Bisexual, Transgender And Intersex
LOMPVIG	Ley Orgánica de Medidas de Protección Integral contra la Violencia de Género
MARACs	Multi Agency Risk Assessment Conferences
NGOs	Non-Governmental Organisation
OTFVAW	Online and Technology Facilitated Violence Against Woman
SGMAI	Secretaria-Geral do Ministério da Administração Interna
UN	United Nations
WHO	World Health Organisation

EXECUTIVE SUMMARY

Introduction

This study delves into the pivotal role of data collection systems in the fight against gender-based violence (GBV), exploring how these systems are designed, developed, and adapted to address both traditional and emerging forms of violence. The work highlights the complexities involved in conceptualising and categorising online and technology-facilitated violence against women (OTFVAW), as well as the gaps in existing legal and institutional responses that hinder effective data gathering. By framing the challenges of GBV data collection within the broader context of rapidly evolving digital abuse, the study emphasises how reliable, disaggregated data is indispensable for shaping informed policies and interventions. Case studies of Austria, Spain, and Portugal demonstrate how countries with different starting conditions and resources can adapt their frameworks to build systems that meet shared goals, underscoring the importance of flexibility, innovation, and harmonisation in tackling violence against women in all its forms.

Problem statement

Technology has significantly transformed the landscape of GBV, introducing new opportunities for abuse through social media, messaging platforms, and tracking systems. However, data collection systems often fail to capture the complexities of this evolving violence, particularly its intersection with traditional forms. Inconsistent legal frameworks and fragmented data collection efforts hinder a comprehensive understanding of the prevalence and impact of both physical and digital violence, leaving policymakers without the tools necessary for effective intervention. Marginalised groups, including LBTI individuals and women with disabilities, are particularly underrepresented in existing data, further compounding these challenges.

Key findings

Chapter I outlines the complex, multidimensional nature of OTFVAW, examining its manifestation, legal challenges, and the difficulties of conceptualising and categorising this evolving form of gender-based violence. It begins by highlighting how technology reshapes human interactions, creating opportunities for abuse through platforms such as social media, messaging tools, and tracking systems, extending traditional gender-based violence into the digital realm.

A key emphasis is on the continuum of violence—the blurred boundaries between online and offline violence, where acts such as cyberstalking, gendertrolling, and image-based sexual abuse amplify and extend traditional forms of abuse. Additionally, it examines the intersectional impacts of online abuse, focusing on how women of different backgrounds (such as LBTI or minority women) face compounded effects.

Legal frameworks are struggling to keep pace with technological developments, and national responses remain fragmented, with inconsistent laws across countries. Many states do not specifically regulate forms of digital violence, often subsuming it under broader gender-neutral legislation. The patchwork of legal responses limits effective data collection and policymaking, hindering comprehensive protections for victims.

Finally, the chapter explores the urgent need for harmonised definitions and frameworks to address this conduct effectively. It emphasises that coordinated international and national efforts are essential to develop robust legal tools and data systems that can tackle the rapidly evolving nature of digital violence, particularly as set out in instruments like the Istanbul Convention.

Chapter II provides an examination of the data gaps surrounding OTFVAW, with an emphasis on how the lack of comprehensive, reliable data impedes the ability to design, implement, and monitor effective policies. The chapter begins by stressing the critical role that data plays in decision-making and accountability, noting that while significant progress has been made in addressing violence against women, technology-facilitated violence remains underreported and poorly understood due to the absence of systematic data collection efforts.

A major theme in the chapter is the fragmentation of legal frameworks across different countries, where inconsistent definitions of OTFVAW hinder the collection of comparable and gender-disaggregated data. It underscores how this lack of uniformity makes it difficult to measure the true prevalence of this conduct and develop evidence-based policies to combat it.

The chapter also discusses the intersectional nature of OTFVAW, noting that marginalised groups, including ethnic minorities, LBTI individuals, and women with disabilities, are particularly vulnerable but often underrepresented in data collection efforts. The failure to include these groups in surveys and studies further skews the understanding of digital violence's impact.

The Istanbul Convention's Article 11 is highlighted as a key framework for improving data collection on violence against women, including OTFVAW. This article sets out obligations for governments to systematically collect and publish disaggregated data, as well as to conduct population-based surveys that can capture the full scope of violence, including its digital dimensions.

The chapter concludes by acknowledging that despite growing awareness of this phenomenon, challenges such as privacy concerns, the transborder nature of digital platforms, and underreporting continue to limit the ability to collect accurate, comprehensive data. It calls for greater international cooperation and the development of harmonised definitions and methodologies to close these data gaps, ensure victim privacy, and enhance legal responses to online violence.

Chapter III explores the evolution and distinct approaches to data collection on GBV, with a focus on Austria, Spain, and Portugal. It highlights the varying national frameworks that respond to the diverse and growing forms of violence against women, including physical and digital violence. While none of the discussed systems are specifically designed to address OTFVAW, they reflect a growing recognition of technology-facilitated violence and are adapting to meet new European Union directives on domestic and gender-based violence.

The aim is to show how, in spite of differing starting conditions—shaped by their legal traditions, policy priorities, and institutional capacities—these countries demonstrate how systems can be adapted to respond to the shared need for comprehensive data collection in the fight against GBV, including OTFVAW. Despite gaps and challenges, these systems illustrate how diverse approaches can align with broader European goals, particularly in addressing emerging forms of OTFVAW.

In Austria, data collection on GBV has traditionally been integrated into general criminal justice systems, where police and judicial data are collected separately and often focus on broad crime categories. Over the past decade, legislative advancements such as the Violence Protection Act 2019 and the Hate Prevention Act have created a clearer foundation for addressing OTFVAW, which in turn has shaped data collection priorities. These laws introduced specific criminal categories, such as cyberbullying and unauthorised image sharing, allowing these offences to be systematically recorded in police and judicial databases. While challenges remain—particularly in aligning police and justice data for seamless case tracking—Austria has made significant strides in improving data granulari-

ty. For example, its systems now capture victim-offender relationships more systematically, an essential step for understanding the dynamics of violence. These incremental adaptations reflect Austria's broader approach: leveraging existing frameworks to progressively address new forms of violence, even when starting from a generalist system.

Spain offers a different example with its highly specialised *VioGén* system, which was specifically designed to monitor and address intimate partner violence. Originating from the *Organic Law 1/2004* on gender-based violence, this system collects detailed, disaggregated data from law enforcement, judicial bodies, and victim support services. Each case in *VioGén* represents a specific victim-offender relationship, allowing for tailored risk assessments and real-time monitoring. While initially focused on physical violence in intimate relationships, the system is expanding (and can be further expanded) to incorporate OTFVAW as addressed in recent legislative reforms. Spain's system exemplifies a compartmentalised yet integrated approach, where specialised courts, cybercrime units, and public campaigns work in tandem to address GBV. By expanding its data collection scope to include femicide categories and other forms of violence, Spain demonstrates how a focused system can evolve to capture a more comprehensive picture of GBV, building on its initial strength in tracking intimate partner violence.

Portugal is currently transitioning to an advanced, integrated system that reflects its ambition to address GBV in a holistic manner. The forthcoming *Database on Violence Against Women and Domestic Violence (BDVMVD)*, set to replace the existing *BDVD* in 2025, represents a significant leap forward. Unlike the earlier system, which primarily captured police data, the new database will integrate information from multiple sources, including law enforcement, judicial systems, victim support networks, and public health services. This integration is guided by recent legislative reforms, such as the *Charter on Human Rights in the Digital Age,* which emphasise the importance of addressing cyber violence and ensuring data interoperability across sectors. By centralising and standardising data collection, the *BDVMVD* will enable more detailed tracking of cases, risk assessments, and interventions, offering a model for how even fragmented starting conditions can evolve into a comprehensive system.

Together, these three countries illustrate that while the starting conditions and approaches to data collection differ, they all work toward the shared goal of improving responses to GBV. Austria builds incrementally on its generalist systems, adapting them to new challenges through legal and institutional adjustments. Spain's specialised framework shows how a dedicated system can evolve to ad-

dress broader forms of violence while maintaining its focus. Portugal's comprehensive, integrated approach highlights the possibilities of creating a unified system that brings together diverse data sources to meet complex needs. These examples underscore the adaptability of data systems and the potential for progress, demonstrating that with commitment and innovation, countries can move toward robust data-driven solutions regardless of their initial conditions.

Implications

Comprehensive data collection systems are critical for addressing the growing challenges posed by GBV, particularly its digital dimensions. By adapting systems to meet new forms of violence, countries can better align with European and international directives, improve victim protection, and develop evidence-based policies. Austria's incremental approach, Spain's specialised framework, and Portugal's integrated model demonstrate that despite differing starting points, progress is possible through innovation and commitment.

Conclusions

Technology has significantly transformed gender-based violence, extending abusive behaviours into digital spaces and amplifying harm through new forms of abuse such as cyberstalking, image-based sexual exploitation, and online harassment. These acts often target victims based on intersecting identity markers, exacerbating their impact on marginalised groups. The intertwined nature of online and offline violence complicates efforts to define and address these phenomena comprehensively, highlighting the need for a continuum-based understanding.

Despite progress in raising awareness and addressing these issues through international frameworks like the Istanbul Convention, major barriers persist. The absence of harmonised definitions, standardised methodologies, and comprehensive data systems limits the ability to measure and address the prevalence and impact of OTFVAW accurately. Current systems often fail to capture emerging forms of abuse, transnational dimensions, or intersectional experiences, leaving vulnerable groups underrepresented. National data systems vary significantly in their scope and design, with promising but fragmented practices across Europe. To combat OTFVAW effectively, integrated, inclusive, and robust data collection frameworks are urgently needed.

Recommendations

To effectively address OTFVAW, it is crucial to establish harmonised definitions and standardised methodologies that reflect the evolving nature of OTFVAW. Legal frameworks must explicitly recognise OTFVAW, enabling consistent data collection and tailored responses. National data systems should integrate disaggregated data to capture intersectional vulnerabilities and emerging forms of violence while fostering international collaboration to address the transnational nature of online abuse. Leveraging technology such as AI can enhance data analysis and predictive capabilities, while victim-centred, privacy-conscious approaches will ensure secure and inclusive data collection. Multi-sectoral collaboration and regular surveys should complement these efforts, supported by public awareness campaigns and transparent reporting to promote accountability and evidence-based policymaking.

CHAPTER I

THE DYNAMICS OF ONLINE AND TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN: LEGAL CHALLENGES, CONCEPTUAL GAPS, AND THE CONTINUUM OF ABUSE

The Istanbul Convention and the online and technology-facilitated violence against women

The Istanbul Convention is a comprehensive treaty that establishes a wide range of obligations for effectively addressing violence against women and domestic violence in all its forms. It mandates proactive measures to prevent violence, protect victims, and prosecute perpetrators. Furthermore, it requires state parties to adopt an integrated policy framework, ensuring a holistic approach with clearly defined roles and responsibilities for various agencies and institutions at the national level.

This Convention sets forth a robust and detailed set of legally binding standards, making it the most far-reaching treaty in this domain to date. It explicitly defines violence against women as both a human rights violation and a form of gender-based discrimination, encompassing "all acts of gender-based violence

against women that result in, or are likely to result in, physical, sexual, psychological, or economic harm or suffering to women, including threats of such acts, coercion, or arbitrary deprivation of liberty, whether occurring in public or private life." Domestic violence is similarly defined as "all acts of physical, sexual, psychological, or economic violence occurring within the family or domestic unit, or between former or current spouses or partners, regardless of whether the perpetrator shares or has shared the same residence with the victim." The Convention emphasises that domestic violence is predominantly a gendered phenomenon.

The Convention's holistic definitions, which include psychological and economic harms, are especially pertinent in addressing the digital dimension of such violence. Article 4, paragraph 3, underscores that the Convention must be implemented "without discrimination on any ground."

Although the Convention does not explicitly address the digital dimension of violence against women, the Explanatory Report[1] accompanying it acknowledges this aspect, including digital stalking. In 2021, GREVIO (the Group of Experts on Action against Violence against Women and Domestic Violence) built on this foundation by issuing its first General Recommendation N. 1 on the Digital Dimension of Violence Against Women. This recommendation clarifies how the Istanbul Convention applies to online and technology-facilitated violence, highlights the intertwined nature of online and offline abuse, and provides state parties with practical recommendations.

In the General Recommendation, GREVIO defines the digital dimension of violence against women as encompassing both online and technology-facilitated harmful behaviors targeting women and girls. Online violence includes actions and data available on the internet—whether on the surface web or dark web—while technology-facilitated violence involves harmful behaviours executed via technological tools such as communication devices, hardware, and software (GREVIO, 2021). This terminology underscores how such violence disproportionately targets women and girls, framing it as a central component of their experiences with gender-based violence.

The digital dimension of violence against women spans a wide array of harmful acts conducted online or via technology. These acts constitute part of the broader continuum of gender-based violence that women and girls endure,

1 Council of Europe Treaty Series - No. 210, Explanatory Report.

including within the domestic sphere. Such digital violence is equally harmful as offline violence and should be recognized as a legitimate manifestation of gender-based abuse.

In treating the digital dimension as a distinct but not separate aspect of violence against women, GREVIO's interpretation aligns with the victim-centred approach envisioned by the drafters of the Istanbul Convention. This approach deliberately avoids creating a dichotomy between online and offline experiences of gender-based violence. For instance, the Explanatory Report treats stalking in the digital sphere as merely another form of stalking, illustrating the interconnectedness of these forms of abuse.

The Istanbul Convention and its role in collecting disaggregated and relevant statistical data

Knowledge is crucial for developing effective policies to prevent and combat violence against women and domestic violence. The systematic development of knowledge equips policymakers and civil society with the tools to assess progress and refine strategies. In this context, effective data collection plays a pivotal role.

Comprehensive data collection and research are essential for designing policies and measures that protect and support victims while addressing the root causes of violence. Furthermore, they are vital for evaluating the effectiveness of existing policies aimed at prevention and intervention. To ensure meaningful outcomes, information provision must adopt an integrated approach that reflects practical developments. Systematic and adequate data collection has long been recognised as a cornerstone of effective policymaking in this domain. However, despite this recognition, examples of systematically collected administrative or population-based data within Council of Europe member states remain scarce. Moreover, the available data are often not comparable across countries or over time, limiting the understanding of the scope and evolution of the issue. Addressing violence against women and domestic violence requires evidence-based policymaking, which necessitates robust, comparative data to document the scale of violence and guide the formulation and implementation of policies.

The Istanbul Convention emphasises the importance of data collection and research in combating violence against women and domestic violence. Article 11

of the Convention specifically obliges state parties to collect disaggregated and relevant statistical data and to support research within its scope. The Convention mandates that parties regularly gather and make publicly available disaggregated statistical data on all forms of violence covered by its provisions. Population surveys should also be conducted to assess the prevalence and trends of such violence. Furthermore, state parties are encouraged to support research examining the root causes and consequences of violence, incidence rates, conviction rates, and the effectiveness of measures implemented under the Convention.

As far as data for statistical purposes are concerned, the Explanatory Report to the Convention elucidates the dual nature of these obligations. First, evidence-based policies require regular collection of disaggregated statistical data on all forms of violence within the scope of the Convention. Such data not only raise awareness among policymakers and the public about the gravity of the issue but also encourage victims and witnesses to report incidents. Accurate administrative and judicial data can significantly enhance national responses to violence by informing on the performance of governmental institutions and the nature of crimes addressed through criminal procedures. Additionally, service utilisation data from agencies can help assess policy effectiveness and estimate administrative costs. Judicial data further provide insights into sentencing patterns, the characteristics of convicted individuals, and conviction rates.

To meet these obligations, public authorities—such as the judiciary, police, and social welfare services—must establish data systems that extend beyond internal agency records. The utility of such data hinges on its quality. While the Convention allows state parties flexibility in defining data categories, it sets minimum requirements. Data should be disaggregated by key factors, including sex and age of victims and perpetrators, type of violence, relationship between victim and perpetrator, geographical location, and additional relevant factors, such as disability.

Moreover, data should encompass conviction rates, the number of protection orders issued, and other critical metrics to monitor the response to all forms of violence covered by the Convention.

The Istanbul Convention also requires Parties to support research and conduct population-based surveys to inform evidence-based policies on violence against women and domestic violence. Research is essential for understanding root causes, effects, incidence rates, and the effectiveness of implemented measures, thereby improving responses by the judiciary, law enforcement, and support services.

What do we talk about when we talk about online and technology-facilitated violence against women?

Technology has fundamentally reshaped human interaction, transcending the constraints of physical communication, with undoubtedly significant benefits associated with this progress[2]. However, alongside these advancements, it has introduced a variety of risks and challenges, particularly in the context of gender-based violence, with a notable impact on women and girls[3]. Rather than simply facilitating communication, learning and socialisation, technology has intensified and extended various forms of violence by creating digital environments where abusive behaviours can flourish.

Online environments have facilitated the transfer of traditional abusive dynamics into the digital realm and provided offenders with new powerful tools to perpetuate or escalate interpersonal violence, regardless of geographical proximity[4].

Expressions of misogynistic hatred

In recent years, social networks have increasingly become stages where the expression and amplification of misogynistic hatred not only occurs but is disturbingly easy to propagate, while messaging tools offer effortless means to reinforce this hostility through threats and intimidation[5]. Misogynistic hatred has grown so pervasive and widespread that it is almost normalised[6], with varied expressions of intolerance directed at women simply because of their gender, often exacerbated by intersecting factors such as race, age, disability, sexuality, or ethnicity, further intensifying the abuse[7]. Behaviours such as the spread of gender-based hostility, the justification of harmful attitudes, and the circulation of violent content that objectifies and degrades women are now commonplace, as is content that portrays women as legitimate targets of violence. The perpetrators exploit the anonymity of the Internet to launch attacks with little fear of accountability, thereby exacerbating the harm inflicted upon those affected.

2 Diamandis & Kotler, 2020
3 King, 2017; Afrouz, 2023
4 Duerksen & Woodin, 2019; Fernet et al., 2019; Fraser et al., 2010; Yardley, 2020
5 Tirocchi, Scocco & Crespi, 2022
6 Gius, 2023
7 Pérez-Tirado et al., 2024.

A particularly virulent form of online gender-based hatred is 'gendertrolling',[8]. Gendertrolling involves gender-specific insults and hostile language, often escalating into alarming practices such as 'doxxing', whereby the victim's personal information is publicly disclosed, exposing them to further harassment or physical danger, and even credible threats[9]. These attacks are frequently prolonged and coordinated across multiple individuals or platforms[10].

One particularly destructive feature of gendertrolling is its tendency to target women who publicly address contentious issues, such as sexism, engage in political discourse, or challenge entrenched social norms[11]. Such attacks are not only designed to undermine the image and personal credibility of the women targeted but also to discredit the causes they champion, including gender equality, sexual and reproductive rights, LBTI inclusion, and democratic values[12]. By attacking these advocates, gendertrolling seeks to silence them and destabilise the progressive movements they represent[13].

Conducts violating individual sexual integrity

Online forms of violence against women can transcend mere verbal expressions of hatred and intolerance, manifesting in deeply disturbing forms that violate the **sexual integrity** of victims for the perpetrator's gratification, even while evading traditional notions of physical violence. Such behaviour often involves the exploitation of images—whether of known or unknown individuals—acquired, used and shared without their consent.

A significant dimension of this phenomenon is the growing variety of behaviours that fall under the concept of **'digital voyeurism'**, now enabled by a combination of factors. On the one hand, the miniaturisation of digital technology and the ubiquitous availability of recording devices, particularly mobile phone cameras, facilitate covert surveillance and the surreptitious capture of so-called 'upskirt' and 'downblouse' images.[14] On the other hand, these still or video images can be effortlessly reproduced and disseminated across the internet, rendering them effectively irretrievable. Such distribution might occur on personal websites created by

8 Paananen & Reichl, 2019.
9 Mantilla, 2013.
10 Bainotti & Semenzin, 2021; Dunn, 2020; Garrido, 2022; Tirocchi, Scocco & Crespi, 2022.
11 Gurumurthy & Dasarathy, 2022; Paananen & Reichl, 2019; Bainotti & Semenzin, 2021.
12 Gurumurthy & Dasarathy, 2022.
13 Dunn, 2020; Garrido, 2022. See also IT for Change Project.
14 Lewis & Anitha, 2023.

voyeurs, on image-sharing platforms, or via any of the numerous adult voyeuristic websites that offer a ready market for this type of content[15].

It should also be noted that this type of violation does not only affect "unknown" women, who have been stolen of their images in public places, such as locker rooms or while sunbathing. Victims of digital voyeurism and other forms of cyber-enabled sexual violence may be people in the perpetrator's circle of acquaintances and with whom the perpetrator has familial or emotional relationships.[16]

However, the landscape of **cyber-sexual violence** extends far beyond this. It encompasses an array of behaviours with complex nuances and interconnections, making it tremendously difficult to capture concisely. Besides the various patterns of voyeurism, the digital forms of sexual violence cover a wide range of media and technological misuse, from obnoxious comments and unsolicited advances to more severe violations intended to persecute the victim, exact revenge, or exert power and control. **Non-consensual intimate image distribution**, for instance, is a particularly pernicious and gendered form of sexual abuse whose prevalence has surged with the widespread use of smartphones[17].

This behaviour forms part of the broader 'continuum of non-consensual intimate image distribution, as it involves the non-consensual dissemination of sexually explicit or compromising images on the Internet by individuals who seek to denigrate and humiliate their ex-partner. Often, name, address, or other identifying information is also shared, ensuring that the victim is easily recognisable. Non-consensual intimate image distribution is also a disturbing business. It is estimated that there are around 3,000 websites dedicated to this practice[18] with considerable visitor numbers.

Another pernicious form of image-based sexual abuse is **sextortion**, which is often driven by a desire for dominance and control, with perpetrators using threats to manipulate their victims into fulfilling specific demands—whether it be financial payment, the provision of additional intimate images, or engaging in unwanted sexual acts[19].

15 Clough, 2015.

16 Well-known are the cases of stepfathers who have used devices to spy on adult stepdaughters in private settings or men who have made illicit use of pictures of their intimate partners.

17 McGlynn et al., 2017.

18 DeKeseredy &Schwartz, 2016.

19 Henry & Umbach, 2024; Cross, Holt & Holt, 2023; O'Malley & Holt, 2022; Powell & Henry, 2019; Patchin & Hinduja, 2020; Thorn, 2017.

This form of abuse permeates various contexts, including online dating and financial scams[20]. What is particularly disconcerting, however, is that this behaviour, like many other forms of technology-facilitated sexual abuse, often occurs within romantic or intimate relationships, regardless of the depth or longevity of such ties.

Online and technology-facilitated violence against women violence in the context of intimate relations

The use of technology—whether through media, communication devices, or digital tools—to exert control is deeply intertwined with intimate partner violence (IPV)[21]. At its core, IPV involves a power dynamic where perpetrators use various means to dominate their partners[22], and technology provides an extensive arsenal for reinforcing and amplifying this control. Digital environments, for example, offer perpetrators a platform for harassing and abusing partners or ex-partners with alarming ease and immediacy. Socially networked technologies allow for public humiliation before family, friends, and the wider community[23] while also facilitating verbal abuse, both during the relationship and after its end, to silence, punish, or manipulate the victim. Moreover, intimate photos and videos are often used as tools of blackmail, threatening victims with the prospect of exposure.

A hallmark of digitally-facilitated IPV is the use of technology for monitoring, tracking, and surveillance, which can also be forms of online and technology-facilitated stalking. Mobile phones are frequently weaponised to carry out 'bombarding', where the perpetrator sends an overwhelming number of messages or calls demanding to know the victim's whereabouts, activities, and company. In some instances, women are required to send 'photographic evidence' to verify their responses, with non-compliance often resulting in 'punishments'. Additionally, mobile phones enable abusers to monitor search histories, conversations, and online activities, all in a paranoid quest for 'evidence' of alleged wrongdoings[24]. This control may be covert, but in many cases, the perpetrator openly demonstrates it, making it clear to the victim that their every move is being watched. Attempts to resist this control, such as setting or changing passwords, often lead to escalated abuse, sometimes culminating in physical violence.

20 Cross, Holt & Holt, 2023; Henry et al., 2020; Patchin & Hinduja, 2020; Thorn, 2017.

21 Al-Alosi, 2017; Douglas et al., 2019; Dragiewicz et al., 2018; Duerksen & Woodin, 2019; Freed et al., 2017, 2018, 2019; Henry et al., 2020; Taylor & Xia, 2018.

22 Southworth et al., 2007.

23 Melton, 2007.

24 Bayley et al., 2023.

The urge to control also extends beyond digital monitoring to include actual **surveillance**. This may be social surveillance, such as scrutinising a partner's appearance and interactions on social media, limiting contact with friends and family, or even 'catfishing' to test loyalty[25], but also physical surveillance. Notably, physical surveillance, enabled by accessible technologies like GPS tracking, spyware, and commercially available smartphone apps,[26] is increasingly common[27]. In some cases, victims remain unaware of this surveillance, as these technologies are easily adaptable to secretly monitor intimate partners and perpetrators may install tracking applications without their knowledge[28] or access cloud data to remotely monitor their phone activity. In other cases, victims are forced to disclose their passwords or download monitoring applications, enabling constant surveillance of their movements and social contacts[29].

In addition to surveillance through social networks and communication tools, various technologies now facilitate **home monitoring**, ranging from traditional CCTV cameras, both inside and outside the home, to more advanced and innovative methods like Airtags are being used to stalk partners.

Technological abuse extends beyond mere location tracking and involves tactics that dismantle the physical boundaries of relationships[30], creating an overwhelming sense of helplessness and inescapability for victims[31]. Perpetrators cultivate an atmosphere of 'omnipresence,' where they appear to be everywhere in the victims' lives[32], reinforcing a 'hostage-like condition' that often persists long after the relationship has ended[33].

The proliferation of home automation technology intensifies this dynamic. What

25 Tokunaga & Aune, 2017.

26 Chatterjee et al. 2018.

27 Fraser et al., 2010; Mason & Magnet, 2012; Woodlock, 2017; Douglas et al., 2019; Brown et al., 2018; Dragiewicz et al., 2018; Yardley, 2020. In more extreme cases, perpetrators may use sophisticated spyware tools, covertly installed, to gain total control over the victim's device. Methods such as 'rooting' or 'jailbreaking' allow the abuser to clone the victim's smartphone or bypass its security features, enabling the installation of spy apps without the victim's knowledge. However, most perpetrators tend to use readily available and affordable technology. GPS software, for example, is widely used to track the location of partners or ex-partners, reinforcing the sense of omnipresence that often defines digital abuse.

28 These applications run in the background and are not visible as normal apps so it's basically impossible for the victim to notice them.

29 Woodlock, 2016; Matthews et al., 2017; Freed, et al., 2018, Afrouz, 2023.

30 Harris, 2018.

31 Brown et al., 2018; Fernet et al., 2019.

32 Woodlock, 2017; Douglas et al., 2019; Yardley, 2020.

33 Stark, 2012, p. 203; Woodlock, 2017; Markwick et al., 2019.

might initially seem like harmless tech tools can evolve into active stalking, transforming intangible fears into real threats or physical violence.[34]

Subtle forms of control may initially seem minor for the victims, but over time, these unusual incidents accumulate, leading victims to realise they are trapped in an unhealthy relationship. Control over essential devices—such as heating systems, kettles, or washing machines—can easily become tool of coercion and control. Once these devices malfunction, only the administrator can fix them, thereby enforcing dependency and further deepening the power imbalance[35].

Overall, this heightened level of interpersonal connectedness not only disrupts cohabitation, but significantly raises the risks of post-separation abuse, presenting new challenges for safeguarding practices. Excluding an abuser from the family home or relocating the victim may no longer suffice without additional technological safeguards.

34 Goulden, 2019, 2021; Brookfield et al., 2024; Dragiewicz et al., 2018, 2019; Leitão, 2021; Tanczer et al., 2021. Smart home technology is marketed to enhance one's comfort and functionality in an environment, as it consists of interconnected, internet-enabled devices that allow household functions to be controlled remotely via apps. Despite this, it is particularly concerning in situations of domestic abuse. When one individual maintains control over the connected ecosystem of devices, it strips others in the same home of their autonomy, as it can become a powerful tool for perpetrators to exert control, erode privacy, and monitor their partner's movements. Perpetrators may even engage in psychological manipulation or gaslighting by using these technologies to confuse and disorient their victims.

35 Riley, 2020. See also Ring, 2022. Smart doorbells represent another example of how such technologies can be abused. These devices, which are becoming increasingly common, send real-time notifications to homeowners' phones and stream live footage whenever movement is detected. For victims, this makes it nearly impossible to leave the house without alerting the abuser. It also complicates visits from social workers, as their presence may be immediately known to the abuser.

Challenges in Conceptualising and Categorising Online and Technology-facilitated Violence Against Women

As OTFVAW becomes increasingly prevalent, conceptualising it remains a formidable task for researchers, policymakers, and legal systems. Although several civil society organisations, academia, and international agencies have made significant efforts to clarify what OTFVAW is, as noted at the beginning, so far, no consensus has been reached on its definition, nor is there a consolidated terminology[36]

The primary difficulties lie in the rapidly changing technological landscape, the complexity and diversity of behaviours involved, the blurred boundaries between online and offline harms, and the intersectionality of gender, race, and other identity markers that shape women's experiences.

The Fluidity and Evolving Nature of Online and Technology-Facilitated Violence against women

One of the primary difficulties in conceptualising OTFVAW lies in the rapid evolution of technology itself. New platforms, apps, and devices continuously emerge, creating new avenues for abuse. As the digital world expands, so too do the opportunities for perpetrators to exploit technology in ways that were previously unimaginable. For instance, the rise of smart devices has introduced new forms of surveillance and control in intimate relationships. Technologies such as GPS tracking, smart home systems, and mobile monitoring applications allow abusers to exert constant surveillance and control over their victims, blurring the line between online and offline spaces[37]. This merging of the online and offline worlds creates a persistent form of abuse that leaves victims unable to escape the abuser's reach, whether they are physically present or not[38]. The integration of these technologies into everyday life makes it increasingly difficult to define where the abuse begins and where it ends.

Moreover, cyberspace has one foot firmly planted in the real world, meaning that online actions have tangible offline consequences[39]. The "online disinhibition effect"[40] further complicates matters, as perpetrators often feel emboldened to en-

36 Van Der Wilk, 2018. See also General Secretariat of the Organization of American States
37 Dragiewicz et al., 2019.
38 Afrouz, 2023.
39 Yar, 2005.
40 Suler, 2004.

gage in behaviours online that they would not exhibit in person, such as harassment or stalking. This psychological distance creates a conceptual gap, making it challenging to categorise such behaviours under traditional notions of violence. These fluid and ever-evolving forms of abuse defy precise categorisation, complicating efforts to address this phenomenon through policy and law.

Complexity and Variability of Online and Technology-Facilitated Violence Against Women

Another major obstacle in conceptualising these kinds of abuse is the inherent complexity and variability of online and technology-facilitated violence against women. Violence against women has traditionally been understood as physical, emotional, or sexual abuse that occurs within specific physical contexts, such as the home or workplace[41]. However, technology has expanded the arenas in which abuse can take place, creating new spaces for violence that transcend geographic boundaries. The digital environment — particularly social media and messaging platforms — allows abusers to harass, stalk, or otherwise victimise women from a distance, often anonymously, making the abuse less tangible and more difficult to categorise within existing legal and social frameworks[42].

Moreover, scholars and policymakers have not reached a consensus on whether all forms of online and technology-facilitated abuse should be considered "violence." For instance, some behaviours, such as certain forms of non-consensual intimate image distribution, are clearly intended to harm the victim and are recognised as a form of sexual violence.

This debate over the definition of violence is crucial, as it affects how victims perceive their experiences and whether they can seek legal recourse. In many cases, women may not even recognise that they are victims of OTFVAW because the conduct suffered does not fit into traditional notions of abuse. For example, constant monitoring or surveillance through digital means, such as tracking a partner's location using GPS or reading their private messages, may be perceived by victims as invasive or controlling but not necessarily as abusive or violent. This lack of clarity in conceptualising online and technology-facilitated abuse can prevent victims from identifying their experiences as violence and limit their access to support services[43].

41 Dragiewicz et al., 2018.

42 Henry & Powell, 2015.

43 Dunn, 2021.

Intersectionality and the diverse experiences of victims

A further critical challenge in conceptualising online and technology-facilitated violence against women is its intersectional nature, which highlights how various forms of discrimination and disadvantage—such as race, gender, class, and disability—intersect to amplify the harm experienced by victims. Women experience OTFVAW in diverse ways depending on their identity markers, including race, ethnicity, sexual orientation, and socio-economic status. This intersectionality complicates efforts to develop a one-size-fits-all understanding of this phenomenon, as different groups of women are targeted in different ways.

For instance, gendertrolling, a form of OTFVAW aimed at silencing women, disproportionately affects women in public or political life, particularly young women who speak out online or pursue political careers. These women are often subjected to gendered disinformation, threats of violence, and sexual harassment, tactics designed to push them out of public spaces[44]. However, when it is a woman of colour who is affected, this type of aggression is often associated with others that have racial as well as gender connotations, making their experience more complex[45]. Similarly, LBTI women face heightened online abuse due to their gender identity or sexual orientation, exacerbating the psychological and emotional toll they experience[46]. Women from culturally and linguistically diverse backgrounds are also particularly vulnerable, facing compounded effects of racism, sexism, and xenophobia.

The diversity of these experiences makes it difficult to create a singular, cohesive concept of OTFVAW that accounts for all forms of abuse. Intersectionality should be one of the key factors to consider in any analysis of violence against women[47]. Ignoring the unique ways in which different women experience abuse risks marginalising the most vulnerable victims. Despite this, it is common for policy and legal responses to overlook this intersectionality, adopting a one-size-fits-all approach that inadequately supports women, especially those more at risk of marginalisation. Addressing OTFVAW effectively requires nuanced approaches that acknowledge and respond to the intersectional nature of victimisation.

44 Jane, 2016.
45 Noble & Tynes, 2016.
46 Dragiewicz et al., 2018.
47 Crenshaw, 1989.

Online and technology-facilitated violence against women Through Multiple Conceptual Lenses

An additional layer of complexity arises from the diverse conceptual lenses through which the phenomenon of OTFVAW can be interpreted and categorised. These perspectives may vary depending on whether the focus is placed on 1) the nature of the harm inflicted, 2) the specific forms of abuse, 3) the platforms, or mediums through which the violence is enacted, or the 4) relational dynamics between the victim and the perpetrator. While each framework may offer valuable insights, they also exhibit certain limitations in providing a holistic understanding of the phenomenon.

These approaches illuminate the different ways in which technology enables abuse, yet none of them alone is sufficient to encompass the full scope of the issue. Thus, the challenge in conceptualising this phenomenon lies in the necessity of adopting a multidimensional approach that synthesises these perspectives, accounting for the interplay of technological, social, and interpersonal factors that contribute to this form of violence.

Conceptualising online and technology-facilitated violence against women through the lens of abuse tactics

Using this framework, the focus shifts to the specific tactics employed by perpetrators to harm, exploit, or exert control over their victims. Consequently, categorisation based on this perspective leads to an understanding of such conduct in terms of the method of abuse utilised and the role technology plays in amplifying its scope, intensity, and efficiency. From this perspective, we can delineate several categories of technology-facilitated abuse, including:

a. Cyberstalking and Online Harassment

This category encompasses persistent, unwanted online behaviours aimed at intimidating, threatening, or harassing victims. Cyberstalking often involves sending abusive messages, creating fake accounts to monitor or track a person, or making public threats. This form of behaviour mirrors physical stalking but is intensified by the omnipresence of the internet[48].

48 Citron, 2014.

b. Image-Based Sexual Abuse

This involves the non-consensual sharing of intimate images or videos of a person online[49]. It can also include threats to share such material as a form of coercion. This type of abuse is particularly harmful because it not only violates a victim's privacy but also leads to reputational harm and emotional distress.

c. Doxing

Doxing refers to the public release of private, identifying information (such as home addresses, phone numbers, or workplace details) without the victim's consent. The goal is to expose the victim to harassment or physical threats, effectively blurring the lines between online and offline harm.

d. Tech-Facilitated Coercive Control

In intimate relationships, perpetrators may use technology (like GPS tracking, monitoring apps, or smart home devices) to exert control over victims[50]. This category of OTFVAW focuses on how technology extends the abuser's ability to monitor, isolate, and coerce victims even when they are physically apart.

While this tactic-based lens helps to identify the specific behaviours that constitute tech facilitated abuse, it does have its limitations. By concentrating solely on the actions of the perpetrator, it risks oversimplifying the broader dynamics of such violence. The complexity of this phenomenon is not limited to individual behaviours but also involves systemic factors—such as platform design flaws or legal shortcomings—that enable this violence to proliferate. Therefore, while this framework is useful in isolating specific tactics, it must be integrated into a broader analysis of how structural inequalities underpin and facilitate such actions.

Conceptualising online and technology-facilitated violence against women through the lens of the type of platform or medium

Another way to categorise this abuse is by the platform or digital medium through which the violence occurs. This type of framework helps understand how specific

49 Henry & Powell, 2016.
50 Dragiewicz et al., 2019.

technologies or platforms are used to perpetrate abuse and how they shape the forms of violence women experience:

a. Social Media Platforms

Violence against women often occurs on platforms like Facebook, Twitter, Instagram, Telegram or TikTok. Gendertrolling often takes place on these platforms[51]. These platforms can also be used for cyberbullying, online stalking, online psychological abuse, public shaming, or spreading disinformation about women, leading to social and reputational harm. The anonymity provided by many platforms emboldens perpetrators, who are often able to harass victims without fear of identification or punishment.

b. Messaging Apps

Platforms such as WhatsApp, Snapchat, and Telegram are often used to send abusive messages, share non-consensual images, or facilitate coercive communication. These platforms allow perpetrators to send harassing messages privately or in group settings, amplifying the victim's feelings of isolation or fear.

c. Gaming Platforms and Online Communities

Women in the gaming industry or online gaming spaces frequently experience harassment in gaming environments like Twitch, Discord, or multiplayer online games. Women who speak out or participate in male-dominated spaces often face harassment, including sexist comments, death threats, and sexual threats[52].

d. Surveillance Technologies

Increasingly, abusers use smart home devices, such as CCTV cameras, smart locks, and location-tracking devices, to monitor their victims' every move. This type of abuse blurs the lines between physical and digital spaces, making it difficult for victims to find a safe refuge[53].

Although this platform-based classificatory system effectively highlights how technological infrastructures facilitate violence, it faces a significant limitation: it

51 Jane, 2016,

52 Fox & Tang, 2017.

53 Havard & Lefevre, 2020.

risks attributing excessive blame to the technology itself rather than recognising the gendered power dynamics and social norms that drive the abuse. While platforms certainly provide the means for violence, they do not inherently generate the misogyny that underpins much of this behaviour. Therefore, this perspective should be integrated with others that consider the social and cultural factors shaping this criminal phenomenon.

Conceptualising online and technology-facilitated violence against women through the lens of the nature of harm

Focusing on the nature of the harm offers another possible classification alternative that, unlike the previous ones, focuses on the victim, examining the psychological, emotional, reputational and economic impact of online and technology-facilitated violence.

a. Psychological and Emotional Harm

OTFVAW can cause significant psychological harm, including anxiety, depression, and suicidal ideation. Victims of online harassment, stalking, or image-based abuse often experience deep emotional distress due to the persistent and public nature of the abuse[54]. The omnipresence of digital surveillance can leave victims feeling trapped and powerless.

b. Reputational Harm

In cases such as image-based sexual abuse or doxing, the reputational harm can be devastating. Victims of experiencing this abuse often face social stigma, shame, and professional repercussions when their intimate images are shared without consent[55]. This harm is long-lasting, as content shared online is nearly impossible to fully erase.

c. Physical Harm and Threats

While technology often creates a symbolic distance between perpetrators and victims[56], it can also result in physical harm or threats of violence. For example, doxing victims may receive physical threats or harassment at their

54 Citron, 2014.

55 Henry & Powell, 2016.

56 Suler, 2004.

homes after their personal information is publicly exposed online. In such cases, the digital abuse leads to direct, real-world consequences.

d. Economic Harm

Violence perpetrated digitally can also result in economic harm, particularly when abusers control victims' access to resources or employment opportunities. It mainly takes place in intimate relationships. For instance, harassment on professional platforms like LinkedIn or disinformation spread about a woman in the workplace can damage her career prospects. Furthermore, victims of sextortion or non-consensual intimate image distribution may be blackmailed financially, adding an economic dimension to the abuse.

A victim-centred framework examining how OTFVAW impacts victims on many levels is essential in highlighting the wide-ranging impacts of violence perpetrated using technology. Nevertheless, it runs the risk of fragmenting the experience of harm into discrete categories, potentially missing the interconnectedness of these consequences. Psychological, economic, and reputational harms often feed into each other, creating a compounded experience of abuse that is difficult to separate into distinct outcomes. Thus, while this approach centres on the victim's experience, it should be applied in a way that acknowledges the holistic nature of the violence and its effects.

Conceptualising online and technology-facilitated violence against women through the lens of the victim-perpetrator relationship

By focusing on the relationship dynamics between victims and perpetrators, this framework highlights the power imbalances and personal contexts in which OTFVAW occurs.

a. Intimate Partner Abuse

In cases of intimate partner violence, technology is often used to extend control and surveillance over victims[57]. Abusers may use GPS tracking, monitor victims' social media activity, or control their access to communication tools. This type of abuse can continue even after the relationship has ended, making it difficult for victims to fully escape. Abusers may indeed

57 Dragiewicz et al., 2019.

continue to monitor and manipulate victims through social media, location-tracking apps, and other forms of digital surveillance[58].

b. Stranger or Anonymous Abuse

Many forms of OTFVAW, such as gendertrolling and online harassment, are perpetrated by strangers or anonymous users. The anonymity of the internet enables abusers to hide behind fake identities or pseudonyms, leading to a sense of impunity[59]. Victims in this context often have no relationship with their abusers, which can make the abuse feel more widespread and uncontrollable.

c. Peer or acquaintance abuse

Violence can also occur between peers or acquaintances, such as in cases of cyberbullying or non-consensual intimate image distribution. In these cases, the betrayal of trust plays a significant role, particularly when intimate images or information are shared by someone close to the victim.

This lens provides valuable insights into the power imbalances inherent in abusive relationships. However, an overly narrow focus on interpersonal dynamics risks overlooking the broader systemic issues that exploit technology to perpetuate and intensify abuse. To fully grasp the complexity of these phenomena, it is essential to integrate this perspective with more comprehensive structural and societal analyses.

National Conceptualizations of Online and Technology Facilitated Violence Against Women in Legislation

The conceptualisation of and legal responses to OTFVAW vary significantly across Europe, as no single harmonised definition of this complex phenomenon has been universally adopted. Consequently, national laws reflect diverse approaches shaped by broader legal, cultural, and historical contexts.

Overall, it is uncommon for national legal frameworks to regulate the various forms of cyber violence as specific offences. Mostly, this is treated as an aggravating

58 Dragiewicz et al., 2019.
59 Jane, 2016.

circumstance or is subsumed under existing laws that govern violence in the physical realm (such as harassment and stalking). The evolution of jurisprudence has also been key in broadening the scope of traditional offences to cover online behaviour. However, these laws are frequently drafted from a gender-neutral perspective, meaning that no specific reference to women is made when addressing cyber violence.

Although many states still lack specific provisions for cyber violence, significant legislative developments are underway. This is particularly likely to happen in EU countries following the adoption of Directive (EU) 2024/1385 on combating violence against women and domestic violence. Indeed, the Directive places a strong emphasis on preventing and addressing cybercrimes, and it aims to harmonise offences such as the non-consensual sharing of intimate or manipulated material (Article 5), cyberstalking (Article 6), cyber harassment (Article 7), and cyber incitement to violence or hatred (Article 8). In addition, GREVIO's General Recommendation No. 1 on the digital dimension of violence against women, adopted on 20 October 2021, holds the potential to significantly advance efforts in this area among participating countries

Online and technology-facilitated violence against women as a Specific Offence

Despite the general trend of subsuming cyber violence under broader legal categories, some countries have adopted more targeted approaches. Romania, for instance, is one of the countries that stands out with a comprehensive legal framework explicitly defining cyber violence. Romanian law addresses a wide range of offences, including online stalking, online threats, unauthorised sharing of intimate content, and illegal interception of communications.

Other states have instead developed legislation targeting specific types of cyber violence, such as cyberbullying, cyber harassment and cyberstalking, introducing targeted measures to address these forms of online abuse (e.g. Greece, Italy, Cyprus and Slovenia). Noteworthy, progress in cyber violence legislation has also occurred in states that now criminalise gendered forms of cyber violence, such as non-consensual intimate image distribution or sexist speech online, or recognise gender considerations, when crimes facilitated by technology, such as cyberstalking, are motivated by gender, gender identity or sexual orientation (e.g. Malta).

Cyberstalking has become a particular legislative priority across several European countries. Some national legal frameworks include penalties for cyberstalking and, in some cases, consider gender identity as an aggravating factor (e.g. Cyprus), while others have criminalised online stalking specifically (e.g. Slovenia, Austria, Spain, and Malta) or expanded their laws on online stalking to cover related offences like cyberbullying and doxing (e.g. Germany).

Efforts to combat online misogynistic hatred have also gained momentum in recent years.

While only a few states have specific laws targeting online hate speech, there is a growing trend toward recognising sex or gender as grounds for incitement to hatred. Additionally, many countries have expanded the prohibited grounds for hate speech to include sexual orientation, gender identity, or gender reassignment, either through legislation or case law[60].

The legal framework surrounding the non-consensual dissemination of intimate images has similarly evolved in response to rapid technological changes. An increasing number of countries (such as Belgium, France, Ireland, Italy, Malta, the Netherlands, Poland, Portugal, Spain, Sweden, and the United Kingdom) have criminalised the non-consensual distribution, publication, or sharing of intimate images. However, some of these laws do not specify whether the illegality applies to images taken with the victim's consent that are shared without their permission, leading to potential ambiguities in legal enforcement. Despite these challenges, the criminalisation of the non-consensual sharing of intimate images has expanded significantly. In cases where specific laws do not exist, courts have often interpreted existing legal provisions to address this behaviour. Several countries are also in the process of reforming their laws to provide clearer definitions and stronger sanctions.

Online and technology-facilitated violence against women as a general offence or aggravating factor

Different strategies are also employed to regulate cyber-violence. One common approach is treating the use of information and communication technologies (ICT) in crimes such as stalking, harassment, defamation, or child sexual abuse as an

60 De Vido & Sosa, 2021; EIGE, 2022.

aggravating factor. In many countries, including Italy, France, Slovakia, and Sweden, using ICT tools in stalking cases leads to more severe penalties. Similarly, in Romania, ICT use in child sexual abuse cases results in harsher punishment, while in France, online harassment through public communication platforms carries stricter penalties.

In some jurisdictions, cyber-violence can also be prosecuted under broader offences such as unauthorised data access or misuse of personal information. This approach is often applied to crimes like non-consensual dissemination of intimate images, identity theft, and impersonation. Additionally, in certain countries, national courts have expanded the scope of traditional criminal offences to cover ICT-related crimes, even when not explicitly mentioned in the law. For example, courts in Bulgaria have extended stalking laws to cover cyberstalking, and in Italy, defamation committed via ICT is treated as an aggravated offence.

Breaking the Vicious Cycle: Attempts for Internationally Recognized Definitions

OTFVAW is an inherently complex phenomenon, both factually and substantively. Its multifaceted nature makes it challenging to fully grasp and categorise, as it manifests in a variety of overlapping and interconnected forms. These acts often intersect, creating a continuum of abuse that is difficult to define and neatly classify within legal frameworks.

This conceptual difficulty complicates the work of national legislators who struggle to develop comprehensive laws that address the full scope of OTFVAW. As a result, legal responses across countries are fragmented, with varying levels of protection for victims. Some states have specific laws targeting certain forms of cyber violence, while others rely on broader legal frameworks that only indirectly address online abuse. This patchwork of legal approaches leads to inconsistent levels of protection, leaving many victims without adequate legal recourse, depending on where they live.

The fragmented nature of these laws also hinders the development of robust systems for data collection and analysis. Without uniform legal definitions or comprehensive legislation across jurisdictions, it becomes difficult to gather accurate and comparable data on the prevalence and nature of OTFVAW. The lack of reliable data impairs the ability to properly analyse the phenomenon, monitor trends,

and understand how it manifests across different countries. This, in turn, makes it challenging to create evidence-based policies and regulations that can effectively combat the problem.

The result is a **vicious cycle**: inadequate legal frameworks lead to incomplete data, and incomplete data hampers the development of stronger, more effective laws and policies. Without a coordinated, harmonised approach to both legislation and data collection, efforts to address OTFVAW will continue to be hampered, perpetuating a system that fails to fully protect victims and prevent abuse.

Despite the inherent difficulties—owing to the ever-evolving nature of technology and the diverse cultural, legal, and social contexts in which violence against women occurs—progress has been made towards establishing internationally recognised definitions for statistical purposes. International organisations have taken proactive steps to lay a strong foundation for developing standardised definitions that can facilitate consistent data collection and inform more effective policymaking.

The United Nations (UN) has played a pivotal role in addressing violence against women, including technology-facilitated violence. In 2018, the Special Rapporteur on Violence Against Women presented a report to the UN General Assembly, emphasising the urgent need to address violence perpetrated through technology. The report called for an "agreed understanding and conceptualisation" of online violence against women to support consistent data collection and policy development across nations. It proposed that digital violence should be considered a continuum of gender-based violence, where digital platforms serve as tools for harm, akin to more traditional forms of violence[61].

In response, UN Women initiated work towards creating comprehensive guidelines for identifying and measuring technology-facilitated gender-based violence (GBV). In 2020, it released the *Measuring the Prevalence of Online Violence Against Women* framework, designed to equip countries with tools for collecting comparable data on this issue (UN Woman, 2020). Also, in 2022, in collaboration with the World Health Organization (WHO), UN Women organised an expert group meeting as part of its Joint Programme on Violence Against Women Data. The gathering included 29 participants from 26 organisations, including government agencies, civil society, and academia, with specialists in gender policy, research, and statistics. Building on prior efforts to address technology-facilitated violence

61 UN Special Rapporteur on Violence Against Women, 2018.

against women, the group aimed to establish a comprehensive definition of it to create tools for collecting data on its prevalence[62].

Significant progress has also been made within the framework of the Council of Europe. The Convention on preventing and combating violence against women and domestic violence (Istanbul Convention) sets a critical benchmark for addressing violence against women and domestic violence in Europe and beyond. While the convention does not explicitly address the digital and technological dimensions of violence, any potential gaps in its application can be bridged by interpreting it in conjunction with GREVIO General Recommendation No. 1on the digital dimension of violence against women. Issued in 2021 by the Council of Europe Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO), this recommendation aims to address the expanding issue of the digital dimension of violence against women.

This seminal document reflects the growing awareness that violence against women has increasingly migrated to the digital sphere, underscoring the need for a comprehensive strategy to combat it. The recommendation clarifies that the Istanbul Convention's standards must extend to the digital dimension of violence against women. GREVIO has called on member states to develop clear definitions of digital forms of violence against women and incorporate these into national legal frameworks and statistical reporting systems[63] . A key strength of the Recommendation is its inclusive terminology, which covers both existing and emerging forms of online and technology-facilitated abuse. This includes relatively recent forms of violence such as cyberflashing, doxing, and deepfakes, which have been enabled by advances in technology. By broadening the scope of what constitutes violence against women, this inclusive approach helps shape legal frameworks and policy responses that are better equipped to address these evolving threats.

The WHO has long been involved in efforts to combat violence against women, particularly through data collection on gender-based violence. Although the WHO has traditionally focused on physical and sexual violence, it has acknowledged the rising importance of addressing technology-facilitated violence. In its *Guidelines for Researching Violence Against Women*[64] , the WHO underscored the

62 UN Woman, 2022.

63 Council of Europe, GREVIO, 2021.

64 2019.

need to include emerging forms of violence—such as cyber harassment and online stalking—in national data collection efforts.

The WHO has also advocated for the integration of technology-facilitated violence into broader gender-based violence surveys, urging governments to adopt standardised tools for measuring digital forms of violence alongside traditional ones. The *Violence Against Women Prevalence Data* initiative, launched by the WHO in collaboration with the UN, underscores the need for robust definitions of technology-facilitated violence to ensure consistency in reporting across countries. However, like other organisations, the WHO faces challenges in developing universally applicable definitions due to the diverse forms and contexts of technology-facilitated abuse[65].

At the European level, the European Institute for Gender Equality (EIGE) has played a crucial role in collecting and analysing data on violence against women. Its report, *Cyber Violence Against Women and Girls*[66] , identified key challenges in defining and measuring online forms of violence, noting that traditional survey tools often fail to capture the unique dynamics of digital abuse. EIGE stressed the need for internationally agreed definitions to ensure consistent data collection on cyber-violence against women across EU member states, thereby facilitating more effective policy development.

According to EIGE, cyber-violence against women encompasses any act of violence committed, assisted, or aggravated using information and communication technologies with the intent to harm women and girls. EIGE highlights the continuum of violence, where the boundaries between online and offline abuse become blurred.

Core elements of the proposed definitions focus on gender and intersectionality, as this violence typically targets individuals based on gender or intersecting identities such as race, disability, or profession. The role of information and communication technologies is also central, enabling these harmful actions in online environments and through digital devices.

The online-offline continuum reflects how violence crosses between virtual and real-world spaces. Furthermore, the perpetrator-victim dynamic can involve either

65 WHO, 2019.
66 2017.

known individuals or anonymous aggressors, with the latter often exacerbating the violence due to anonymity.

Harmonised definitions are critical in overcoming the challenges posed by the fragmented nature of legal responses across states. Many national laws fail to capture the full complexity of this multi-layered phenomenon, often overlooking the intersectionality of violence, where women face different risks based on their gender, race, sexuality, or other identity factors. By promoting standardised definitions, the comparability of data across countries can be improved, enabling more comprehensive research and policymaking to combat online and technology-facilitated forms of violence against women.

National responses to cyberviolence across Europe reflect a complex landscape of diverse legal frameworks and cultural understandings of gender-based violence. While some countries have made significant progress, others lag in providing adequate protections for women in digital spaces. International organisations such as the UN, Council of Europe, and EIGE play a critical role in pushing for harmonised definitions and standardised data collection practices, ensuring that the digital dimension of violence against women is recognised as a serious issue across Europe and beyond. These harmonisation efforts are essential for creating effective, coordinated responses to this pervasive form of violence.

CHAPTER II

BRIDGING THE DATA DIVIDE: ADDRESSING GAPS IN TECHNOLOGY-FACILITATED VIOLENCE AGAINST WOMEN IN THE COUNCIL OF EUROPE MEMBER STATES

Data Gaps in Technology-Facilitated Violence Against Women: an Overview

Data is a vital element in any decision-making process and the raw material of accountability. Without data that provides the right information about the right things at the right time, it is not possible to design, monitor and evaluate effective policies.

For this reason, improving the ability to obtain and manage high-quality data should be a goal for every national system. Progress in the area of violence against women, sometimes significant, has been made in recent years, but there are still many aspects of this diverse and pervasive phenomenon that still struggle to be accounted for due to the multitude of multi-layered factors outlined in the previous sections of this report. This can lead to the denial of fundamental rights[67].

67 United Nations Secretary-General, 2014.

The paucity of data on OTFVAW remains one of the most significant barriers to understanding and addressing the full extent of this pervasive issue. Digital forms of violence against women, which span a range of actions from online harassment and cyberstalking to non-consensual intimate image sharing, have risen sharply with the increasing ubiquity of digital platforms. Yet, there is a critical lack of systematic, comparable, and gender-disaggregated data to inform policy responses and prevention efforts.

According to EIGE, the absence of a harmonised legal framework and consistent definitions of cyber violence across States complicates the collection and analysis of data on this form of violence[68]. This definitional fragmentation, coupled with underreporting, means that the actual prevalence of OTFVAW remains largely hidden.

Internationally, the challenge is not just the lack of data but also the lack of specificity in data collection systems. For example, while many countries collect data on general forms of violence, few capture the unique dynamics of this phenomenon. This issue was highlighted by UN Women in their foundational meeting on technology-facilitated violence, which emphasised the urgent need for a common conceptual framework to standardise data collection efforts[69]. Without clear definitions and metrics, it is difficult to measure the prevalence, nature, and impact of these forms of violence, making it nearly impossible to develop effective, evidence-based interventions.

The scarcity of data is exacerbated by the failure to adequately recognise tech-facilitated violence against women within existing legal frameworks. Many countries do not yet classify digital forms of violence as a specific criminal offence, further complicating reporting, and prosecution efforts. This is echoed in the GREVIO General Recommendation No. 1 on the digital dimension of violence against women, which stresses that despite the increasing digital dimension of violence, many nations still lack specific laws targeting online forms of abuse, treating these acts as extensions of general laws[70]. This not only limits the legal avenues available for victims but also impedes data collection by law enforcement and other government agencies.

68 EIGE, 2022.

69 UN Women, 2020, 2022 and 2023.

70 GREVIO, 2021.

Moreover, existing data often fails to capture the intersectional nature of this criminal conduct. Women from marginalised groups—including ethnic minorities, LBTI individuals, and those with disabilities—are particularly vulnerable to digital forms of violence against women, yet these groups are often left out of mainstream data collection efforts.

Therefore, data collection should be expanded and made more inclusive, incorporating the experiences of vulnerable populations who are often disproportionately impacted by digital forms of violence. This involves developing standardised tools for measuring both the prevalence of violence enabled (or favoured) by technology and the effectiveness of interventions aimed at combating it. Furthermore, involving diverse stakeholders, including survivors, in the data collection process would be beneficial to ensure that policies and interventions are both responsive and survivor-centred.

The relevance of the Istanbul Convention in Improving Data Collection on Digital Violence against women

The absence of robust and reliable data on OTFVAW presents a significant barrier to addressing this escalating issue and formulating comprehensive policy responses. Without accurate data, the true scale of this phenomenon remains obscured, resulting in gaps in both academic research and policy interventions[71]. To develop effective strategies, policymakers and researchers require harmonised definitions, gender-disaggregated statistics, and data that reflects the intersectional nature of digital violence.

To this end, the Istanbul Convention attaches great importance to the collection of data and research to support efforts in preventing and combating violence against women and domestic violence. **Article 11 of the Istanbul Convention** is pivotal in setting standards for the **systematic collection of data** on all forms of violence against women, including in its digital dimension. It serves as a framework for ensuring that data collection and research underpin all efforts to prevent violence against women and domestic violence, offering the necessary evidence to evaluate and enhance the policies and interventions designed to address these issues.

71 Powell & Henry, 2016,

Data Collection Obligations Under Article 11

Article 11 of the Istanbul Convention underscores the critical role of systematic and comprehensive data collection in shaping effective policies to prevent and combat violence against women and domestic violence. Despite the recognised importance of gathering such data, it remains rare for parties to the convention to have systems that consistently collect administrative or population-based information. This scarcity of reliable data makes it difficult to compare the scope of the problem across countries and over time. Consequently, the article emphasises the need for evidence-based policymaking, which relies on producing robust and comparable data to guide decision-making and monitor the progress of measures implemented to address violence. It sets forth the obligation for governments to regularly collect representative and comparable data to inform and improve policy interventions.

Collecting disaggregated data and supporting research in this field

The obligations set out in paragraph 1 are twofold. First, governments are required to collect relevant statistical data at regular intervals on cases involving all forms of violence addressed by the Istanbul Convention. This data must be disaggregated to ensure a clear understanding of the different dimensions of the issue. For instance, statistical information may be gathered from health care services, social welfare agencies, law enforcement bodies, and non-governmental organisations, as well as from judicial records maintained by authorities such as public prosecutors. Such data plays an essential role not only in raising awareness among policymakers and the public about the severity of the problem but also in encouraging victims or witnesses to come forward and report incidents of violence.

Additionally, collecting data about service use by victims offers insight into how effectively government agencies, health services, and other institutions respond to victims seeking justice, medical care, counselling, housing, or other forms of support. Administrative and judicial data serve another crucial function: they help assess the performance of government institutions and estimate the administrative costs associated with responding to violence.

The article also stresses the importance of gathering judicial data, including information about conviction rates, sentences handed down to perpetrators, and the characteristics of those convicted. Public authorities, including the judiciary, police, and social services, must develop data systems that go beyond internal records and focus on capturing the broader social context of violence and the

effectiveness of responses to it. To assess whether preventive measures and protection policies are yielding results, countries must collect administrative and judicial data at regular intervals. The quality of this data is paramount, as it determines its usefulness in shaping responses to violence. While countries are given some flexibility in determining the exact categories of data collected, as a minimum, the data should cover details about the victims and perpetrators, such as gender, age, the type of violence involved, and the relationship between the victim and perpetrator. It should also include information about the geographical location and, where relevant, factors like disability status.

In addition to statistical data collection, paragraph 1 also mandates that governments support research in this field. Effective policymaking must be grounded in state-of-the-art research and knowledge. Research can provide insights into the root causes of violence, its frequency, conviction rates, and the efficiency of measures taken under the Istanbul Convention. This provision calls upon governments to actively encourage research efforts to deepen understanding of the problem and improve the real-world responses of law enforcement agencies, support services, and the judiciary.

Conducting population-based surveys

Paragraph 2 of the Istanbul Convention further requires parties to conduct population-based surveys, which collect data representative of the broader population. These surveys offer valuable sociological insights into the prevalence, nature, causes, and consequences of violence. They also shed light on the experiences of victims, reasons for underreporting, the services victims receive, and their opinions and attitudes toward the violence they face. Such surveys must be conducted at regular intervals to track trends in violence over time and assess the effectiveness of policies. The size and scope of the surveys can vary depending on the country, with some opting for national studies and others focusing on regional or local levels. Combining different levels of data collection provides a comprehensive view of the phenomenon, identifying both broad patterns and local specificities.

The article distinguishes between two key types of data collection: population-based surveys and administrative/judicial data. These methods serve different purposes and answer different questions. While surveys provide insights into the frequency and severity of violence, as well as the socio-economic and cultural factors at play, administrative data helps assess the capacity of government agencies and the effectiveness of services provided to victims. When used together, these two forms of data collection offer a more complete and nuanced

understanding of the issue. However, a lack of standardised definitions and indicators often makes it difficult to compare data across countries, which is why it would be advantageous for governments to align their data collection efforts with existing standardised methodologies.

Making data publicly available

Article 11(4) of the Istanbul Convention emphasises the significance of making the collected data accessible to the public while ensuring that the privacy rights of the individuals involved are adequately protected. Governments are allowed some flexibility in determining both the nature and the scope of the data to be made public, but transparency is crucial in efforts to prevent and address violence against women and domestic violence.

Merely collecting data and storing it within government bodies or academic institutions is insufficient. This information must be made available to the public to fuel informed debate. In today's digital age, this means publishing data on an accessible online platform. To ensure its usefulness for the general public, the data should be summarised into key indicators. For experts, access to the underlying databases is essential. Furthermore, it is critical that the published data retains its relevance to the issues of violence against women and domestic violence. As a best practice, this data should be consolidated into a single, easily accessible location for policymakers, practitioners, and the public alike. Another important goal is to ensure the comparability of data between institutions within a country, across different time periods, and, ideally, between countries.

Special care must be taken to protect individuals' privacy when releasing this information. Article 65 of the Istanbul Convention, referencing the Council of Europe's Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108), ensures this protection. At a minimum, this means that no personal details should be identifiable in the publicly available data.

Why is it difficult to have complete and consistent data?

The evidence base surrounding OTFVAW is growing, but significant gaps remain in both scope and depth. Privacy issues, the transborder nature of digital platforms, and the fragmented legal frameworks that govern online spaces collectively create substantial barriers to the development of comprehensive data collection systems for OTFVAW. To overcome these challenges, there is a need for greater

international cooperation, harmonisation of legal definitions, and the development of privacy-conscious, victim-centred data collection practices that can operate effectively in a globally interconnected digital environment.

Privacy concerns

One of the key challenges in collecting data on OTFVAW is balancing the need for disclosure with the protection of victims' privacy. Many victims are reluctant to report incidents due to fear of further exposure, retaliation, or social stigma. This is especially true for acts like image-based sexual abuse (e.g., the non-consensual sharing of intimate images), where victims are often targeted precisely to shame them publicly.

Additionally, the process of reporting OTFVAW can sometimes require victims to provide sensitive personal information, including details about their online activities, communications, and location. This can create a dilemma for data collection systems, which must ensure that victims' privacy and anonymity are fully protected while still gathering enough detail to assess the scope and impact of the violence.

Data collection efforts must navigate various legal and ethical obligations to ensure that victims' information is secure and that the process does not inadvertently re-traumatise those who have experienced violence. Safeguards, such as informed consent, data anonymisation, and secure storage protocols, are critical, although additional steps may be needed to collect granular, disaggregated data.

Transborder Digital Spaces

The nature of the internet and online communication transcends national boundaries, making it difficult to regulate, monitor, or address behaviours that cross jurisdictions. A single case of online harassment or abuse can involve individuals and platforms located in multiple countries, all governed by different laws, making it challenging to hold perpetrators accountable or to gather consistent data.

For instance, platforms like Facebook, Twitter, and Instagram may be based in one country, while the victim and perpetrator are located in others. Each of these jurisdictions may have different laws regarding privacy, data protection, and the prosecution of online crimes. This can lead to situations where the legal protections

available to victims in one country are insufficient because the abuse originated from or is hosted in another country.

This transborder nature creates significant challenges for data collection, as countries may collect and report data in different ways, or not at all, and international cooperation may be limited. Global efforts, such as those led by UN Women and the Council of Europe, are pushing for more harmonised frameworks to enable cross-border collaboration on data collection and legal responses to digital violence against women. However, the lack of cohesive international standards remains a major barrier.

Inconsistent Legal Frameworks

Inconsistent legal frameworks have long been cited as a major barrier to producing reliable, comparable data, as this lack of standardisation hampers efforts to capture the full scope of the issue. Legal responses to technology-facilitated violence vary widely across countries, and many jurisdictions still lack specific laws that address the unique characteristics of online abuse.

Some nations have comprehensive cybercrime laws that encompass forms of online violence, while others rely on outdated or fragmented legal frameworks that do not adequately account for the OTFVAW . For instance, certain countries may have laws against stalking or harassment, but these laws might not explicitly apply to online behaviours, or they may not recognise digital actions like doxing, cyberstalking, or gender-based online hate speech as criminal offences.

In many instances, tech companies which host the platforms where violence occurs operate under different legal expectations depending on their jurisdiction, further complicating the situation. While some platforms have voluntarily adopted transparency reporting or content moderation policies aimed at reducing online forms of violence, their efforts are not consistent globally, and their ability to share data with governments or international bodies is often constrained by differing national privacy laws.

The current landscape of data collection

The current landscape of data collection on online and technology-facilitated violence against women is shaped by a variety of sources, including surveys, administrative data, and qualitative research. Each of these plays a critical role in offering

insights into the prevalence and impact of this phenomenon, but each also comes with its own set of limitations. To understand the scope and challenges of data collection in this area, it is necessary to explore these data sources more profoundly and to identify promising practices that can improve the comprehensiveness and reliability of the data.

National Surveys and ICT-Specific Studies

National surveys, particularly those addressing violence against women, have traditionally been among the primary methods for measuring the scale of OTFVAW. These surveys are invaluable in gathering comprehensive data, as they often provide more extensive and nuanced information than administrative sources. This is particularly crucial because many cases of cyber violence go unreported to authorities like the police, making surveys a key tool for capturing the subtle dynamics of online forms of violence, especially against women, which administrative data may not adequately reflect.

Usually conducted by national statistical agencies or international organisations, these surveys aim to assess the prevalence of violence against women across different population groups. Some surveys include questions on digital abuse, such as cyberstalking or online harassment. In contrast, information and communication technology-specific studies explore the role of technology in society, frequently focusing on how digital platforms are used and the risks they pose, particularly for women and girls.

However, the global coverage of these surveys remains inconsistent, with many countries lacking the infrastructure or resources to conduct them regularly. Even when such surveys are undertaken, they often fail to disaggregate data in ways that capture the full scope of technology-facilitated violence against women. For example, surveys may not differentiate data by race, disability, sexual orientation, or socioeconomic status—all critical factors for understanding the intersectional nature of online violence. Research has consistently shown that women from marginalised communities face multiple, intersecting forms of violence.

For example, LBTI individuals, racial minorities, and women with disabilities are disproportionately affected by technology-facilitated violence against women, yet existing data often fail to capture this complexity. This leads to a skewed understanding of vulnerability and how various groups experience online abuse. Without disaggregated data, policymakers are limited in their ability to create targeted interventions that address the specific needs of all affected groups.

Administrative data

Administrative data, including records from law enforcement agencies, courts, and service providers (such as shelters, helplines, or legal aid organisations), represents a crucial source for understanding OTFVAW. This data is valuable because it is consistently collected, providing insight into legal and institutional responses to online forms of violence against women.

However, administrative data, such as crime statistics, tends to reflect service utilisation rather than the actual prevalence of violence. Many incidents go unreported, meaning that statistics primarily capture interactions with services such as the police or social support systems, often leading to an underestimation of the problem's true scale.

There are significant challenges associated with administrative data in this context. Many data systems are not designed to capture the specific technological nature of certain violent incidents. As a result, cases of online harassment or abuse are frequently subsumed under broader categories such as harassment, stalking, or general violence, without recognition of their technology-facilitated nature. This lack of distinction diminishes the visibility of OTFVAW in national crime statistics and complicates the development of policies aimed at addressing the specific traits of online abuse.

In addition, administrative data often suffers from underreporting. Many victims of technology-facilitated violence against women do not report their experiences to authorities due to fears of retaliation, feelings of shame, or a lack of trust in law enforcement and the judicial system. As a result, the data collected may not reflect the true prevalence of technology-facilitated violence against women. For certain groups, such as migrant women or LBTI individuals, these barriers to reporting are even higher, making administrative data an incomplete and potentially skewed representation of the issue.

Qualitative research

Qualitative research has proven to be a crucial tool for addressing the limitations of surveys and administrative data in the study of OTFVAW. Methods such as in-depth interviews, focus groups, and case studies allow researchers to collect rich, nuanced insights into how women experience this form of violence across various social contexts and identities. This type of research is especially effective at

shedding light on the psychosocial impacts of online forms of abuse, such as its effects on mental health, social participation, and professional prospects.

One of the key strengths of qualitative research is its flexibility and responsiveness. It enables researchers to investigate emerging forms of technology-facilitated violence against women, such as gender-based trolling or the use of deepfakes, which may not yet be covered by standardised surveys. However, qualitative research often involves smaller, more focused samples, making it less generalisable to the wider population. As such, it serves as a complementary tool alongside larger-scale data collection methods.

Promising Practices in Data Collection

Several innovative approaches are being developed to improve data collection, particularly in response to the limitations of existing methods. These include:

Community-Driven Research: Civil society organisations, especially those working directly with vulnerable groups, have played a critical role in filling data gaps through community-based research. For example, NGOs often conduct their own surveys or qualitative studies to capture the intersectional dimensions of violence occurring online or through digital means, focusing on specific groups such as young women, women of colour, or LBTI individuals. This research often uncovers patterns of violence that government data systems may overlook.

Integration of Social Media Data: Increasingly, social media platforms are becoming key sources of data for understanding this phenomenon. By analysing patterns of online harassment, hate speech, and abuse on platforms like Twitter, Facebook, and Instagram, researchers can gain real-time insights into how digital forms of violence manifests and spreads. Social media data, when combined with more traditional data sources like surveys or administrative records, offers a more comprehensive view of the scale and nature of online forms of violence.

Mixed Methods Approaches: There is a growing recognition that no single method of data collection can capture the full extent of this type of conduct. As a result, researchers are increasingly combining quantitative and qualitative methods to produce more nuanced and actionable insights. For example, surveys can provide baseline prevalence data, while qualitative research can explore the lived experiences of women facing online forms of violence. This mixed-methods approach

can yield more holistic findings, helping to inform policy interventions that are both broad in scope and deeply attuned to individual needs.

National data collection systems on online and technology-facilitated violence against women in Europe: an integrated overview[72]

In response to the rising concern about online and technology-facilitated violence against women and girls, European countries have developed various national systems to collect data on this issue. These systems vary widely in terms of sectoral involvement, the extent of institutional collaboration, and the specific forms of cyber violence tracked. This overview focuses on the key features of these data collection efforts, as well as the gaps that need to be addressed for a more comprehensive understanding of technology-facilitated violence against women.

Holistic and Multi-Sectoral Approaches

Some countries exemplify a comprehensive and multi-sectoral approach to data collection on OTFVAW. Their systems integrate input from law enforcement, justice systems, government agencies, academia, and NGOs. This cross-sector collaboration facilitates the gathering of detailed information on a wide range of forms of violence against women committed in the digital sphere, including cyberbullying, online harassment, and online stalking. However, even in well-integrated systems, there are still gaps in capturing newer forms of abuse, such as non-consensual image sharing and online grooming. Addressing these emerging threats would ensure that data collection remains responsive to evolving challenges in digital spaces.

Broad Coverage of Emerging Forms of Cyber Violence

Systems that demonstrate a broader scope not only cover traditional forms of OTFVAW (e.g., cyberbullying and online harassment) but also incorporate emerging and harmful practices such as online grooming, hate speech, and non-consensual image sharing. This wide-ranging approach allows for the identification and documentation of both established and lesser-known forms of abuse, positioning these systems at the forefront of data collection efforts. The

72 Information elaborated in this section is mainly taken from the analysis of Tables 6 and 7 in section 3.3.5 of the following report: European Institute for Gender Equality, (2022). Combating cyber violence against women and girls. https://eige.europa.eu

inclusion of diverse sectors such as law enforcement, academia, and NGOs ensures that the collected data captures a full spectrum of online violence, offering insights into both reported and unreported incidents.

Focused but Incomplete Systems

Other systems show a strong focus on certain forms of OTFVAW, including online harassment, online stalking, and non-consensual image sharing. While comprehensive in these areas, such systems often fall short in addressing newer threats like online grooming and hate speech. Expanding the scope to include these emergent forms would create a more holistic approach, ensuring that the data collected reflects the full range of risks women face online.

Systems with Gaps in Sectoral Involvement

Countries like Romania demonstrate strong involvement from certain sectors, such as law enforcement and NGOs, in their data collection efforts. However, the absence of broader government or academic engagement limits the system's ability to conduct comprehensive research or develop nuanced policy responses. This restricted scope leads to gaps in addressing certain forms of OTFVAW, such as cyberbullying and hate speech. Expanding sectoral participation and ensuring a more inclusive data collection approach would help bridge these gaps and provide a clearer picture of the issue.

Limited Institutional Involvement but Focused Data Collection

In some instances, such as in Italy, the data collection system is predominantly driven by police and justice authorities, with less involvement from NGOs or academia. This narrower institutional approach may miss key data on incidents not reported to law enforcement, particularly in cases where victims choose not to seek help from formal systems. While Italy's system covers online harassment, online stalking, and non-consensual image sharing, it currently lacks focus on critical emerging areas such as online grooming and hate speech. Broadening the institutional scope and tracking these newer forms would significantly enhance the system's responsiveness.

Narrow Data Collection but Emerging Forms Addressed

Poland offers an example of a system that primarily relies on police and justice data, which results in a somewhat narrow focus on traditional forms of OTFVAW such as cyberbullying, online harassment, and online stalking. Despite this, there has been progress in addressing some emerging forms of technology-facilitated abuse, like online grooming and hate speech. However, the limited involvement of other sectors, such as NGOs and social services, constrains the system's capacity to document unreported cases and develop more comprehensive insights. Expanding sectoral participation could significantly improve data coverage and policy effectiveness.

Limited Systems with Minimal Sectoral Involvement

Countries with more limited data collection systems, such as Bulgaria, Estonia, and Lithuania, tend to focus primarily on cyberbullying, with data gathered largely by the police and justice sectors. The lack of involvement from NGOs, academia, and broader government authorities limits the ability of these systems to capture the full extent of OTFVAW, particularly in relation to sensitive or underreported forms of abuse like non-consensual image sharing or online harassment. Expanding the scope of these systems to include a wider array of OTFVAW forms and increasing cross-sector collaboration would greatly improve their effectiveness.

A call for harmonisation and expansion

The national systems for collecting data on OTFVAW across Europe exhibit significant variation in their comprehensiveness and sectoral involvement. While some countries, such as Germany, Spain, and Austria, have established multi-sectoral systems that address a broad range of OTFVAW, others, like Romania, Italy, and Poland, are still developing their capacities. In contrast, countries with limited systems, such as Bulgaria, Estonia, and Lithuania, need to significantly expand their scope to ensure more accurate documentation of both well-known and emerging forms of OTFVAW.

For a truly effective and harmonised response to OTFVAW, national systems must broaden both their sectoral engagement and the range of violence forms they track. Greater involvement of NGOs, social services, and academia will provide a more complete picture of the problem, ensuring that unreported cases

and emerging threats like online grooming, deepfakes, and non-consensual image sharing are fully documented and addressed. A coordinated, multi-sectoral approach is essential for developing policies that respond to the diverse and evolving challenges posed by OTFVAW.

CHAPTER III

DISTINCT PATHWAYS IN DATA COLLECTION FOR GENDER-BASED VIOLENCE: EVOLVING PRACTICES IN CRIME TRACKING AND SYSTEM DESIGN

This chapter focuses on the evolution and distinct approaches in data collection systems related to gender-based violence (GBV), with an emphasis on the practices and legislative developments in Austria, Spain, and Portugal. It examines how different countries have adapted their data collection frameworks to address the growing and evolving forms of violence against women, including both physical and digital violence.

The data collection systems discussed in this study were not specifically designed to address OTFVAW. This issue remains underdeveloped in many national contexts. However, the regulatory framework surrounding OTFVAW is continuously evolving and will likely continue to do so in the coming years, particularly in EU countries that are subject to the recent directive on domestic and gender-based violence, which places a strong emphasis on OTFVAW. As a result, positive developments in this area can be expected from these countries, driven in part by

the need to comply with European legal requirements, potentially leading to improvements in information and management systems.

The case studies included in this research are significant because they illustrate how, despite varying starting conditions, data collection systems can be adapted to better address new forms of violence against women, including OTFVAW.

The systems featured in this study reflect a growing awareness of the issue and efforts to adapt general information systems to capture this form of crime. Among them, examples like the Austrian system show increasing recognition of the issue and efforts to adjust generalist information systems to address this type of crime. Other systems, such as Spain's, have long focused on violence against women and have developed specialised frameworks within various public service sectors specifically for this purpose. These systems now face the challenge of expanding their scope and improving data integration. Finally, some systems, such as those in Portugal, are making commendable strides in developing data collection structures with a holistic and specialised approach, involving all relevant stakeholders and enabling advanced processing capabilities.

All of the systems analysed in this study can serve as reference models, adaptable to the specific starting conditions of each context.

Adapting Data Collection Systems to Emerging Crimes (the Austrian case study) [73]

The Austrian federal government considers preventing and combating violence against women and domestic violence an absolute priority, which is also reflected by the current Government Programme 2020-2024.[74] Consequently, over the last years, Austrian authorities have taken important steps to align national legislation with the requirements of the Istanbul Convention through legislative measures impacting training initiatives and expanding victims' rights in criminal proceedings.

73 The information in this section was gathered through documentary research as well as in-depth interviews and materials provided by the Bundeskanzleramt, Sektion VII - Digitalisierung und E-Government, Ediktsdatei & Business Intelligence Justiz.

74 See Report submitted by Austria pursuant to Article 68, paragraph 4 of the Council of Europe Convention on preventing and combating violence against women and domestic violence (1st thematic evaluation round) Received by GREVIO on 7 June 2023, GREVIO/Inf(2023)13. Published on 7 June 2023. Available at https://rm.coe.int/thematic-evaluation-report-on-the-implementation-of-the-istanbul-conve/1680ab8593. See also the Government Programme 2020-2024 "Out of a Sense of Responsibility for Austria."

In this respect, the adoption of the Violence Protection Act 2019 marked a major advancement, as this new piece of legislation supplemented both emergency barring orders and court-issued protection orders with a prohibition to approach the victim.[75] Also, it has the merit to having reintroduced multi-agency risk-assessment conferences (MARACs), implemented mandatory violence prevention counselling for perpetrators of domestic violence[76] and raising criminal sanctions for rape through the use of force, threat or coercion, for stalking and the continuous use of force.[77]

These advancements reflect Austria's broader commitment to addressing both physical and digital violence against women, a stance underscored by recent legislative responses to OTFVAW. High-profile cases have highlighted the continuous nature of violence that women experience both online and offline, leading to additional legislative measures. In addition to legislative changes, Austria has introduced various public support initiatives aimed at raising awareness of online and technology-facilitated violence and improving support services for victims. These measures include expanded funding for violence protection centres, specialised training for staff handling cyber-violence cases, and the establishment of cybercrime competence centres within public prosecutors' offices. Such initiatives help foster a robust institutional response to digital violence, enhancing investigative capabilities and supporting victims more effectively.

As Austria continues to adapt its legal framework to address emerging forms of violence, it also faces challenges in adapting its data collection systems to capture these crimes accurately. This section examines Austria's approach to adapting data collection systems to these emerging forms of violence and underscores Austria's commitment to improving data accuracy and comprehensiveness. While challenges remain—particularly in aligning police and justice systems to enable a seamless, case-based tracking mechanism—these developments reflect a clear trajectory toward a data-driven approach to combating violence in all its forms.

Legislative and policy context concerning cyber violence against women

On January 1, 2021, Austria introduced a comprehensive statutory package to combat online hate, marking a significant step forward in addressing hate speech

75 See Article 51 of the IC, Emergency barring orders.

76 See Article 16 of the IC, Preventive intervention and treatment programmes.

77 See the Federal Law Gazette I, no. 105/2019, 29 October. Available at www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2019_I_105/BGBLA_2019_I_105.html

and cyberbullying.[78] Although certain "hate posts" and acts of cyberbullying could already constitute criminal offences before this change—and victims could seek claims under civil and media law—the legal framework has become notably stricter since 2021. This shift came with the enactment of the Hate Prevention Act (*Hass-im-Netz-Bekämpfungsgesetz*, HiNBG) and the Communication Platforms Act (*Kommunikationsplattformen-Gesetz*, KoPl-G), which expanded the scope of criminal offences and improved enforcement options, while introducing new obligations for communication platforms to ensure compliance. Among other provisions, the new package allows victims of online severe violations of personality rights to obtain cease-and-desist orders under specific conditions without a prior oral hearing. Additionally, new provisions in the Civil Code extend cease-and-desist claims for unlawful personality rights violations not only to the perpetrators but, in some cases, also to online platforms hosting unlawful content.

The Hate on the Net Prevention Act introduces substantial changes across criminal law, media law, and enforcement practices. In criminal law, the Act broadens offences related to online harassment, hate speech, and personal privacy violations. Through an amendment to Section 107c of the Austrian Criminal Code, the Act makes cyberbullying punishable following the first instance of publication, including single instances of unauthorised explicit image sharing. Section 283 of the Criminal Code has also been expanded to make incitement based on religion, ethnicity, or disability a punishable offence. Notably, a new provision, art. 120a, criminalises "upskirting" and other unauthorised visual recordings of intimate areas, along with the dissemination of such images, thus strengthening protections against privacy violations.

In media law, the Hate on the Net Prevention Act establishes a minimum compensation of EUR 100 for violations of personality rights by media outlets and increases the maximum compensation to EUR 40,000, or up to EUR 100,000 in particularly serious cases. The Act also improves remedies and enforcement options for victims, simplifying the process of requesting the removal or blocking of illegal content on communication platforms and allowing complaints against platforms that fail to comply with removal requests. Also, victims can now report illegal conduct even if the author's real identity is unknown, and courts may issue injunctions against the author of the post based on substantiated complaints without an oral hearing. Importantly, the Act expands access to free psychosocial

78 Federal Law Gazette I, no. 148/2020, 23 December. Available at www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2020_I_148/BGBLA_2020_I_148.html

and legal support for victims, strengthening available resources and protections for affected individuals.

As a complement to the Hate on the Net Prevention Act, the Communication Platforms Act introduces specific requirements for both domestic and foreign providers of profit-oriented communication platforms that meet certain thresholds in terms of user volume and revenue generated in Austria. This Act strengthens the obligations of media platforms toward their users, particularly in relation to handling illegal content.

Key obligations under the Act include the requirement for platforms to implement effective and transparent procedures for reporting alleged illegal content, with clear guidance provided to users throughout the reporting process. Platforms are also required to conduct a transparent review of these reports, ensuring decisions are both fair and comprehensible to users.

The Act further mandates timely action on illegal content. If the reported content is manifestly illegal, platforms must delete or block it within 24 hours of receiving the report. In cases where the content is not immediately identifiable as illegal, platforms are given a maximum of 7 days to complete their review and take action.

Through these provisions, the Communication Platforms Act aims to create a safer online environment by ensuring swift responses to harmful content while holding platforms accountable for transparent communication and user guidance.

The Austrian authorities' commitment to addressing digital violence against women extends beyond strictly legal actions. Austria has introduced numerous public support and funding initiatives aimed both at raising awareness of different forms of cyberviolence and at combating it, allowing women victims to place greater trust in the criminal justice system.

One key area of focus has been the increased counselling needs within violence protection centres, given the complex demands of preventing and addressing online and technology-enabled violence, such as stalking, sexual harassment, and psychological abuse. These needs have been met through additional funding, expanded staffing, and an increase in contracts with violence protection centres.[79] A dedicated counselling service has also been established specifically for victims of

79 See Report submitted by Austria, supra 74, pp. 68-69

online hate and violence, and staff members at these centres have received specialised training to handle cases involving cyber violence.

In addition to these initiatives, Austria has taken steps to strengthen its institutional response. In 2023, cybercrime competence centres were set up at multiple public prosecutors' offices nationwide. These centres offer specialised training on cybercrime to law enforcement personnel, facilitating more effective investigations of digital violence against women. Evidence collection in cases of digital violence has proven especially challenging, as it is labour-intensive and hindered by limited police resources. Specialised cybercrime officers within the police force—trained to recognise and address digital forms of violence against women—are intended to improve law enforcement's capabilities in this area. This measure is also expected to benefit victims by addressing several challenges identified by NGOs and recent thematic reports, including the lack of recognition of such phenomena, the tendency to trivialise reports,[80] and inadequate methods of evidence collection.

Although some weaknesses remain, which may be addressed in the future, Austria's efforts to promote digital literacy and online safety among young people are commendable. These initiatives aim to achieve positive outcomes in both the short and medium term, with programs that teach young people to recognise and protect themselves against harmful behaviours such as sexting and cyber-grooming.[81] In the long term, these programs are also expected to contribute to broader awareness, equipping youth to recognise and reject discrimination, violence, power imbalances, and abuse.

80 Habringer et al., 2023.

81 Consider, for example, the work undertaken by the Safer Internet Centre (SIC), established to promote the safer and more responsible use of the internet and mobile technologies among children and young people. The Centre comprises several key organizations: the Austrian awareness centre Saferinternet.at (www.saferinternet.at), the Helpline Rat auf Draht (www.rataufdraht.at), and the Hotline Stopline (www.stopline.at). Coordination is overseen by the Austrian Institute for Applied Telecommunications (ÖIAT, www.oiat.at), with additional support from the Association of Austrian Internet Service Providers (ISPA, www.ispa.at) as a consortium partner.
Saferinternet.at works closely with public authorities, non-governmental organizations, and industry partners to achieve its mission. This initiative is part of the European Union's 'Digital Europe/Safer Internet' programme and receives funding from the Austrian Research Promotion Agency (FFG), federal ministries, and industry stakeholders.

Data collection approach and developments in the field of violence against women

Despite commendable legislative progress in this area, data collection on OTFVAW currently lacks a specific focus and an emerging strategy. However, ongoing efforts by Austrian authorities to improve their national data collection system on violence against women are noteworthy, as they demonstrate how a system can be progressively adapted to address new forms of crime. This adaptation is essential to understanding the dynamics and evolution of these problems fully, enabling the design of more effective public policies and institutional responses.

Austria has access to a range of relevant administrative data sources. For instance, beyond core sources, such as law enforcement agencies and the criminal justice system, data can also be drawn from civil courts (for issuing civil protection orders), prison and probation services, agencies providing psychosocial and legal support, and specialised victim support services. More recently, steps have been taken to improve data collection from the healthcare sector. However, these data are, in some cases, partial, not very granular, complex to extract for statistical reasons and, above all, are sometimes defined in such a way that they cannot be traced back to the gender of the victim or the relationship between victim and perpetrator. For a more effective policy response to violence against women, these data sources should be more comprehensive, disaggregated and systematically integrated.

Austria has been making strides in this direction, particularly in response to recommendations from GREVIO's baseline evaluation report on Austria, published in 2017. The evaluation identified three key areas for improvement. First, it emphasised the need to create specific data categories for law enforcement to document the relationship between perpetrators and victims, enabling a more precise understanding of these relationships. Second, it recommended harmonising these categories, along with other data, across different sectors to ensure consistency. Finally, the report highlighted the importance of making the gendered nature of all forms of violence against women more visible in crime statistics, including in publicly presented data on gender-related killings of women in Austria.

In response to these recommendations, steps have been taken to collect and publish data from various sources, providing a more comprehensive overview of gender-related domestic violence and femicides.

A key factor contributing to these improvements has been the criminalisation of specific behaviours, which are now clearly classified under the Austrian Penal Code. This allows them to be systematically recorded within data collection and management systems, as in the case of upskirting, now regulated under Article 107c of the Penal Code.

Similarly, progress has resulted from efforts to refine legal definitions. Guided by the definition of violence in Article 3(a) of the Istanbul Convention, a reform launched in 2021 and currently underway envisages numerous measures to protect children and women against domestic violence better. The decree *Guidelines for the Prosecution of Offences in the Immediate Social Environment* introduced a single, nationwide definition of violence in close social relationships for public prosecutors, which impacts data collection systems managed by the police and judicial authorities, providing specific codes to be selected by users to classify events imputed.

The recently adopted change to the hate crime motives registration system also contributes positively to this goal. On 1 November 2020, the 'Motive' tab was activated in the police registration programme to collect data for the registration of motives according to nine categories. The nine categories of bias motives are age, disability, gender, skin colour, national/ethnic origin, religious belief, sexual orientation, social status and ideology.[82] The entered data are then transferred to the administration of justice via a specifically designed interface through 'electronic legal communication' [Elektronischer Rechtsverkehr].[83]

Law enforcement data

The data collection system in use at Austrian law enforcement agencies has historically been considered a good data collection system, producing crime statistics on the annual number of crimes reported to the police, the number of solved crimes and the percentage of solved crimes. The system has also long been able to provide information on both the number of suspects and the number of victims, which can also be broken down by gender and age groups.

All data are collected on the basis of offences under the Austrian Criminal Code and on the basis of specific pre-defined marks. There is also the possibility for certain

82 See the Austrian Police Crime Statistics 2022. Available at https://bundeskriminalamt.at/501/files/2023/PKS_Broschuere_2022.pdf

83 Report submitted by Austria, supra 74.

offences (such as most sex offences and offences against the physical integrity of another person) to include "additional" information on the relationship between victim and offender. The categories of data used for this purpose are (i) acquaintance, (ii) family relationship in the same household, (iii) family relationship not in the same household, (iv) none, (v) unknown, and (vi) casual acquaintance. These categories have been gradually introduced over time and are intended to shed more light on the specific nature of the offence.

Recently, this system has evolved further to better capture the relationship dynamics between victims and offenders in response to GREVIO's recommendations in its 2017 baseline evaluation report. The report pointed out that existing categories were insufficiently specific to draw accurate conclusions about the relationships involved, limiting the system's ability to identify systemic gaps in the institutional and judicial response to violence. The "Police Crime Statistics 2023" report reflects this trend, offering detailed data on specific types of violent crime within private settings. It also includes substantial information on digital crimes, such as sextortion, although these sections currently lack data on victim gender or the relationships between victims and perpetrators.

The report also devotes ample space to crimes committed in the digital sphere, including sextortion; however, here, no evidence is given of statistics based on the gender of the victims or the relationships between them and the perpetrators, thus hampering a comprehensive understanding of the scope and dynamics of technology-facilitated violence against women.

In recent years, substantial advancements in data analysis have been made, driven in part by the Federal Ministry of the Interior and the Federal Criminal Police Office. Noteworthy examples include the *Report on Protection from Violence 2020–2022*,[84] which provides an in-depth analysis of "violence in close relationships" based on police data, and *Facts and Figures on Women's Homicides in 2021*,[85] which focuses on gender-related killings. Although these reports are currently published on an ad hoc basis, there are hopes they will soon become regular publications, eventually expanding to include data on prosecutions and convictions to offer a more comprehensive view of violence in Austria.

84 See the Federal Criminal Police Office, Violence Protection Report 2020-2022, available at: www.bmi.gv.at/bmi_documents/3035.pdf. As to the definition of "violence in close relationships", see Article 3 "Definitions".

85 Document available at Available at: https://bundeskriminalamt.at/501/files/2022/Morde_weibliche_Opfer_2021.pdf

This shift reflects a growing awareness that data collection must serve a broader purpose. While Austrian law enforcement originally collected data primarily for internal tracking (e.g., monitoring personnel hours), this data has since become critical for evidence-based policymaking, underscoring a commitment to addressing systemic issues.

Extending this consideration, it is important to recognise that the quality of data within this system depends not only on technical capabilities but also on the judgement and practices of individual data entry agents. Although the system offers ample options for granular data collection, consistency can vary due to differences in agents' experience, specialisation, and approach. Efforts to promote a more standardised approach to data entry through ongoing training may, over time, help to gradually reduce these variations, enhancing the overall accuracy and reliability of the data.

Judicial data

With regard to criminal justice information, management information systems collect comprehensive crime and court data. During criminal proceedings, data is gathered on the accused and their victims, including details such as gender, age, and nationality, as well as information on the alleged crimes. All data is collected based on the offences defined in the Austrian Criminal Code, following the same legal framework as law enforcement agencies. The cases examined are those brought to court and adjudicated, including the primary offence that determines the level of punishment (*strafsatzbestimmendes Delikt*).

The data acquisition process begins with the transmission of information from the police department to the state prosecutor's office. Most data collected at police stations regarding reported offences—including information on perpetrators, victims, and the type of crime (classified under the Criminal Code)—is transferred to the state prosecution service in a structured digital format. However, the structured digital data flow does not include a detailed description of the case, meaning that case narratives are not captured in a way that allows for systematic data extraction.

The prosecution and court systems share the same IT infrastructure, though each has different functionalities. Once a case proceeds to court, data flows into the system; however, a separate digital case file is created, which functions as an image copy of the original file.

As to the data gathering system of law enforcement agencies, data categories are in use by the criminal justice sector to record the relationship between perpetrator and victim. It is also possible to identify circumstances or factors that are interesting in terms of legal analysis and policy, such as offences committed within families or child abuse, by applying special crime identification codes or additional entries in the electronic register. With regard to criminal cases, data from the case automation system, including perpetrator data (e.g. gender, age, nationality), victim data (gender, age, nationality, civil claimant status), and metadata on investigations and criminal proceedings (e.g. competent court/public prosecutor, subject of the case, closing of cases, procedural steps and duration of proceedings, etc.) is available for analysis already at this point. The Ministry of Justice and the Datawarehouse Team (DWH Team) of the Federal Computing Centre (BRZ) provide federal statistics from the case automation system "Verfahrensautomation Justiz (VJ)" upon request at any time and regularly.

An important development was the introduction of the "FAM code," designed to categorise and track cases of violence within family or intimate relationships for legal and statistical purposes. Although welcomed, the use of this code initially raised some concerns because its scope was quite broad, covering relationships too varied to make the data category meaningful for policy-making. Additionally, it did not allow for distinctions between current and past partners or clarify whether the perpetrator and victim lived or had lived together.

To address these issues, a single, Austria-wide definition of "violence in the immediate social environment" was introduced to close data gaps and improve international comparability. On October 1, 2021, the third amendment to the decree "Guidelines for the Prosecution of Offenses in the Immediate Social Environment" entered into force, providing a unified framework for all cases classified as violence in the immediate social environment, regardless of the jurisdiction of district or regional courts.

Accordingly, "violence in the immediate social environment"[86] encompasses offences committed with willful intent against life and limb, offences against sexual integrity or self-determination, and delinquency[87] to the detriment of a partner, spouse, or registered partner of the accused, even after the relationship has ended. In cases where statements from the parties involved contradict each other,

86 To further information about FAM offences, see Section 4(3a) of the Ministry of Justice's Regulation on the Implementation of the Public Prosecutors' Act [DV-StAG].

87 See the Austria Criminal Code (Strafgesetzbuch – StGB), Sections 99, 105, 106, 106a, 107, 107a, 107b, 107c, 109.

cohabitation is assumed in cases of doubt. Offences against minor (adopted or foster) children of the accused or their spouse, registered partner, or partner, as well as against direct-line relatives or the brother or sister of the accused, are also included in this category. Other relatives[88] of the accused are recorded only if criminal police report that they live together in the same household.

Through identifier analysis in the case automation system, it is now possible to identify key metrics for this category of offences, including the number of cases opened, indictments, alternative measures, and court actions.[89] Additionally, data on convictions, acquittals, case closures, and investigation proceedings are now accessible.

This tracking system provides valuable data and also allows some conclusions as to the relationship between the victim and the perpetrator and the recording of the same. However, the absence of the crucial disaggregation of data by perpetrator-victim relationship at the judicial level does not capture the specifics of the familial relationship but categorises it within a broad group of close relations. This results in some inherent ambiguity in the data and, consequently, in the lack of a comprehensive view of criminal justice responses to different forms of violence against women.

With the intent to provide a more solid basis for evidence-based policy-making, the case automation system is constantly enhanced (most recently by an extension of the offence codes for recording of prejudice motives), and further upgrades are in the pipeline. Recording the relationship between the victim and the perpetrator in the case automation system will be considered the next expansion phase, which will also require an analysis of the technical upgrades required in this context.[90]

Challenges and ongoing efforts in data collection within Austria's justice system focus on improving tracking and alignment between different governmental bodies. A significant challenge in criminal justice data collection arises from the distinct approaches used by the Ministry of the Interior (police) and the Ministry of Justice, resulting in a lack of alignment between their systems. The Ministry of

88 See the Austria Criminal Code (Strafgesetzbuch – StGB), Section 74.

89 See the Austria Criminal Code of Procedure (Strafprozeßordnung – StPO), Sections 200 -204.

90 See the Comments submitted by Austria on GREVIO's first thematic evaluation: Building trust by delivering support, protection and justice. Received by GREVIO on 10 September 2024, GREVIO/Inf(2024)9. Published on 10 September 2024, p 17. Available at https://rm.coe.int/austria-s-comments-on-grevio-s-first-thematic-evaluation-report/1680b18c9b

the Interior, responsible for police operations, employs an event- or offence-based method of recording data, where each offence is logged separately. In contrast, the Ministry of Justice uses a case-based approach, consolidating multiple offences committed by a single perpetrator into one case. This fundamental difference creates discrepancies between the two datasets, often giving the impression that fewer cases are processed through the justice system than initially recorded by the police.

This discrepancy, occasionally amplified by media coverage, can contribute to a perception of judicial inaction or inefficiency. Journalists and the public may interpret the lower number of cases as a lack of responsiveness in the judiciary.

This issue, however, cannot be resolved purely at a technical level, as each method is established by law. However, authorities are working to harmonise data collection methods across the police and judiciary to bridge these gaps. Efforts include expanding the interface between the Ministry of the Interior and the justice system to improve data reliability and ease workloads. For instance, recent updates have incorporated the "prejudice motive" offence identifier, with further expansion planned for 2024 to meet growing statistical demands. Additionally, maintaining a comprehensive "list of facts" in criminal proceedings, which could cover various statistical requirements, would require significant human resources, even if some data can be carried over from criminal police records.[91]

Dedicated Systems with a Compartmentalised Structure (the Spanish case study)[92]

Spain has developed a structured legal and policy framework to address various forms of violence against women. Initiated with Organic Law 1/2004, which focused on gender-based violence in intimate relationships, Spain's approach has expanded over the years to encompass additional forms of violence, including stalking, harassment, and sexual violence. The country's legislative measures are supported by specialised courts and law enforcement protocols, aiming to provide targeted protection and judicial support for victims.

91 See the Implementation report submitted by Austria on the conclusions adopted by the Committee of the Parties on 7 December 2021, IC-CP/Inf(2023)22. Received on 7 December 2023, Published on 8 January 2024. Available at https://rm.coe.int/ic-cp-inf-2024-01-reply-by-austria-to-reporting-form-on-implementatin-/1680ae1a87

92 The information in this section was gathered through documentary research as well as in-depth interviews and materials provided by the Digital Transformation Service of the Spanish Ministry of Justice.

While comprehensive protections against OTFVAW are still limited, legislation has evolved to cover certain digital forms of abuse. Organic Law 10/2022 along with prior reforms criminalise criminal conducts perpetrated online or using digital means (e.g. cyberstalking and unauthorised sharing of intimate content). Also, at the regional level, autonomous communities have launched educational campaigns and initiatives to raise awareness about digital abuse, particularly aimed at young people, in addition to public campaigns.

These regulatory efforts are reflected in the design of data collection systems, the development of their functionalities, and the ways in which the data is used—both to track crime and monitor social phenomena, as well as to draw lessons for more effective prevention and law enforcement policies. The Spanish system stands out for its dedicated and specialised approach to addressing violence against women. Some of these information systems are intentionally designed to capture these social phenomena and are adaptable to an increasingly broad and complex landscape, all while demonstrating a growing and significant integration effort.

Legislative and policy context concerning cyber violence against women

Since 2004, Spain has been a pioneer in tackling gender-based violence, with a strong focus on violence against women within intimate or former partner relationships. The Organic Law 1/2004, passed on December 28, set out Comprehensive Protection Measures against Gender-Based Violence, defining such violence as a manifestation of discrimination, inequality, and power imbalances exerted by men over women. This legal commitment has also led to institutional reforms, including the establishment of specialised courts for cases arising from these crimes, ensuring focused and expert handling.

Spain's legal framework also addresses stalking; Article 172 of the Criminal Code criminalises persistent, intrusive behaviours such as following, contacting, or collecting personal information about a victim. Notably, these behaviours are prosecutable even if they do not directly instil fear but disrupt the victim's life. In 2015, protections were extended to cover digital harassment under Article 172 ter, explicitly criminalising "cyberstalking" and positioning Spain among the first European nations to address online stalking formally.

More recently, to address low awareness of other forms of violence against women, including female genital mutilation (FGM), forced marriage, sexual harassment,

and sexual violence, Spain has expanded its legislation and policies. Among recent milestones, the Organic Law 10/2022, approved on September 6, 2022, introduced comprehensive guarantees for sexual freedom and focused on tackling sexual violence. In addition, several regulations have been enacted from 2020 to 2023, contributing to a broader legislative foundation.

In the realm of OTFVAW, while there is room for improvement in legislation and sector-specific policies, notable developments have emerged. The Organic Law 10/2022 is particularly significant in addressing sexual violence in digital environments, targeting acts such as the unauthorised dissemination of sexual content, non-consensual pornography, and sextortion.

Efforts at the autonomous community level further extend these protections, focusing on issues like technology-facilitated abuse and control. For example, initiatives targeting young people educate them on the dangers of installing spyware or engaging in sextortion. One of the most recent developments is Ley 15/2021, adopted by the Galician Parliament on December 3, 2021, which amends the regional Law 11/2007 to expand protections for women who suffer digital forms of gender violence.

Additionally, civil society has launched campaigns to raise awareness about digital violence in relationships, with an emphasis on helping young people recognise and address early signs of abuse, such as controlling behaviour via mobile devices or social media. Some of these initiatives also address sexual violence among teenagers, fostering early awareness. More recently, institutional campaigns have been held on March 8 (International Women's Day) and November 25 (International Day for the Elimination of Violence against Women). Campaigns like "Formas Parte," aimed at preventing digital violence, and "No, y punto," along with other efforts against male violence during local festivities, have raised public awareness.

In response to the growing digital threat, as recognised by the Ministry of the Interior's Directorate General of Police, Spain has equipped its Cybercrime Units within the National Police and Guardia Civil with specialised tools to investigate online sexual crimes effectively. The Guardia Civil also operates technological crime units under its Judicial Police Headquarters, dedicated to addressing digital offences. Moreover, the gender violence units within the provincial prosecutor's offices are authorised to intervene in all related criminal proceedings, even from the preliminary stages, particularly in cases within the jurisdiction of the specialised courts for violence against women, as per Article 87 of Organic Law 6/1985 of the Judiciary.

Furthermore, judicial magistrates receive in-service training on issues related to gender violence, including topics such as online gender violence, the digital gender gap, practical approaches with a gender perspective, best practices, protection measures for women and children affected by gender violence, and labour rights related to work-life balance in cases involving violence against women. This training ensures that Spain's judicial system remains equipped to address and understand the complexities of gender violence in both physical and digital spaces.

Data collection approach and developments in the field of violence against women

Historically, Spain has been recognised for its thorough collection of statistical data on gender-based violence. In recent years, the country has taken deliberate steps to enhance these capabilities further, especially over the past four years, with a significant increase in its capacity to gather, process, and disaggregate data on violence against women. Key institutional actors, including the Ministry of the Interior, the General Council of the Judiciary, the Directorate General of the Public Justice Service at the Ministry of the Presidency, Justice, and Relations with the Courts, have collectively developed advanced methods for data collection and categorisation. These efforts focus on tracking specific case types and outcomes and are especially attentive to variables such as the age and sex of victims and offenders, the type of violence, and the relationship between involved parties.

Law enforcement data

In Spain, the Ministry of the Interior compiles and publishes monthly data on intimate partner violence against women,[93] which is entered by law enforcement agencies and other public institutions into the Integrated Monitoring System for Gender Violence, better known as VioGén.

VioGén system, overseen by the Secretary of State for Security within the Ministry, has been operational since July 26, 2007, and was created in response to Law 1/2004, "Ley Orgánica de Medidas de Protección Integral contra la Violencia de Género" (LOMPVIG).[94] Articles 31 and 32 of this law form the legal basis for the

93 Monthly statistical reports are available at: www.interior.gob.es/ca/web/servicios-al-ciudadano/violencia-contra-la- mujer/estadisticas

94 The system was developed by the Office of Internal Security Studies (GESI, by its Spanish acronym) within the SES to support the implementation of the general mandates outlined in Articles 31 and 32 of Organic Law 1/2004, dated December 28. This law addresses "comprehensive protection measures against gender violence."

system, mandating institutional protections and structured collaboration between public security forces in matters of gender-based violence.[95]

LOMPVIG's provisions led to the establishment of specialised police units tasked with preventive monitoring and enforcement of court-issued protective measures in gender violence cases. Also, to standardise police response, they called for protocols governing the work of law enforcement in this field, which in turn inspired the 2007–2008 National Plan for Awareness and Prevention of Gender-Based Violence and the comprehensive monitoring system now known as VioGén.[96] Police powers were later extended in 2015 to include the assessment of victim risk through Article 282 of the Criminal Procedure Act, amended by the Crime Victims' Statute Act.[97]

Cases are initiated in VioGén upon the filing of a complaint and are defined as specific incidents involving a victim and an identified offender; thus, each victim-offender pair is registered as a separate case. This structure means that each unique victim-offender relationship is treated distinctly, with multiple cases assigned if a victim suffers violence from different offenders or if an offender harms multiple victims. Each case is assigned to a specific police unit according to the victim's residence, with that unit bearing responsibility for ongoing monitoring and exclusive authority to update case records.[98]

The system collects extensive data on crimes related to gender violence, including offender criminal records, legal restrictions (such as restraining orders), and the offender's prison status. Additionally, it records identifying information—such as personal identification numbers, photographs, contact details—and demographic data like family relations, employment status, and marital status. VioGén also

95 González-Álvarez et al. 2018.

96 Sánchez López 2020.

97 VioGén, Spain's comprehensive monitoring system for gender violence cases, is implemented nationwide, except in Catalonia and the Basque Country. In these regions, autonomous police forces—the Mossos d'Esquadra in Catalonia and the Ertzaintza in the Basque Country—utilize their own risk assessment and management protocols. The Basque Country specifically employs the EBA (Emakumeen eta Etxekoen Babesa) platform, operational since 2007 and updated in 2010 to EPV-R. Although VioGén is not directly applied in these autonomous communities, efforts have been made to ensure interconnection and coordination between the national system and regional police forces. This collaboration seeks to facilitate information sharing and enhance victim protection across jurisdictions. However, details regarding the scope and effectiveness of this interconnection remain limited. See Farías Pereira 2024; Sánchez López 2020; González-Álvarez et al.2018.

98 González-Álvarez et al. 2018; Farías Pereira, 2024.

gathers information on support services provided to victims, which includes shelter use and other forms of assistance from various support agencies.[99]

In VioGén, a case encompasses all information linking a specific victim to a specific aggressor. Should a victim face violence from multiple offenders, or if a single offender has multiple victims, distinct cases are generated for each unique relationship. A case is active while subject to police monitoring, adapting over time as its risk level changes. It becomes inactive when police monitoring is no longer required but may be reactivated if risk levels rise. Cases classified as "low risk" may be closed under specified conditions.

To avoid duplicative data entry across different databases, VioGén integrates with other criminal information systems (e.g., the Prison Information System N-SIP), and efforts are being made to further integrate interfaces with other services, including social and welfare services in the Autonomous Communities.[100]

To ensure detailed reporting, the Ministry of the Interior publishes monthly statistical summaries from VioGén, which are available on both the Ministry's official website and the Statistical Portal of the Government Delegation against Gender-Based Violence. These reports offer granular insights into patterns and instances of gender violence across the country.[101]

Significantly, VioGén is designed as a dynamic tool that functions beyond data monitoring, supporting Spain's risk assessment protocols. It is aimed at enhancing victim protection, monitoring the evolution of risk in individual cases, issuing alerts as risk levels change, and facilitating appropriate protective responses. The system's core objectives include victim protection, crime prevention, and offender containment, while it also serves secondary roles in statistical tracking and victim support.[102]

99 González-Álvarez et al. 2018.

100 See European Commission – Interoperable Europe, Public Sector Tech Watch, Viogen 5.0: discovering Spain's risk assessment system of gender-based violence. Available at https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch/viogen-50-discovering-spains-risk-assessment-system-gender-based-violence

101 Report submitted by Spain pursuant to Article 68, paragraph 1of the Council of Europe Convention on preventing and combating violence against women and domestic violence (1st thematic evaluation round). Received by GREVIO on 12 February 2024, GREVIO/Inf(2024)1. GREVIO/Inf(2024)1. Available at https://rm.coe.int/grevio-inf-2024-1-spain-1st-thematic-evaluation-round-eng/1680ae0c38 Published on 13 February 2024

102 González-Álvarez et al. 2018.

Central to VioGén is its integration with the Police Risk Assessment questionnaire (VPR), which establishes an initial risk assessment upon the registration of a complaint. Following any significant incident, or at scheduled intervals, cases are re-evaluated using the VPER (Evolving Risk Assessment) questionnaire, which takes into account new developments, such as fresh complaints or protection order breaches.

The information entered in the questionnaires can be derived from various sources, including the victim's statements, witness testimonies, and police records, among others.[103] Thus, once the VPR questionnaire is applied, the system displays a designated level of risk, and for each level, specific protective measures are associated.[104]

In addition, a new scale (VPR5.0-H) has recently been incorporated into the questionnaire to predict the risk of femicide. This scale comprises 13 indicators and categorizes risk into two levels: low and high. Consequently, as of March 2019, the VioGén form contains two scales, each with its respective algorithm.[105]

The VPER questionnaire, by contrast, incorporates any new information or incident relevant to adjusting the risk level over time.[106] This questionnaire should be updated at the request of a judge or prosecutor, upon the occurrence of a relevant event (e.g., a new complaint or breach of protection measure), or at the discretion of the police.[107] The frequency of police reviews is contingent upon the risk level associated with each case, meaning that higher-risk cases undergo more frequent assessments.[108] Initial risk assessments and subsequent updates are communicated to the courts and the public prosecutor's office,[109] whereupon the judiciary evaluates the necessity of precautionary measures to safeguard the victim.[110]

In March 2019, an additional risk assessment scale, VPR5.0-H, was introduced to predict femicide risk, evaluating 13 indicators to categorize cases as either low or high risk. The VPER is updated upon relevant incidents, judicial or prosecutorial request, or through police initiative. The update frequency depends on the assessed

103 Sánchez López 2020.
104 González-Álvarez et al. 2018.
105 González-Álvarez et al. 2020.
106 González-Álvarez et al. 2018.
107 Sánchez López 2020.
108 *Ibid*.
109 González-Álvarez et al. 2018.
110 Sánchez López 2020.

risk level, with higher-risk cases requiring more frequent evaluations. Initial and modified risk assessments are communicated to the judiciary and prosecutors, informing decisions on potential precautionary measures to protect victims.[111]

VioGén offers a range of additional functionalities. First, it automatically issues notifications to users, alerting them to deadlines, situational changes, and other significant updates, enabling law enforcement officers to stay informed of critical developments. Among the most noteworthy features is a tool for transmitting critical incident information, which allows for the rapid exchange of urgent or significant updates among specialists involved in case management. This module primarily supports violence prevention by promptly informing law enforcement personnel, who must verify the validity of incidents prior to taking necessary action. Furthermore, the module accommodates multimedia attachments and documents deemed important, and it enables users to select specific recipients in addition to those automatically designated by the system.

Other significant components of the VioGén System include the statistical module, a subsystem for deceased victims of gender violence, a case unification function, a user management module, and modules for the efficient administration of system entities (such as templates, units, and districts).

Like any advanced digital system, VioGén is technically equipped for expansion as needed. While its current scope is limited to specific forms of gender violence cases, it could potentially extend to include additional vulnerable groups, thereby enhancing protection for the most at-risk populations and allowing for the development of tailored security strategies responsive to their specific needs.

Judicial data

In Spain, the General Council of the Judiciary (Consejo General del Poder Judicial, CGPJ), which is the governing body of the Spanish judiciary, is responsible for gathering data on cases of intimate partner violence at all stages of the judicial process, covering both general criminal courts and specialised violence against women courts. This data includes specifics on the number of charges brought and dropped, protection orders requested, granted, and denied, as well as details on the types of procedures initiated and their outcomes. Data is largely disaggregated by age, sex, perpetrator-victim relationship, type of intimate partner violence

111 González-Álvarez et al. 2020.

(including physical, psychological, sexual, and honour-related violence), and geographical location, such as autonomous community.

The CGPJ's data also includes information on the number of civil cases related to gender-based violence brought to the specialist violence against women courts. These cases commonly involve matters of divorce, child custody, and visitation rights.

Data collection efforts in other forms of violence against women, such as rape and sexual violence, have been less comprehensive in the past, but significant developments occurred more recently.

As an example, an expansion has been registered concerning data on **femicide**. Since 2003, Spain has tracked the murders of women in the context of intimate partner or ex-partner violence (referred to as gender-based violence); however, in response to international human rights commitments and a historical demand from the feminist movement, the Government Delegation against Gender-Based Violence extended, effective January 1, 2022, the scope of femicide data to include all forms of violence against women. This expansion makes Spain the first European country to publish statistical data on femicides across multiple categories, adopting the UN Special Rapporteur's general definition of "femicide," consistent with the European Institute for Gender Equality (EIGE) glossary. This data now categorises femicides into:

- Intimate Partner or Ex-Partner Femicide
- Family Femicide
- Sexual Femicide (as established in Organic Law 10/2022 on the Comprehensive Guarantee of Sexual Freedom)
- Social Femicide
- Vicarious Femicide: This includes minors killed as a result of violence against women and is classified further as either vicarious (when the woman was not killed in the same event) or non-vicarious (when the woman was killed in the same event).

Important developments have also concerned data on crimes affecting **sexual freedom**. The CGPJ has incorporated a new study on sentences for crimes against sexual freedom. Developed by the Observatory against Domestic and Gender Violence, the study seeks to expand knowledge on violence against women by

analysing judicial decisions and judicial statistics. Its first edition, published in 2022, examines Supreme Court rulings on gender violence cases from 2020. Since 2002, the Observatory has conducted annual studies on deaths related to gender violence based on data from the relevant courts, and it publishes an annual report analysing the circumstances and characteristics of all gender violence-related femicides. These reports give special attention to cases where prior records of violence existed. New indicators recently incorporated into these reports include analyses of:

- Legal qualification of offences
- Circumstances modifying criminal liability, specifically mitigating and aggravating factors
- Related offences
- Socio-economic characteristics of both the victim and the aggressor, which is currently being further developed.

As a result of these efforts, two significant reports addressing gender violence-related femicides have been made public. One of them addresses fatal victims in cases where the perpetrator is an intimate partner or ex-partner.[112] The second one is an analysis of sentences from 2020 on gender-based and domestic violence-related homicides or murders.[113]

To further support disaggregated data collection, the General Council of the Judiciary has recently expanded its publication of detailed data in several critical areas.

The first area covers Emergency Barring Orders, Protection Orders, and Related Breaches. Courts and Tribunals must now submit quarterly reports on the issuance of emergency barring and protection orders, including data on order breaches and resulting sanctions. This information is consistently published in mandatory statistical bulletins, ensuring regular and comprehensive updates.

112 See Poder Judicial Espana, Informe sobre víctimas mortales de la violencia de género y doméstica en el ámbito de la pareja o expareja en 2021. Published 17 January 2023. Available at https://www.poderjudicial.es/cgpj/es/Temas/Violencia-domestica-y-de-genero/Actividad-del-Observatorio/Informes-de-violencia-domestica-y-de-genero/Informe-sobre-victimas-mortales-de-la-violencia-de-genero-y-domestica-en-el-ambito-de-la-pareja-o-expareja-en-2021

113 See Poder Judicial Espana, Análisis de las sentencias dictadas en el año 2020 relativas a homicidios o asesinatos por violencia de género y doméstica. Published 26 June 2023. Available at https://www.poderjudicial.es/cgpj/es/Temas/Violencia-domestica-y-de-genero/Actividad-del-Observatorio/Informes-de-violencia-domestica-y-de-genero/Analisis-de-las-sentencias-dictadas-en-el-ano-2020-relativas-a-homicidios-o-asesinatos-por-violencia-de-genero-y-domestica

The second area involves Custody Restrictions and Parental Rights Withdrawal. Quarterly data is also provided on cases where custody decisions have led to the restriction or withdrawal of parental rights due to violence by one parent against the other. These updates have gained particular importance following modifications introduced by Organic Law 8/2021, which maximizes restrictions on parents under investigation for gender-based violence, severely limiting their custody and visitation rights to safeguard the welfare of the children involved.

Data Collection and Analysis Initiatives by the Ministry of Justice and Related Agencies

The Directorate General of the Public Justice Service, part of Spain's Ministry of the Presidency, Justice, and Relations with the Courts, serves as a key body in consolidating and coordinating data related to gender-based violence. To monitor and report on gender-based violence cases, the Directorate compiles annual activity reports from the Institutes of Legal Medicine and Forensic Sciences (IMLCF), which are then sent to the State Observatory on Violence against Women under the Ministry of Equality and to the National Commission on Judicial Statistics. These reports provide insights, forming a basis for evaluating the impact of forensic and legal interventions on gender-based violence.

To further enhance both public transparency and internal oversight, the Directorate has initiated the development of two specialised scorecards. One scorecard is designed for internal use, enabling government agencies and judicial entities to access up-to-date information on gender-based violence cases and response efforts. The second is a public-facing portal that provides daily information on actions undertaken by the Comprehensive Forensic Assessment Units (UVFI) of the IMLCF, giving citizens a clearer view of the scope and responsiveness of forensic support in these cases.

The Directorate also manages a robust data catalogue, developed in collaboration with the National Institute of Toxicology and Forensic Sciences (INTCF), that includes detailed toxicological findings on cases of suspected chemical submission in sexual assaults that can enable the identification of specific trends and risk factors associated with these crimes.

A major component of the Directorate's work is its oversight of the System of Administrative Support Records, or SIRAJ, which consolidates records on gender-based violence across the criminal justice system and improves coordination

and response capabilities across jurisdictions, ensuring that all operators within the justice system have timely access to information. The recent launch of SIRAJ 2 in 2022 has integrated multiple previously separate databases, centralising records on adult and juvenile offenders, victims of domestic and gender-based violence, and sex offenders.[114]

Further supporting national data efforts, the Directorate maintains the Central Registry for the Protection of Victims of Domestic and Gender-Based Violence, a database that forms the foundation of the Statistics of Domestic Violence and Gender-Based Violence. Managed by the National Statistics Institute (INE) since 2011, this registry tracks victims and suspects under precautionary measures or protection orders. In 2023, for the first time, child victims were included, with data showing that 1,376 minors, including children in care, custody, or cohabitation with victims, were recorded in 2022 as victims of gender-based violence.

Additionally, the Directorate oversees the Central Register of Sexual Offenders, which supplies data to the INE's Conviction Statistics, including statistics on individuals convicted of sexual offences. This register, by tracking convictions related to sexual and gender-based violence, enables policymakers to assess long-term trends in offender behaviour and the effectiveness of judicial measures.

Developments in data collection at the Public Prosecutor's Office

In the justice sector, the Public Prosecutor's Office has introduced new categories in data collection and analysis. Specifically, regarding completed and attempted femicides and other severe acts of physical, psychological, or sexual violence, data is now analyzed by factors such as the sex and age of both victim and assailant, their relationship, the means of the assault, and the location of the incident. A quantitative study has been added to examine the incidence of completed and attempted femicides and other severe acts in rural areas, breaking down data by population clusters and further by whether or not the victim had previously reported the crime. This study has revealed a lower incidence of prior reports in

114 In accordance with the provisions of Chapter III of Royal Decree 95/2009, dated February 6, which regulates the SIRAJ, the information contained within the system includes, among other records, the Central Registry for the Protection of Victims of Domestic and Gender-Based Violence, which logs sentences and security measures imposed in cases of crimes or misdemeanors, along with precautionary measures and protection orders issued in ongoing criminal proceedings. It also includes the Central Register of Precautionary Measures, Requisitory Measures, and Non-Final Judgments, and the Central Register of Convicted Persons, which records final judgments for crimes or misdemeanors, detailing penalties or security measures imposed by criminal courts or tribunals on individuals of legal age.

smaller population clusters. Additionally, the factors of disability and migrant status have been introduced to assess the impact of violence against women with disabilities and migrant women.

Specialised and holistic data collection systems (the Portuguese case study)

In recent years, Portugal has significantly advanced its policies on domestic violence and gender-based violence (VAW), reflecting the rising importance of data collection, analysis, and policy formulation to prevent and address these complex issues. The systematic gathering and processing of data on violence against women and domestic violence has become a national priority, essential to developing effective interventions and protection measures for vulnerable populations. Recognised as critical by international organisations, this focus has informed Portugal's commitment to continually refining and expanding its data infrastructure on violence against women.

Currently, Portugal is in the process of implementing an advanced, integrated data system on violence against women, intended for launch in early 2025. This system, evolving since 2018, incorporates the insights and contributions of multiple government agencies and organisations. Centralising data from key actors in urban and rural areas, the new database will enable the comprehensive collection of data from the justice system and police forces and aims to consolidate, standardise, and expand the existing data sources in use. It will ultimately replace the present database, which is supposed to remain operational until the end of 2024, providing a foundation of historical data upon which the new database will be built.

Legislative and policy context concerning cyber violence against women

Portugal has increasingly recognised cyber violence against women as a serious issue that requires targeted legislative responses, especially given the global rise in online harassment, stalking, and non-consensual sharing of intimate images. Although the country does not yet provide independent classifications for offences of violence committed via the internet and does not have a single comprehensive law dedicated to cyber violence against women, recent legislative reforms and policies reflect a shift towards more protective measures.

Notably, the Portuguese Charter on Human Rights in the Digital Age, enacted through Law 27/2021 on May 17, emphasises the application of constitutional rights, freedoms, and protections within cyberspace. This law mandates the Portuguese state to foster a digital environment conducive to human rights, including gender equality and protection against online violence. Specifically, Article 3 calls for initiatives to combat the spread of illegal content online and defend cybercrime victims, reflecting Portugal's broader commitment to addressing online violence against women through legal and policy frameworks.

Along with this, in recent years, the Portuguese government has integrated protections within its criminal framework. In Portugal's Criminal Code, cyber elements often appear as aggravating or essential factors in certain crimes. For example, Article 176a criminalises the grooming of minors for sexual purposes explicitly when conducted "(...) by means of information and communication technologies (...)." Similarly, in the offence of child pornography, the Code explicitly references (though not exclusively) the use of computer systems for actions such as acquiring, possessing, accessing, obtaining, or facilitating access to pornographic content involving minors, as well as aiding, facilitating, or enabling access to pornographic performances involving minors (Article 176(5) and (6)).

Also, in cases where offences involve the internet or other widespread dissemination methods as aggravating factors, certain legal consequences follow. For example, the minimum sentence for domestic violence increases from 1 to 2 years if the perpetrator "disseminates through the Internet or other means of widespread public dissemination, personal data, particularly images or sounds, relating to the privacy of one of the victims without their consent" (Article 152(2)(b)). Additionally, offences against privacy, as defined in Articles 190 to 195, incur a penalty increase of one-third for minimum and maximum sentences if committed via media or by broadcasting through the internet or other widely accessible platforms (per Article 197). Crimes of defamation and insult (Articles 180 to 182) are subject to a similar aggravation: penalties are increased by one-third in their minimum and maximum terms if the offence is carried out under conditions that facilitate broader dissemination (as per Article 183). The proposed increases in penalties specifically target offences committed or promoted using information and communication technologies, including threats (Article 153), stalking (Article 154a), coercion (Article 163), sexual fraud (Article 167), sexual immorality (Article 170) and nearly all offences against sexual self-determination (Articles 171 to 176a), such as sexual abuse of children, abuse of minors who are dependent or in vulnerable situations, sexual acts with adolescents, and the exploitation or prostitution of minors, as well as child pornography and grooming for sexual purposes.

Also contributing to this path of strengthening legal protections against digitally perpetrated forms of violence is the Cybercrime Act, passed by Law 109/2009 on 15 September, which provides substantive and procedural provisions for cybercrime, and the more recent National Strategy for Security in Cyberspace, established by Council of Ministers Resolution No. 92/2019 (5 June), which lists in Article 177 the circumstances that aggravate penalties for crimes against sexual freedom and self-determination.

Overall, Portugal's legislative progress reflects an ongoing commitment to addressing cyber violence against women, also marked by the most recent reform proposals that mark a critical shift in addressing digital forms of gender-based violence. Projeto de Lei 347/XV/1[115] proposes greater protection for victims of non-consensual sharing of intimate content, recommending changes to the Penal Code and e-commerce regulations to safeguard personal data better. To complement this, Projeto de Lei 157/XV/1[116] seeks to establish clear criminal liability for the unauthorised distribution of intimate or sexual material, recognising the harm this practice inflicts on victims. Furthermore, Projeto de Lei 208/XV/1[117] introduces the crime of non-consensual pornography, outlining specific penalties and updating both the Criminal Code and the Code of Criminal Procedure to strengthen the legal consequences of these actions. Finally, Projeto de Lei 780/XV/1[118] broadens the scope by proposing the criminalisation of various forms of cyberviolence, recognising the increasingly complex ways in which women can be abused online. Overall, these proposals reflect Portugal's forward-looking approach to adapting its legal framework to the realities of digital abuse, offering a more comprehensive protective response to the evolving challenges of online violence.

Legislative and policy context concerning data collection

For over 15 years, Portugal has maintained records on violence against women, which have been collected through annual reports like the Annual Domestic

115 Projeto de Lei 347/XV/1, Reforça a proteção das vítimas de crimes de disseminação não consensual de conteúdos íntimos, alterando o Código Penal e o Decreto-Lei n.º 7/2004, de 7 de janeiro, que aprova o Comércio Eletrónico no Mercado Interno e Tratamento de Dados Pessoais, DAR II série A n.º 93, 2022.09.30, da 1.ª SL da XV Leg (pág. 51-54)]

116 Projeto de Lei 157/XV/1, Prevê o crime de divulgação não consentida de conteúdo de natureza íntima ou sexual, [DAR II série A n.º 42, 2022.06.15, da 1.ª SL da XV Leg (pág. 48-51)]

117 Projeto de Lei 208/XV/1, Criação do crime de pornografia não consentida (55.ª alteração ao Código Penal e 45.ª alteração ao Código do Processo Penal), [DAR II série A n.º 51, 2022.07.01, da 1.ª SL da XV Leg (pág. 10-14)]

118 Projeto de Lei 780/XV/1, Prevê a criminalização da ciberviolência, DAR II série A n.º 223, 2023.05.12, da 1.ª SL da XV Leg (pág. 58-60)]

Violence Monitoring Report and the Annual Internal Security Report (RASI), also processing information on the crime of homicide in the context of a parental/family and conjugal/analogue relationship.

A pivotal development was the enactment of Despacho n.º 16/98, de 9 de março, which introduced an autonomous statistical category for domestic violence, making it possible to document 21 distinct types of offences related to family and intimate relationships under the Criminal Code, thus enhancing the visibility and accuracy of domestic violence data and ensuring it could be tracked and analysed separately from other crimes.

This categorisation marked a shift in understanding domestic violence not merely as a general crime but as a separate category deserving focused attention, thereby guiding policy and resource allocation. Crucially, the focus on separate statistical recording played an essential role in shaping public policy, improving victim support, and recognising the true scale of domestic violence in Portugal. It also facilitated the development of procedures for systematically collecting domestic violence data, resulting in a series of indicators that provided a more comprehensive grasp of the issue.

The Despacho, alongside subsequent amendments, strengthened mechanisms for reporting cases, gathering data, and ensuring adequate responses from authorities, including law enforcement and victim support services.

The launch of *Programa INOVAR* in **1999**[119] reinforced this commitment by empowering the National Republican Guard (GNR) and Public Security Police (PSP) to adopt data-driven approaches and offer enhanced public safety services to support vulnerable groups, particularly women and the elderly. Extended in 2002, this program underscored the need for structured data collection and evidence-based public policy.

In parallel with these efforts, legislation has continuously evolved to support a systematic approach to addressing domestic violence. In **2007,** the Domestic Violence Database (BDVD) was established, following the introduction of the Domestic Violence Report Form (Auto VD) in 2006. The BDVD has since served as a central repository for domestic violence cases, aiding knowledge development, criminal

119 See Presidência do Conselho de Ministros, Resolução do Conselho de Ministros n.º 6/99 de 8 de Fevereiro, Diário da República n.º 32/1999, Série I-B de 1999-02-08. Available at https://dre.tretas.org/dre/99772/resolucao-do-conselho-de-ministros-6-99-de-8-de-fevereiro

investigations, and policymaking by allowing law enforcement to assess risk, track case progress, and monitor ongoing interventions. In **2015**, *Lei n.º 129/2015*[120] formalised the BDVD, assigning data management responsibilities to the Secretaria-Geral do Ministério da Administração Interna (SGMAI) and explicitly limiting access to authorised personnel who are bound by confidentiality obligations. The law stipulated that data collected through the BDVD would support criminal policies and internal security initiatives, assisting entities like the Public Prosecutor's Office and security forces.[121]

These achievements did not, however, constitute a point of arrival but the first step towards the realisation of an information processing system based on a comprehensive and integrated view of homicides and other forms of violence against women and domestic violence. In 2018, BDVD was accredited by the National Commission for Data Protection. Then, the Council of Ministers Resolution No. 139/2019, dated 19 August, prioritised the enhancement of official data collection on violence against women and domestic violence. This resolution highlighted the importance of defining a comprehensive set of relevant data and indicators derived from various collection mechanisms and information systems, which require adaptation and harmonisation. Additionally, it called for improved interoperability and centralised access to these data, culminating in reforming the database referenced in Law 112/2009 of 16 September.

Law No. 57/2021, enacted on 16 August, formally approved these amendments, thereby establishing the "Database on Violence against Women and Domestic Violence" (BDVMVD). This updated database is designed to incorporate a wider scope of data and indicators, not only from the originally identified source entities but also from additional agencies specified in the Council of Ministers Resolution No. 139/2019. This initiative requires a collaborative effort involving at least ten source entities, encompassing various governmental sectors and the Attorney General's Office, alongside the General Secretariat of the Ministry of Internal Affairs (SGMAI), which oversees the BDVMVD's overall management

120 Lei n.º 129/2015, de 03 de Setembro, Terceira alteração à Lei n.º 112/2009, de 16 de setembro, que estabelece o regime jurídico aplicável à prevenção da violência doméstica, à proteção e à assistência das suas vítimas, Diário da República n.º 172/2015, Série I de 2015-09-03, Artigo 37º-A. Available at https://diariodarepublica.pt/dr/detalhe/lei/129-2015-70179158

121 For an overview of Portuguese legislation in the field of Gender and Domestic Violence, see the website of the Assembly of the Republic. Available at https://www.parlamento.pt/Legislacao/paginas/legislacao_areaviolenciadomestica.aspx

A Comprehensive Approach to Data Collection: Transitioning from BDVD to BDVMVD[122]

In Portugal, data management for domestic and gender-based violence is undergoing a substantial upgrade with the transition from the Database on Domestic Violence (BDVD), established in 2015 and operational until the end of 2024, to the Database on Violence against Women and Domestic Violence (BDVMVD), set to launch in early 2025.

The BDVD, active since 2015, was originally created to improve understanding of domestic violence and support criminal justice and internal security policies. This database was designed to provide analytical insights and support criminal justice and internal security policies by capturing domestic violence trends, all while ensuring individual privacy by excluding personal identifiers. Through its structured data, the BDVD has also supported preventive and investigative efforts by the Public Prosecutor's Office and Security Forces.

The BDVD's data is sourced mainly from the two primary police forces under the Ministry of Internal Affairs: the Public Security Police (PSP), which operates in urban areas, and the National Republican Guard (GNR), which serves smaller towns and rural areas. Although they function as distinct entities with separate jurisdictions, both forces adhere to the same indicators and use identical data-collection forms to contribute to the database. This consistency across organisations has allowed the BDVD to operate as a unified source of information, covering the entire country despite differing local responsibilities

The current database systematically captures data through standardised forms, including reports on domestic violence incidents and risk assessments completed during initial contacts (RVD 1L) and subsequent follow-ups (RVD 2L). In addition, it records safety-related actions such as information-sharing across agencies, weapon seizures, protective measure applications, and the creation of safety plans. This comprehensive range of information has enabled the database to act as a key resource for law enforcement agencies and the Secretaria-Geral do Ministério da Administração Interna (SGMAI), who rely on its data for decision-making and policy development.

122 The information in this section was gathered through documentary research as well as in-depth interviews and materials provided by the Comissão para a Cidadania e a Igualdade de Género (CIG), the national body responsible for promoting and defending this principle. The CIG aims to address the significant social and political changes in society related to citizenship and gender equality. It is one of the key institutional actors actively involved in the efforts to implement the information systems under consideration in Portugal.

The focus is exclusively on administrative data. Each time a new complaint is filed with the police, judiciary, or prosecutor's office, a case is created in the system, allowing for the comprehensive collection of related administrative data.

Broader Data Integration in the BDVMVD

The upcoming Database on Violence against Women and Domestic Violence (BDVMVD) represents a significant expansion over its predecessor, the BDVD. Designed with a broader scope, the BDVMVD will integrate data from a wide range of public services that collect information on various types of violence, including sexual, cyber, physical, and economic violence. The primary goal of this new database is to consolidate information to support effective protection for victims and improve criminal justice and internal security policies. Additionally, the BDVMVD will contribute to the production of enhanced statistical data on violence, aided by connections to a broader IT platform.

Data for the BDVMVD will come from an expanded list of sources beyond the Public Security Police (PSP) and the National Republican Guard (GNR). It will also include information from the Polícia Judiciária, a specialised police force under the Ministry of Justice, which operates in close coordination with the Public Prosecutor's Office to handle complex cases such as homicide, sexual violence, and human trafficking. Furthermore, the BDVMVD will integrate with the judicial system's IT platform, CITIUS (Sistema informático de suporte à actividade dos tribunais), which holds information on court cases nationwide, allowing the database to automatically gather data on cases as they progress through the courts.

The BDVMVD will also connect with the Commission for Citizenship and Gender Equality (CIG), which coordinates support centres and shelters across Portugal. This commission holds data on victims receiving services, including those under protection measures like the panic button system. Currently, around 5,000 individuals benefit from these measures, and CIG's data on these individuals is expected to be integrated into the BDVMVD by early 2025.

Another key data source will be the National Commission for the Protection of the Rights of Children and Young People (CNPDPCJ), which gathers administrative data on minors involved in cases of violence. The BDVMVD will thus cover three main areas: domestic violence, violence against women, and gender-based violence. Additional connections will be made with data from the Directorate-General for Reintegration and Prison Services (DGRSP), under the Ministry of Justice, and

from the National Commission for Victim Protection (CPVC), as well as the Institute of Social Security (ISS).

In the future, other services, such as the health sector, may also be integrated. However, the health sector's data-collection systems are still under development and not yet ready to connect with the national platform. Nevertheless, the BDVM-VD platform has been designed to accommodate these future additions once they become feasible.

Enhanced Data Scope and Risk Assessment Tools

As a result of these enhancements, the BDVMVD will contain a broader and more diverse set of information, forming a highly detailed, multi-faceted database. This will include standard forms for documenting offences, records on safety plans, weapon seizures, and applications for protective measures, along with expanded data on criminal justice processes involving perpetrators and relevant social security information.

One of the BDVMVD's key features is its unified risk assessment tool, which is already part of the current system. This instrument is standardised across police forces, support networks, and public prosecutors. Initially developed in 2014, it is now undergoing an update, with the revised version expected by the end of November 2024. The standardised approach ensures consistency in risk evaluations across the country, enabling all stakeholders to assess cases using the same criteria. The tool is highly practical for everyone involved, as it allows authorised users to review the most recent risk assessments completed for any given case.

Developed as a national standard tailored for the Portuguese population, the current risk assessment tool has been applied consistently by police forces, support centres, shelters, and public prosecutors. The shared use of this tool simplifies reading and interpreting results, no matter who conducted the assessment, and each evaluation is stored in the database for future reference. The risk assessment tool also includes an option for "victim status" designation, allowing individuals who report qualifying crimes to apply for this status. Though optional, more than 90% of victims choose to accept the designation, which provides certain rights, mainly administrative rather than judicial, that can significantly improve access to services.

This advanced, integrated information system will allow a wide range of authorised users, including both law enforcement agencies and judicial authorities, to consult summary case information and access detailed records as needed, with regular updates tailored to each user's profile. An alert system will automatically flag cases involving individuals with prior records, while continuous monitoring will ensure that records are updated automatically. Also, this will serve as a key data source for the Annual Internal Security Report and the Annual Domestic Violence Report. It will also provide valuable information for decision-making and specific requests from public administration entities, international bodies, and academic researchers.

Enhanced Cross-Referencing and Data Integration Capabilities in the Evolving BDVD System

Currently, the Database on Domestic Violence (BDVD) lacks automated tracking capabilities to identify prior records related to victims or perpetrators with histories in the system. However, it includes robust cross-referencing features, allowing users to develop comprehensive profiles of victims and aggressors, examine connections between risk assessments and reported incidents, and analyse the specifics of individual occurrences.

The database enables the creation of regional prevalence maps, filterable by indicators such as sex, age, and incident location. Additionally, users can cross-reference various data points, facilitating the study of correlations such as victim demographics alongside perpetrator age or geographic area. One example is the ability to correlate risk levels with the presence of children in a household, revealing trends that can inform interventions.

The system's high degree of customisation is particularly valuable for researchers and policymakers. Researchers, especially at universities, frequently request access to this data to support in-depth studies on domestic and gender-based violence patterns. The database's flexibility and extensive analytical capabilities make it an invaluable resource for generating insights with nearly limitless applications.

The database comprehensively collects data on all complaints, risk assessments, detentions, restraining orders, and victim status assignments. Additionally, it records details of the support victims receive when engaging with the court system and police interventions, such as accompanying victims to collect personal belongings from a residence.

Another important feature of the database is its ability to track incidents involving witnesses, such as children, and correlate these with risk levels. Recent analyses, for instance, show that increased risk levels often coincide with the presence of children in the household, allowing for a deeper understanding of specific case dynamics.

All variables in the current database, including its cross-referencing functionalities, will be incorporated into the new system. However, the database will be much larger, thus exponentially increasing monitoring and analysis possibilities. In addition to the data currently in the system (GNR and PSP police data), additional security data from the judiciary police will be added. Moreover, a wide range of judicial data will be integrated through the CITIUS system and the Institute for Financial Management and Equipment of Justice (IGFEJ), which manages the financial, patrimonial, and technological resources of the Ministry of Justice. This will include data on court proceedings, such as protection orders issued in family, divorce, and child custody cases. Integrating these judicial records is particularly valuable, as it enables the linkage of different types of cases—domestic violence, cyber violence, sexual exploitation, and more—across various jurisdictions, providing a more comprehensive view of each case.

This framework will also be enriched by data from the Directorate-General for Reintegration and Prison Services, the organisation responsible for crime prevention, sentence execution, social reintegration, and the management of the juvenile and prison systems.

Probation and prison records will then be incorporated into the system. For instance, if a perpetrator is scheduled for release, the system will flag this information, allowing police to notify the victim as a precautionary measure. This is especially critical in high-risk cases. In jurisdictions where this information is not automatically shared, efforts are underway to establish connections that ensure victims receive timely notifications.

The database will also incorporate additional indicators by linking with national security records to track work and medical leave, which may signal underlying issues. Additionally, a dedicated national team will analyse retrospective homicide cases, contributing these findings to the system and further enhancing its insights.

Confidentiality and Data Access

Both versions of the database share key technical features, hosted as web applications within secure internal networks. While the Secretaria-Geral do Ministério da Administração Interna (SGMAI) does not have direct access to personal data, law enforcement agencies do. In the BDVMVD, judiciary authorities will also be granted selective access to sensitive data as necessary.

This platform is confidential and does not store personal identifiers. Each complaint generates a unique code, so all data linked to an individual is anonymised. This strict coding system, which took over a year to gain approval from the National Data Protection Commission, is essential to safeguarding data security and privacy. The purpose of this database is to enable the sharing of relevant information from multiple systems concerning individual cases. For example, if a person has interacted with social services, been involved in a court case, or received support from shelters, the database can compile this information to provide a complete picture of their case without disclosing personal identifiers.

The system will also allow for tracking individuals across cases. If a perpetrator is involved in multiple judicial processes, the system can link these to identify patterns, which is valuable for both law enforcement and judicial coordination. This connectivity also enhances victim protection by showing what support has already been provided, ensuring that services are not duplicated and that new interventions build on existing assistance.

Each agency will only have access to data pertinent to its specific role. For example, a shelter worker will only see information relevant to their responsibilities, not data from other areas like law enforcement or judiciary records. The Ministry of Internal Affairs will act as the main administrative authority, overseeing the system but without direct access to personal data. Law enforcement and judiciary authorities will be the only entities with access to detailed records, and police data will be automatically migrated into the system.

CONCLUDING REMARKS

Technology has transformed gender-based violence by extending traditional abusive behaviours into digital spaces, amplifying their impact and creating new forms of harm. The continuum of abuse demonstrates how online and offline violence is intertwined, making it difficult to separate these phenomena and further complicating efforts to define and address OTFVAW comprehensively. Misogynistic hatred, image-based sexual abuse, and digitally facilitated intimate partner violence are identified as key manifestations of OTFVAW, with victims often targeted based on intersecting identity markers such as race, ethnicity, or sexual orientation. Perpetrators exploit the anonymity, accessibility, and reach of technology to intimidate, control, and silence victims, with severe psychological, reputational, and economic consequences. The absence of harmonised definitions and frameworks significantly limits the effectiveness of legal and policy responses. Many countries rely on gender-neutral legislation or subsume technology-facilitated violence under broader legal categories, which hinders the ability to collect accurate and comparable data. This gap not only marginalises the victims of OTFVAW but also prevents the development of comprehensive interventions.

Efforts by international organisations, such as the United Nations, WHO, the European Union and the Council of Europe, demonstrate progress towards establishing standardised definitions and methodologies for addressing OTFVAW. These initiatives underscore the importance of viewing technology-facilitated violence as a continuum of gender-based violence while integrating intersectional and contextual dimensions into legal and policy responses. However, significant challenges remain in translating these frameworks into effective, actionable measures at the national level. The conceptualisation of OTFVAW requires multidimensional approaches, combining insights from abuse tactics, platforms, harm dynamics, and victim-perpetrator relationships. Yet, each lens alone is insufficient to capture the full scope of this phenomenon. An integrated approach that synthesises these perspectives is essential to develop robust legal, policy, and data-collection frameworks capable of addressing the growing complexities of OTFVAW.

The lack of harmonised definitions, standardised methodologies, and gender-disaggregated data remains a major barrier to understanding the prevalence, nature, and impact of OTFVAW. Without these tools, it is impossible to design and implement effective, evidence-based policies. The Istanbul Convention, particularly through Article 11, underscores the essential role of systematic data collection and research in combating violence against women, including its digital dimensions.

While some progress has been made—through administrative records, national surveys, and qualitative research—current efforts remain fragmented and inconsistent across Council of Europe member states. Challenges such as privacy concerns, the transborder nature of digital platforms, and varying legal frameworks impede comprehensive data collection. Many systems fail to capture the intersectional dimensions of this phenomenon, leaving marginalised groups—such as ethnic minorities, LBTI individuals, and women with disabilities—underrepresented. Furthermore, emerging forms of violence, like online grooming, deepfakes, and hate speech, are inadequately documented.

Promising practices, including community-driven research, the use of social media data, and mixed-method approaches, offer potential solutions to address these gaps. However, significant variation in national data collection efforts across Europe, with some countries employing comprehensive, multi-sectoral systems and others maintaining minimal or narrow approaches, underscores the urgent need for harmonisation. Ultimately, without a coordinated and inclusive framework for data collection, OTFVAW remains underreported, misunderstood, and inadequately addressed, perpetuating gaps in protection and accountability.

The dynamic evolution of the data collection systems analysed exemplifies varied pathways in adapting to the increasing prevalence and complexity of both physical and technology-facilitated violence against women. While the systems in each country differ in design, scope, and functionality, they share a common objective: to improve the accuracy, comprehensiveness, and usability of data for effective policymaking and victim protection.

The Austrian system illustrates the gradual adaptation of general data frameworks to address emerging forms of violence, driven by increasingly robust legislative measures and public support initiatives. Challenges remain in integrating police and judicial data systems to ensure seamless tracking, but progress reflects a clear commitment to capturing digital and physical violence against women more comprehensively. Spain's system demonstrates a specialised and highly structured approach, integrating risk assessment protocols and dynamic case management tools. Its alignment with judicial and law enforcement mechanisms allows for the proactive protection of victims, although room for expansion exists to encompass newer forms of OTFVAW. Portugal is transitioning from its existing Domestic Violence Database (BDVD) to a more holistic and integrated Database on Violence Against Women and Domestic Violence (BDVMVD). This new system aims to consolidate diverse data sources and enhance analytical capabilities while maintaining a strong emphasis on victim confidentiality and data security.

The analysis reveals three key trends. First, the importance of legislative foundations. Legal reforms play a pivotal role in shaping and refining data collection systems. Clear legal definitions and targeted legislation facilitate the recording of specific offences, enhancing the granularity and relevance of data. Second, the necessity of multi-sectoral collaboration. Effective data systems require input from diverse stakeholders, including law enforcement, the judiciary, social services, and NGOs. Integrated approaches enable more comprehensive insights into the scope and dynamics of GBV. Finally, technological innovation and adaptability are key. Advanced data systems must incorporate evolving technological tools and methodologies to track emerging forms of violence, such as cyber violence while ensuring flexibility for future challenges.

RECOMMENDATIONS

Develop Harmonised Definitions of OTFVAW

To strengthen the understanding and response to GBV, particularly technology-facilitated violence against women OTFVAW, harmonised definitions must be established. These definitions should be internationally recognised and reflect evolving forms of OTFVAW, such as cyberstalking, sextortion, image-based abuse, and deepfake exploitation. International organisations, such as the UN, WHO, and EIGE, CoE should continue leading efforts to ensure definitions align with technological advancements and address intersectional vulnerabilities, including race, ethnicity, disability, and socioeconomic status. Unified terminology will enable consistent data collection across regions and sectors, facilitating a clearer picture of the problem's scale and diversity.

Strengthen Legal Frameworks

Legal and policy frameworks must be revised to reflect the complexities of OTFVAW, recognising it as a distinct form of violence with gendered dimensions. Countries should adopt legislation that explicitly addresses OTFVAW, including online harassment, hate speech, and non-consensual image sharing. Complementing these efforts, digital platforms should be required to implement robust mechanisms for reporting and removing and help ensure that victims of technology-facilitated violence receive adequate protection while curbing abusive online behaviour. Strengthened legal frameworks will also contribute to standardised data collection, as crimes will be better defined and categorised in line with the evolving digital landscape.

Improve Data Collection Practices

Improving data collection practices is essential to fully capture the prevalence and nuances of gender-based violence, particularly in its digital forms. Data collection efforts should integrate OTFVAW-specific indicators into existing national and international surveys, while administrative data systems must evolve to disaggregate data by gender, age, ethnicity, disability, and other markers of identity and relationship between victims and perpetrators. Such disaggregation will provide

insight into intersectional dimensions of violence, ensuring the inclusion of marginalised populations often left out of mainstream datasets. Also, it would help address forms of abuse occurring in an intimate context. Tools for collecting comparable and standardised data across jurisdictions should be developed, allowing for consistent monitoring and cross-country comparisons. Additionally, involving diverse stakeholders, including NGOs, academic institutions, and survivor groups, in the design and analysis of data collection frameworks will ensure their inclusivity and relevance.

Promote International Cooperation

To address the transnational nature of OTFVAW, international cooperation must be prioritised. Countries should work together to establish protocols for sharing data across borders, particularly in cases involving anonymous perpetrators or abuse facilitated by global digital platforms. Regional bodies such as the CoE can facilitate the exchange of best practices and ensure the interoperability of national data systems to support coordinated responses. Further, international organisations can provide technical assistance to member states in harmonising data collection methodologies, creating a more comprehensive global framework to address the problem.

Leverage Emerging Technologies

The integration of emerging technologies into safeguarding practices can also significantly enhance data collection and response mechanisms. Advanced tools like artificial intelligence (AI) and machine learning can be used to analyse patterns of abuse, predict high-risk cases, and generate real-time insights into the spread of harmful content online. Collaboration with social media platforms to access anonymised data on online harassment trends can enable more proactive interventions. Additionally, the misuse of emerging tools such as spyware or smart devices should be addressed through regulatory measures, ensuring these technologies do not exacerbate violence against women.

Adopt Victim-Centred and Privacy-Conscious Approaches

It is equally important to develop victim-centred and privacy-conscious systems for data collection. Victims must feel confident that reporting incidents will not expose them to further harm or breach their privacy. This requires robust anonymisation protocols, secure data storage, and informed consent procedures. Law enforcement, judiciary, and social services should adopt a unified approach that

respects survivors' rights while enabling comprehensive tracking of their cases. Transparency about how data is used and who has access to it will build trust in these systems and encourage higher reporting rates, which are often hindered by fears of retribution or exposure.

Foster Multi-Sectoral Collaboration

The development of multi-sectoral collaboration is crucial to ensuring that data collection systems address the full spectrum of gender-based violence. This requires fostering partnerships between law enforcement, social services, NGOs, academia, and healthcare providers to create an integrated, holistic understanding of the issue. These sectors should share data using interoperable systems to reduce duplication and fill gaps in understanding. Cross-sector collaboration also allows for the inclusion of unreported cases and underrepresented populations, providing a more comprehensive and actionable dataset.

Conduct Regular Population-Based Surveys

Regular population-based surveys should complement administrative data to track trends and identify risk factors associated with GBV. These surveys, conducted in line with Article 11 of the Istanbul Convention, provide insights into the prevalence, severity, and socio-economic factors influencing violence. They should be designed to capture technology-specific dimensions of abuse and disaggregate data by key identity markers. The findings from such surveys should be published in accessible formats, encouraging informed debate and targeted policymaking.

Expand Awareness and Training Initiatives

Finally, public awareness campaigns should be launched to enhance understanding of technology-facilitated violence and encourage reporting. Educating the public about the risks and signs of digital abuse can empower individuals to seek help and hold perpetrators accountable. At the same time, specialised training should be provided to law enforcement, legal professionals, and data collectors to ensure sensitive and accurate reporting of OTFVAW cases. When combined with transparent data-sharing practices and regular publication of anonymised findings, these measures will foster a culture of accountability and pave the way for stronger evidence-based responses to gender-based violence.

In conclusion, these recommendations call for a harmonised, victim-centred, and technologically advanced approach to data collection systems. By strengthening

legal frameworks, promoting multi-sectoral collaboration, leveraging emerging technologies, and prioritising privacy, governments and international organisations can create robust data collection systems that not only capture the full scope of violence against women but also provide a solid foundation for evidence-based interventions.

APPENDIX 1

REFERENCES

- Afrouz, R., (2023). The Nature, Patterns and Consequences of Technology-Facilitated Domestic Abuse: A Scoping Review. In: Trauma, Violence, & Abuse, 2023, Vol. 24(2) 913–927.
- Al-Alosi H. (2017). Cyber-violence: Digital abuse in the context of domestic violence. University of New South Wales Law Journal, 40(4), 1573–1603.
- Amanda, P., & Reichl, A. J. (2019). Gendertrolls just want to have fun, too. Personality and Individual Differences, 141,152–156. https://doi.org/10.1016/j.paid.2019.01.011.
- Bainotti, L., & Semenzin, S. (2021). Gendertrolling: Hostility towards women online. Journal of Digital Harassment Studies, 2(1), 23-45.
- Barker, K., & Jurasz, O. (2020). Online violence against women as an obstacle to gender equality: A critical view from Europe. European Equality Law Review, 2020(1), 47–60.
- Bailey, L., Hulley, J., Gomersall, T., Kirkman, G., Gibbs, G., & Jones, A. D. (2024). The Networking of Abuse: Intimate Partner Violence and the Use of Social Technologies. Criminal Justice and Behavior, 51(2), 266-285. https://doi.org/10.1177/00938548231206827
- Brookfield, K., Fyson, R., & Goulden, M. (2024). Technology-facilitated domestic abuse: An under-recognised safeguarding issue? British Journal of Social Work, 54(1), 419–436. https://doi.org/10.1093/bjsw/bcad206
- Brown M. L., Reed L. A., Messing J. T. (2018). Technology-based abuse: Intimate partner violence and the use of information communication technologies. In Vickery J. R., Everbach T. (Eds.), Mediating misogyny: Gender, technology, and harassment (pp. 209–227). Springer International Publishing.
- Buckels, E. E., Trapnell, P. D., & Paulhus, D. L. (2014). Trolls just want to have fun. Personality and Individual Differences, 67,97–102. https://doi.org/10.1016/j.paid.2014.01.016
- Button, M., Blackbourn, D., Sugiura, L., Shepherd, D., Kapend, R., & Wang, V. (2021). From feeling like rape to a minor inconvenience: Victims' accounts of the impact of computer misuse crime in the United Kingdom. Telematics and Informatics, 64, 101675.

- Calvert, C., & Brown, J. (2000). Video voyeurism, privacy and the internet: Exposing Peeping Toms in cyberspace. Cardozo Arts & Entertainment Law Journal, 18, 469–516.
- Chatterjee, R., et al., "The Spyware Used in Intimate Partner Violence," 2018 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2018, pp. 441-458, doi: 10.1109/SP.2018.00061.
- Citron, D. K. (2014). Hate crimes in cyberspace. Harvard University Press.
- Clough, J. (2015). Voyeurism. In Principles of Cybercrime (pp. 454–472). Cambridge University Press.
- 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, vol. 1989, issue 1, article 8.
- Cripps, J., & Stermac, L. (2018). Cyber-sexual violence and negative emotional states among women in a Canadian university. International Journal of Cyber Criminology, 12(1), 1-12.
- Cross C., Holt K., Holt T.J. (2023). To pay or not to pay: An exploratory analysis of sextortion in the context of romance fraud. Criminology & Criminal Justice (2023), pp. 1-16
- DeKeseredy, W. S., & Schwartz, M. D. (2016). Thinking sociologically about image-based sexual abuse: The contribution of male peer support theory. Sexualization, Media, & Society, 2(4), 1-8.
- De Vido, S., & Sosa, L. (2021). Criminalisation of gender-based violence against women in European states, including ICT-facilitated violence. European Commission. https://doi.org/10.2838/345057
- Diamandis, P. H., & Kotler, S. (2020). The future is faster than you think: How converging technologies are transforming business, industries, and our lives. Simon & Schuster.
- Dimond J. P., Fiesler C., Bruckman A. S. (2011). Domestic violence and information communication technologies. *Interacting with Computers*, 23(5), 413-421.
- Donato, S., Eslen-Ziya, H., & Mangone, E. (2022). From offline to online violence: New challenges for the contemporary society. International Review of Sociology, 32(3), 400–412. https://doi.org/10.1080/03906701.2022.2133405
- Douglas H., Harris B. A., Dragiewicz M. (2019). Technology-facilitated domestic and family violence: Women's experiences. British Journal of Criminology, 59(3), 551–570. 10.1093/bjc/azy068
- Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N. P., Woodlock, D., & Harris, B. (2018). Technology-facilitated coercive control:

Domestic violence and the competing roles of digital media platforms. Feminist Media Studies, 18(4), 609–625.

- Dragiewicz, M., Burgess, J., Matamoros-Fernández, A., Salter, M., Suzor, N., Woodlock, D., & Harris, B. (2019). Technology-facilitated coercive control: Domestic violence and the competing roles of digital media platforms. Feminist Media Studies, 19(4), 498–514.
- Duerksen, K. N., & Woodin, E. M. (2019). Technological intimate partner violence: Exploring technology-related perpetration factors and overlap with in-person intimate partner violence. Computers in Human Behavior, 98, 223-231.
- Dunn, M. (2020). Gender-based online violence: The rise of gendertrolling. Internet Policy Review, 9(2), 1-19.
- Farías Pereira, J. (2024). The relevance of the data collection process in the VioGén system from a feminist perspective. Oñati Socio-Legal Series. https://doi.org/10.35295/osls.iisl.1922
- Fernet, M., Lapierre, A., He´bert, M., & Cousineau, M.-M. (2019). A systematic review of literature on cyber intimate partner victimization in adolescent girls and women. Computers in Human Behavior, 100, 11-25.
- Fox, J., & Tang, W. Y. (2017). Women's experiences with general and sexual harassment in online video games: Rumination, organizational responsiveness, withdrawal, and coping strategies. New Media & Society, 19(8), 1290–1307.
- Fraser, C., Olsen, E., Lee, K., Southworth, C., & Tucker, S. (2010). The new age of stalking: Technological implications for stalking. Juvenile and Family Court Journal, 61(4), 39-55.
- Freed, D., Palmer, J., Minchala, D. E., Levy, K., Ristenpart, T., & Dell, N. (2017). Digital technologies and intimate partner violence: A qualitative analysis with multiple stakeholders. Proceedings of the ACM on Human-Computer Interaction, 1(CSCW), 1–22. http://doi.org/10.1145/3134681
- Garrido, A. (2022). Digital misogyny and the silencing of women: A sociopolitical perspective. Feminist Media Studies, 22(3), 211–230.
- Gius, C. (2023). (Re)thinking gender in cyber-violence: Insights from awareness-raising campaigns on online violence against women and girls in Italy. Media Education, 14(2), 95–106. https://doi.org/10.36253/me-14896
- González-Álvarez, J.L., López-Ossorio, J.J., Urruela, C. & Rodríguez-Díaz, M. (2018). Integral Monitoring System in Cases of Gender Violence. VioGén System. Behavior & Law Journal, 4(1), 29-40: https://doi.org/10.47442/blj.v4.i1.56
- González-Álvarez, J.L., Santos Hermoso, J., and Camacho-Collados, M., 2020. Policía predictiva en España. Aplicación y retos futuros. Behavior & Law Journal [online], 6(1), 26–41. https://doi.org/10.47442/blj.v6.i1.75

- Goulden M. (2019) "Delete the family': Platform families and the colonisation of the smart home', Information, Communication and Society, 24(7), pp. 903–20.
- Goulden M. (2021) 'Folding and friction: The internet of things and everyday life', In Rohlinger D.A., Sobieraj S. (eds.), Oxford Handbook of Sociology and Digital Media, Oxford, Oxford University Press.
- Gurumurthy, A., & Dasarathy, A. (2022). Profitable provocations: A study of abuse and misogynistic trolling on Twitter directed at Indian women in public-political life. IT for Change. https://itforchange.net/sites/default/files/2132/ITfC-Twitter-Report-Profitable-Provocations.pdf
- Gurumurthy, A., Dasarathy, B. (2022). Gendered violence and resistance in the digital age: A global feminist perspective. Global Media Journal, 14(1), 57–70.
- Habringer M., et al. (2023). (No) space: cyberviolence against women in (former) partnerships. University of Applied Sciences Campus Vienna, pp. 3-4, June 2023. Available at: www.fh-campuswien.ac.at/forschung/projekte-und- aktivitaeten/kein-raum-cyber-gewalt-gegen-frauen-in-ex-beziehungen.html
- Harris B. (2018). Spacelessness, spatiality and intimate partner violence technology-facilitated abuse, stalking and justice administration. In Fitz-Gibbon K., Walklate S., McCulloch J., Maher J. (Eds), Intimate Partner Violence, Risk and Security. Routledge.
- Havard T. E., Lefevre M. (2020). Beyond the power and control wheel: How abusive men manipulate mobile phone technologies to facilitate coercive control. *Journal of Gender-Based Violence*, 4(2), 223-239. https://doi.org/0.1332/239868020X15850131608789.
- Henry N., Flynn A., Powell A. (2020). Technology-facilitated domestic and sexual violence: a review. *Violence against Women*, 26(15-16), 1828-1854.
- Henry N., McGlynn C., Flynn A., Johnson K., Powell A., Scott A.J. (2020). Image-based sexual abuse: A study on the causes and consequences of non-consensual nude or sexual imagery, Routledge
- Henry, N., Powell, A. (2015). Beyond the 'sext': Technology-facilitated sexual violence and harassment against adult women. Australian & New Zealand Journal of Criminology, 48(1), 104–118.
- Henry, N., Powell, A. (2015). Embodied harms: Gender, shame, and technology-facilitated sexual violence. Violence Against Women, 21(6), 758–779. https://doi.org/10.1177/1077801215576581
- Henry, N., Powell, A. (2016). Sexual violence in a digital age. Palgrave Macmillan.
- Henry, N., Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. Trauma, Violence, & Abuse, 19(2), 195–208.

- Henry, N., Umbach, R. (2024). Sextortion: Prevalence and correlates in 10 countries, Computers. In Human Behavior, (158)2024, 108298, ISSN 0747-5632, https://doi.org/10.1016/j.chb.2024.108298.
- Henson, B., & Reyns, B. W. (2016). Taking stock: The current status of cyberstalking research. In T.J. Holt (Ed.), Crime on-line (pp. 199–224). Durham, NC: Carolina Academic Press
- Huber, A. (2023). 'A shadow of me old self': The impact of image-based sexual abuse in a digital society. *International Review of Victimology*, *29*(2), 199-216. https://doi.org/10.1177/02697580211063659
- Iroegbu, M., O'Brien, F., Muñoz, L. C., & Parsons, G. (2024). Investigating the psychological impact of cyber-sexual harassment. Journal of Interpersonal Violence, 39(15–16), 3424–3445. https://doi.org/10.1177/08862605241231615
- Jane, E. A. (2016). Misogyny online: A short (and brutish) history. SAGE Publications Ltd.
- Killean, R., McAlinden, A. M., & Dowds, E. (2022). Sexual violence in the digital age: Replicating and augmenting harm, victimhood and blame. Social & Legal Studies, 31(6), 871–892.
- King, R. (2017). Digital domestic violence: Are victims of intimate partner cyber harassment sufficiently protected by New Zealand's current legislation. Victoria University of Wellington Law, Review, 48, 29-54.
- Leitão R. (2021) 'Technology-facilitated intimate partner abuse: A qualitative analysis of data from online domestic abuse forums', Human–Computer Interaction, 36(3), pp. 203–42.
- Lewis, R., Anitha, S. (2023). Upskirting: A Systematic Literature Review. Trauma, Violence, & Abuse, 24(3), 2003-2018. https://doi.org/10.1177/15248380221082091
- Mantilla, K. (2013). Gendertrolling: Misogyny adapts to new media. Feminist Studies, 39(2), 563–570. http://www.jstor.org/stable/23719068
- Noble, S., Tynes, B. (2016). The intersectional internet: race, sex, class and culture online, Peter Lang Publishing, NY
- Maher J. M., McCulloch J., Fitz-Gibbon K. E. (2017). New forms of gendered surveillance?: Intersections of technology and family violence. In Segrave M., Vitis L. (Eds), *Gender, technology and violence* (pp. 27-14). Routledge.
- Markwick K., Bickerdike A., Wilson-Evered E., Zeleznikow J. (2019). Technology and family violence in the context of post-separated parenting. *Australian and New Zealand journal of family therapy*, 40(1), 143-162.
- Mason C. L., Magnet S. (2012). Surveillance studies and violence against women. surveillance & society, 10(2), 105-118.

- Matthews, T., O'Leary, K., Turner, A., Sleeper, M., Woelfer, J. P., Shel- ton, M., Woelfer, J. P., Shelton, M., Manthorne, C., Churchill, E. F., Consolvo, S. (2017). Stories from survivors: Privacy & security practices when coping with intimate partner abuse. Proceedings of the 017 CHI conference on human factors in com- puting systems (pp. 2189–2201). ACM.
- McGlynn, C., Rackley, E., Houghton, R. (2017). Beyond 'revenge porn': The continuum of image-based sexual abuse. Feminist Legal Studies, 25(1), 25–46. https://doi.org/10.1007/s10691-017-9343-2
- Melton, H. C. (2007). Predicting the occurrence of stalking in relationships characterized by domestic violence. *Journal of Interpersonal Violence*, *22*(1), 3–25. http://doi.org/10.1177/0886260506294994
- Mitchell, M., Wood, J., O'Neill, T., Wood, M., Pervan, F., Anderson, B., & Arpke-Wales, W. (2022). Technology-facilitated violence: A conceptual review. Criminology & Criminal Justice. https://doi.org/10.1177/17488958221140549
- O'Malley R.L., Holt K.M. (2022). Cyber sextortion: An exploratory analysis of different perpetrators engaging in a similar crime. Journal of Interpersonal Violence, 37 (1–2) (2022), pp. 258-283
- Paananen, A., Reichl, C. (2019). Misogyny online: The new face of digital gender violence. Journal of Gender Studies, 28(4), 386–401.
- Patchin, J. W., Hinduja, S. (2020). "Sextortion among adolescents: Results from a National Survey of U.S. Youth": Erratum. Sexual Abuse: Journal of Research and Treatment, 32(5), 614. https://doi.org/10.1177/1079063220916354
- Perez-Tirado, I., Calvo Viota, A. C., & Igarzábal, B. (2024). Insta-hate toward female political leaders: Six case studies from Instagram. International Journal of Communication, 18,3392–3417.
- Powell, A. (2022). Technology-facilitated sexual violence: Reflections on the concept. In Rape(pp. 143–158). Routledge.
- Powell, A., Henry, N. (2017). Conceptualising technosocial sexual harms. In Sexual violence in a digital age(pp. 49–76). Palgrave Macmillan.
- Powell, A., Henry. N. (2019). Technology-Facilitated Sexual Violence Victimization: Results From an Online Survey of Australian Adults. J Interpers Violence. 2019 Sep;34(17):3637-3665. doi: 10.1177/0886260516672055. Epub 2016 Oct 3. PMID: 27697966.
- Ring (2022) There is a Ring for Every Home [Online], Santa Monica, Ring.
- Rogers, M. M., Fisher, C., Ali, P., Allmark, P., & Fontes, L. (2023). Technology-facilitated abuse in intimate relationships: A scoping review. Trauma, Violence, & Abuse, 24(4), 2210–2226.

- Sánchez López, B., 2020. La diligencia policial de valoración del riesgo de violencia de género en el sistema Viogén. FORO. Revista de Ciencias Jurídicas y Sociales, Nueva Época [online], 22(1), 119–130. https://doi.org/10.5209/foro.66637
- Southworth, C., Finn, J., Dawson, S., Fraser, C., & Tucker, S. (2007). Intimate partner violence, technology, and stalking. Violence Against Women, 13(8), 842–856. http://doi.org/10.1177/1077801207302045
- Stark E. (2012). Looking beyond domestic violence: Policing coercive control. *Journal of Police Crisis Negotiations*, 12(2), 199-217.
- Suler J (2004) The online disinhibition effect. *Cyber Psychology and Behaviour* 326–321 :(3)7
- The Networking of Abuse: Intimate partner violence and the use of social technologies. (2024). Criminal Justice and Behavior, 51(2), 266–285.
- Tanczer L., López-Neira I., Parkin S. (2021) 'I feel like we're really behind the game': perspectives of the United Kingdom's intimate partner violence support sector on the rise of technology-facilitated abuse', Journal of Gender-Based Violence, 5(3), pp. 431–50.
- Taylor, S., & Xia, Y. (2018). Cyber partner abuse: A systematic review. Violence and victims, 33(6), 983-1011.
- Tirocchi, S., Scocco, A., Crespi, M. (2022). The impact of digital misogyny on women in public spaces. Media & Society, 10(2), 49–67.
- Thorn H. (2017). Sextortion summary findings from a 2017 survey of 2,097 survivors
- Thorn (2017). Available at: https://www.thorn.org/wp-content/uploads/2019/12/Sextortion_Wave2Report_121919.pdf
- Tokunaga, R. S., Aune, K. S. (2017). Cyber-Defense: A Taxonomy of Tactics for Managing Cyberstalking. Journal of Interpersonal Violence, 32(10), 1451-1475. https://doi.org/10.1177/0886260515589564
- Van der Wilk, A., (2018). Cyber violence and hate speech online against women, PE 604.979 48 (Policy Department for Citizen's Rights and Constitutional Affairs, 2018). Study requested by the European Parliament's Committee on Women's Rights and Gender Equality). Available at: https://www.europarl.europa.eu/RegData/etudes/ STUD/2018/604979/IPOL_STU(2018)604979_EN.pdf
- Woodlock, D. (2017). The abuse of technology in domestic violence and stalking. Violence against Women, 23(5), 584-602.

- Woodlock, D., McKenzie, M., Western D., Harris, B., (2020). Technology as a Weapon in Domestic Violence: Responding to Digital Coercive Control. Australian Social Work, 73:3, 368-380, doi: 10.1080/0312407X.2019.1607510
- Yar M (2005) The novelty of 'cybercrime': An assessment in light of routine activity theory. *European Journal of Criminology* 427–407 :(4)2.
- Yardley, E. (2020). Technology-facilitated domestic abuse in political economy: a new theoretical framework. Violence against Women, 1-20.

Reports and documents from national authorities and international organisations

- Austrian Government Programme 2020-2024, Out of a Sense of Responsibility for Austria.
- Council of Europe, GREVIO. (2021). Report on the implementation of the Istanbul Convention in the digital age. https://www.coe.int
- Council of Europe Treaty Series - No. 210, Explanatory Report to the Council of Europe Convention on preventing and combating violence against women and domestic violence, Istanbul, 11.V.2011
- European Commission – Interoperable Europe, Public Sector Tech Watch, Viogen 5.0: discovering Spain's risk assessment system of gender-based violence. Available at https://interoperable-europe.ec.europa.eu/collection/public-sector-tech-watch/viogen-50-discovering-spains-risk-assessment-system-gender-based-violence
- European Institute for Gender Equality (EIGE). (2022). Combating cyber violence against women and girls. https://eige.europa.eu
- European Institute for Gender Equality (EIGE). (2017). Cyber violence against women and girls. https://eige.europa.eu
- Poder Judicial Espana, Informe sobre víctimas mortales de la violencia de género y doméstica en el ámbito de la pareja o expareja en 2021. Published 17 January 2023. Available at https://www.poderjudicial.es/cgpj/es/Temas/Violencia-domestica-y-de-genero/Actividad-del-Observatorio/Informes-de-violencia-domestica-y-de-genero/Informe-sobre-victimas-mortales-de-la-violencia-de-genero-y-domestica-en-el-ambito-de-la-pareja-o-expareja-en-2021
- Poder Judicial Espana, Análisis de las sentencias dictadas en el año 2020 relativas a homicidios o asesinatos por violencia de género y doméstica. Published 26 June 2023. Available at https://www.poderjudicial.es/cgpj/es/Temas/Violencia-domestica-y-de-genero/Actividad-del-Observatorio/Informes-de-violencia-domestica-y-de-genero/Analisis-de-las-senten-

cias-dictadas-en-el-ano-2020-relativas-a-homicidios-o-asesinatos-por-violencia-de-genero-y-domestica

- General Secretariat of the Organization of American States, Online gender-based violence against women and girls: Practical self-protection handbook: digital security tools and response strategies, OAS. Official records; OEA/Ser.D/XXV.25, ISBN 978-0-8270-7307-4. Available at https://www.oas.org/en/sms/cicte/docs/Guide-basic-concepts-Online-gender-based-violence-against-women-and-girls.pdf
- Report submitted by Austria pursuant to Article 68, paragraph 4 of the Council of Europe Convention on preventing and combating violence against women and domestic violence (1st thematic evaluation round). Received by GREVIO on 7 June 2023, GREVIO/Inf(2023)13. Published on 7 June 2023. Available at https://rm.coe.int/thematic-evaluation-report-on-the-implementation-of-the-istanbul-conve/1680ab8593
- Report submitted by Spain pursuant to Article 68, paragraph 1of the Council of Europe Convention on preventing and combating violence against women and domestic violence (1st thematic evaluation round). Received by GREVIO on 12 February 2024, GREVIO/Inf(2024)1. GREVIO/Inf(2024)1. Available at https://rm.coe.int/grevio-inf-2024-1-spain-1st-thematic-evaluation-round-eng/1680ae0c38
- UN Special Rapporteur on violence against women (2018). Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective. (2018, June 18). A/HRC/38/47. https://digitallibrary.un.org/record/1641160?ln=en&v=pdf#files
- United Nations Secretary-General (2014), A world that counts. mobilising the data revolution for sustainable development. Report prepared by the Independent Expert Advisory Group on a Data Revolution for Sustainable Development. https://www.undatarevolution.org/wp-content/uploads/2014/12/A-World-That-Counts2.pdf
- UN Women. (2020). Measuring the prevalence of online violence against women. https://www.unwomen.org
- UN Women. (2022). Technology-facilitated Violence against Women: Towards a common definition. Report of the meeting of the Expert Group 15-16 November 2022, New York, USA. https://www.unwomen.org/sites/default/files/2023-03/Expert-Group-Meeting-report-Technology-facilitated-violence-against-women-en.pdf

- WHO. (2019). Guidelines for researching violence against women. https://www.who.int

Websites

- BBC, Riley A., How your smart home devices can be turned against you, 12 May 2020. Full story available at https://www.bbc.com/future/article/20200511-how-smart-home-devices-are-being-used-for-domestic-abuse
- IT for Change Project, Online Gender-based Violence Judicial Resource Guide, Module 2 – Typologies of Online Gender-Based Offenses in Law, chapter 2.5: Gender Trolling. Available at https://projects.itforchange.net/online-violence-gender-and-law-guide/module-2-typologies-of-online-gender-based-offenses-in-law/2-5-gender-trolling/

ENG

www.coe.int

The Council of Europe is the continent's leading human rights organisation. It comprises 46 member states, including all members of the European Union. All Council of Europe member states have signed up to the European Convention on Human Rights, a treaty designed to protect human rights, democracy and the rule of law. The European Court of Human Rights oversees the implementation of the Convention in the member states.

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE