#HerNetHerRights

Mapping the state of online violence against women & girls in Europe
Introduction

As we have entered the second wave of the digital age, the growing reach of internet-based technologies, virtual contents and the wide diffusion of social media have not only reinforced existing forms of male violence, but have also created new tools to inflict harm on women and girls. The rise of online violence against women and girls (VAWG) has denied women autonomy over their own bodies and voices in cyberspaces, causing not only severe social implications on their online and offline lives but also on their financial resources (in terms of legal fees, online protection services and missed wages, among others). Online VAWG often also has lifelong consequences in terms of mental and physical health and well-being. Despite research showing that women and girls in Europe experience violence in digital spaces, there is very little known about the specific characteristics or extent of the problem. The available information often remains spotty and is rarely aggregated on a European level. #HerNetHerRights is a six-month project led by the European Women’s Lobby (EWL) to analyse the current state of online VAWG in Europe, to raise awareness of the problem through the EU institutions, and to bring diverse actors from across Europe together to come up with innovative solutions and policy recommendations to fight online male violence and create a safer, more inclusive web for all women and girls.

About this report

This report aims at taking stock of existing research, available data, innovative initiatives and active stakeholders. It cannot be exhaustive, but wants to provide a basis for reflection and action.

Methodology and acknowledgments

This report is the result of a desk research/literature review conducted by Adriane van der Wilk and Marianne Niosi, consultants, under the coordination and input of Pierrette Pape, European Women’s Lobby Policy and Campaigns Director. It is completed by a series of interviews with members of the European Women’s Lobby, experts to the EWL Observatory on violence against women, members of the Youth 4 Abolition network, members of EWL Board of Administration, as well as with Members of the European Parliament and politicians, academics, activists and other stakeholders. Partner organizations and individuals have kindly shared their own findings and perspectives in order to extend the scope of the research. EWL staff members have also contributed and reviewed the findings.

Research purpose

This report aims at bridging applied research and advocacy regarding Online Violence Against Women and Girls (VAWG) and technology-related VAWG in Europe.

Objectives of the research

- Understanding the current state of violence against women and girls in digital spaces in Europe;
- Identifying current good practices on protection and prevention;
- Mapping legislation at EU level and national level;
- Assessing burning issues, challenges and policy gaps.

Methodology

The European Women’s Lobby produces knowledge within the five following principles: Women’s rights are human rights, Solidarity, Autonomy, Participation, Inclusion. Hence, an intersectional feminist framework has been adopted as the theoretical background for this report. The desk research is built on a corpus of literature produced in the fields of gender studies, cybersecurity, psychology and law, grey literature produced by institutions and organizations and press articles. It includes the review and analysis of existing bodies of law and policies, at country level and at European level, statistics, knowledge and initiatives produced by organizations, projects, support services and activists. The research draws moreover on interviews conducted with 17 key informants. Finally, the research highlights the outputs of the #HerNetHerRights Online Conference organized on October 13th, 2017.
# TABLE OF CONTENTS

1. Online Violence Against Women and Girls: a Prevalent and Growing Phenomenon 5
   - The facts 5
   - Online violence against women and girls is a reality 6
   - Forms of online VAWG 6
   - Perpetrators and mechanisms of abuse 9
   - The victims/survivors 12

2. Online Violence Against Women and Girls is Part of the Continuum of Male Violence, Impacts all Women and Perpetuates Gender Inequality 15
   - Online violence has a gender 15
   - Consequences of male online violence on women’s health and autonomy 17
   - Impact of male online violence on women’s employment and reputation 18
   - Digital technologies and intimate partner violence 19
   - Facilitating trafficking and prostitution, normalising pornography 20
   - Online sexualized violence and pornography are urgent issues to be addressed 21
   - Online violence and harassment at work and in education 21

3. Understanding the Root Causes to Take Action to End Online Violence Against Women and Girls 23
   - Rape culture 23
   - The digital sphere is a male-dominated world 24
   - Structure of the Tech industry and nature of online spaces 25
   - Dialectics between freedom of speech and protection 26
   - Demands for a feminist internet 26
   - Prevention, Protection and Punishment 26
   - Normalisation of male violence in other virtual spaces 27

4. Taking action: Existing Legislation and Policies in Europe 29
   - Existing EU legislation and policies 29
   - National pieces of legislation and good practices 31

5. European Women’s Lobby Recommendations and Demands 34
   - Recommendations on ending violence against women 34
   - Other EU policies dealing with the digital world 35
   - Recommendations towards tech companies and internet providers 36
   - Recommendations regarding Media and Advertisement 36
   - Recommendations regarding pornography 36
   - Recommendations to end online violence against women and girls 35

BIBLIOGRAPHY 38
ANNEX 1. Interesting resources - Protection and Agency on digital platforms

- Governmental support services
- Campaigns (governmental and NGOs)
- Organizations
- Programs, Projects and Research
- Social enterprises
- Initiatives by type of online VAWG
- Informal networks on the web

ANNEX 2 - Online Conference Outputs

Supported by Google.

This publication has been produced with the financial support of the Rights, Equality and Citizenship (REC) Programme of the European Commission. The contents of this publication are the sole responsibility of the European Women’s Lobby and can in no way be taken to reflect the views of the European Commission.
1. Online Violence Against Women and Girls: a Prevalent and Growing Phenomenon

In this chapter, we will examine the scale of the phenomenon, through the data available, and will analyse current research on the different forms of online violence against women and girls, the women and girls specifically targeted, and the types of abusers. All this information gives a picture of the reality of the phenomenon: prevalent, expanding, and therefore requiring action.

The facts

Research on online VAWG is yet in its infancy and there is very little data available. When available, data is rarely disaggregated by gender. What has been proved however is that online VAWG is just as damaging to women as physical violence1; it also has “adverse impact on the exercise of and advocacy for free speech and other human rights”2.

Numbers show the prevalence of the phenomenon:

- In Europe, 9 million girls have experienced some kind of cyber violence by the time they are 15 years old3;
- Across continents, women are 27 times more likely to be harassed online4;
- According to a recent UN report, 73 percent of women had reported experiencing online abuse, with 18 percent -- around 9 million women -- experiencing serious internet violence5;
- Despite the rapidly growing number of women experiencing online violence, only 26 percent of law enforcement agencies in the 86 countries surveyed are taking appropriate action6;
- 93% of image based sexual abuse (revenge porn) victims said they suffered significant emotional distress due to being a victim7;
- 70% of women victims of cyberstalking also experienced at least one form of physical or/and sexual violence from an intimate partner8.
- 1 in 5 teenagers in Europe experience cyberbullying and among them, girls are at higher risk (23.9% vs. 18.5%)9;
- In 2014, 87% of all reported child sexual abuse images depicted girls10;
- 1 out of 4 young women have been stalked or sexually harassed at least once11.

Furthermore, the numbers below illustrate how a male dominated sector such as the media/advertisement sector produces harmful stereotypes that deeply impact how society sees women and how women see themselves.

---

2 Ibid.
3 Ibid.
4 Ibid.
6 Ibid.
7 End Revenge Porn campaign, https://www.cybercivilrights.org
9 https://cyberbullying.org/research/map/romania
Online violence against women and girls is a reality

Despite the prevalent belief in the liberating and empowering potential of a new, democratic digital sphere, on the internet and via the use of new technologies, women and girls experience violence in many appalling ways. They are targeted because of their sex/gender and encounter diverse forms of violence by different types of perpetrators, including intimate partners, such as online harassment, sexist hate speech, online stalking, online bullying, multiple threats, impersonation or non-consensual sharing of graphic contents. Online channels and spaces are new or more opaque ways to perpetrate other forms of violence against women and girls. Digital spaces are also used to lure women and girls into prostitution and pornography, or can contribute to further intimate partner violence.

Online abuse can be categorised along two axes\(^{15}\): verbal online abuse which includes sexist hate speech reinforced by intersecting identities/vulnerabilities, sextortion and death, rape and torture threats, and graphic online abuse, including creepshots, graphic threats and revenge porn\(^{16}\).

Digital spaces and the new technologies where these forms of pervasive violence happen include emails, text messages, social networks such as Facebook, Twitter, LinkedIn and Periscope (used by 90% of young people on a daily basis\(^{17}\)), search engines such as Google or Yahoo and their multiple functionalities, blogs, Reddit threads, dating websites and applications, communication apps like Whatsapp, Facebook Messenger, Snapchat or Skype, online media and their comments sections, forums, online videogames and their chatrooms, virtual reality spaces, etcetera.

All these spaces and their various functions allow for misogynistic violence to manifest itself in many different ways. This violence is constantly shifting because of the nature of the digital sphere, where innovation and trends are fluid. Moreover, online VAWG takes place across platforms\(^{18}\) (spaces to share information, exchange, buy products, learn, get updates), which makes it a difficult phenomenon to grasp.

Forms of online VAWG

The European Women’s Lobby noticed a great interest among activists and researchers in coining a feminist lexicon of online VAWG. Moreover, both academics\(^{19}\) and practitioners\(^{20}\) highlight the need for reframing the terminology used by media to describe the diverse forms of online abuse and online crimes victimising women.

---


\(^{14}\) Ibid.


\(^{16}\) See paragraph below for a more detailed note regarding terminology


\(^{18}\) Interview with Nicole Shephard, independant researcher, on August 4, 2017

\(^{19}\) See for example Lumsen and Morgan, 2017; McGlynn and Rackley, 2017

and girls. Terms like “Revenge Porn” or “Grooming”, are challenged by scholars and activists as they describe the reality of the abuser rather than the victim’s abuse and the attacks on women and girls’ dignity, safety, integrity and health. Terms like “image-based sexual abuse” or “child sexual abuse” should be used. This is why the list below includes the alternate terms that illustrate a women-centred approach.

Moreover, it is crucial to keep in mind that the same type of abuse might impact women and girls differently because of the intersectional oppressions they live.

Finally, research finds that women and girls are statistically more at risk and impacted by online violence, but patriarchal stereotypes, values and norms can be used and transmitted as socially accepted behaviors of the total population, especially among minors where girls can act in accordance with the norm and harass girls in the same extent and in similar ways as boys.

Here below are defined the most common aspects of online VAWG and VAWG using new technologies. Due to the lack of consensus regarding terminology, the ever shifting digital tools and spaces and the contemporary character of the topic, the list is non exhaustive but goes through the main forms of abuse found online. The Women’s Media Center Speech Project provides a longer list of forms of online violence against women and girls.

While the abusers use different tactics and means, the goal remains the same: to embarrass, humiliate, scare, threaten, silence women and girls, or to encourage mob attacks or malevolent engagements against women and girls.

- **Sexist hate speech** is defined by the Council of Europe as “expressions which spread, incite, promote or justify hatred based on sex”. Typically, these are the rape, death and torture threats women and girls can receive because they are (self-)identified as women and bear the stereotypes enforced by rape culture and patriarchy.

- **Cyberbullying** consists of repeated behaviour such as sending mean text messages, starting rumours, or posting images with the objective of frightening and undermining someone’s self-esteem or reputation, which sometimes pushes vulnerable individuals to depression and suicide.

- **Cyber harassment** is the use of digital means to communicate or interact with a non-consenting person. Cyberbullying occurs the most between minors. Online sexual harassment can take the form of comments, videos, photos, and graphic images of sexual nature aimed at vilifying women and creating conditions of humiliation and sexualisation, because they are women. Offensive sexist and insulting words such as “slut”, “whore”, “cunt”, “bitch” can be used, as well as commentaries on women’s physical appearances.

- **Cyberstalking** is the act of spying, fixating or compiling information about somebody online and to communicate with them against their will.

- **Doxxing** refers to the online researching and publishing of private information on the internet to publicly expose and shame the person targeted.

- **Creepshots** are also called digital voyeurism. “Creepshots consist of perpetrators surreptitiously taking photos or videos of women’s private areas for the purpose of sexual gratification. In some cases, the act of taking the image without the victim’s knowledge, and the subsequent violation of their privacy and agency, is what provides the sexual gratification.” Creepshots are then posted on the internet, sometimes accompanied by

---


22 See the campaign of Osez le Féminisme! in France, part of “Stop the Attackers” campaign, to call “Revenge Porn” Cyber Rape, available online at [http://osezlefeminisme.fr/stopagresseurs-le-cyberviol/](http://osezlefeminisme.fr/stopagresseurs-le-cyberviol/)


24 Council of Europe, “CoE Factsheet Hate Speech”, 2017, available online at [http://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf](http://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf)


the hashtag (#) #creepshots. The term “Upskirting” has been coined by Gina Martins who was the victim of a man “placing his phone between her legs, positioning his camera up her skirt and taking pictures of her crotch in broad daylight”. Her taking her case to the police and then lobbying for a change in the law, started a conversation about this crime in the UK.27

- **Revenge porn**, or “image-based sexual abuse” following McGlynn and Rackley, is the fact of using private pictures and videos of sexual character, given or exchanged, and posting them online to shame and humiliate the victim. It can be the extension of intimate partner violence to online spaces. Images can also be obtained by hacking into the victim’s computer, social media accounts or phone, and can aim to inflict real damage on the target’s ‘real-world’ life (such as getting them fired from their job). Research suggests that up to 90 % of revenge porn victims are female and that the number of cases is increasing. There are also a growing number of websites dedicated to sharing revenge porn, where users can submit images alongside personal information such as the victim’s address, employer and links to online profiles.28 The phenomenon of image based sexual abuse has epitomized with the case of Danish journalist Emma Holten whose naked pictures were posted broadly on the internet. She defended herself by posting the naked pictures online herself, in a successful attempt to reclaim control.29 The numbers speak for themselves: in January 2017 alone, Facebook had to evaluate 54,000 potential cases of revenge porn and close more than 14,000 accounts.

- **Hacking**, the act of intercepting private communications and data, can target women and girls, especially in the form of web-cam hacking.

- **Online impersonation** is the fact of using the name or identity of someone else with the intend to harm, defraud, intimidate, or threaten any person, online impersonation may be used to discredit targeted women with their social and professional peers or for criminal purposes similar to offline identity theft.

- **Malicious distribution** is the use of tech tools to distribute defamatory material related to the victim and/or organizations; e.g. by using new technologies as a propaganda tool to promote violence against women, call for violence against abortion providers, etc.

- **Mob attacks / cyber mobs**: Hostile mobs include hundreds, sometimes thousands of people, systematically harassing a target. #Slanegirl, a hashtag that was used for the trending global public shaming of a teenage girl filmed performing fellatio, is one example. Attacks on public figures like Anita Sarkeesian or Caroline Criado-Perez have been conducted by cyber mobs.

- **Abusive sexting**: Sexting is the consensual electronic sharing of naked or sexual photographs. This is different, however, from the non-consensual sharing of the same images. while teenage boys and girls sext at the same rates, boys are between two and three times more likely to share images that they are sent.

Some forms of online VAWG are directly linked to prostitution and sex trafficking. Because of the anonymity provided by the Internet, and because the internet has the characteristics of an opaque transnational marketplace, victims can be sold numerous times to multiple buyers on a daily basis.31 Social media profiles and other new technologies allow clients to “shop” for women and girls.

- **Recruitment** is the use of technology to lure potential victims into trafficking and prostitution. “Social media is used by traffickers to sell people whose photographs they share, without their consent, often including

---

30 [https://www.theguardian.com/commentisfree/video/2015/jan/21/naked-pictures-this-is-what-i-did-revenge-porn-emma-holten-vide](https://www.theguardian.com/commentisfree/video/2015/jan/21/naked-pictures-this-is-what-i-did-revenge-porn-emma-holten-vide)
31 Women Media Center, “WMC Speech Project, Online Abuse 101”, available online at [http://www.womensmediacenter.com/speech-project/online-abuse-101#mobAttacksCybermobs](http://www.womensmediacenter.com/speech-project/online-abuse-101#mobAttacksCybermobs)
32 Women Media Center, “WMC Speech Project, Online Abuse 101”, available online at [http://www.womensmediacenter.com/speech-project/online-abuse-101#sextingAbusiveSexting](http://www.womensmediacenter.com/speech-project/online-abuse-101#sextingAbusiveSexting)
photographs of their abuse of women as an example to others. Seventy-six percent of trafficked persons are girls and women and the Internet is now a major sales platform.34

- **Online grooming** is the process of building an online abusive relationship with a child, in order to lure the child into sexual abuse, child-trafficking situations, child prostitution, or child documented rape. The term “grooming” is widely criticised by survivors themselves, as it fails to name explicitly the child sexual abuse dimension of the act.

- “Dishonorable propositions”, as in escort contracts and questionable model contracts that are sent to women and girls online can be connected to and an extension of Recruitment to sex trafficking.

New technologies can also be misused to perpetrate violence against women and girls:

- **In Real Life Attacks** describe incidents where online abuse either moves into the “real” world or is already part of an ongoing stalking or intimate partner violence interaction. IRL trolling can also mean simply trying to instil fear by letting a target know that the abuser knows their address or place of employment.35

- **Abuse of new technologies** can coincide with online violence but can also be different and foster offline violence: for example, installing spyware; misusing private/family accounts for online services; changing passwords. In the context of domestic and family violence, smart homes and/or smart personal devices have a Jekyll and Hyde quality: a smart home/device could become a vector for technology-facilitated aggression, but it could also be part of the solution.36 The program SafetyNed, showcased below, takes into account and tackles the misuse of new technologies in domestic violence cases.37

### Perpetrators and mechanisms of abuse

There are different types of perpetrators, using different platforms. Perpetrators can be relatives or acquaintances of the victim: (ex-)intimate partners, school/college classmates, co-workers, but also online criminals like impersonators and hackers. Perpetrators can have a political or religious motive or agenda, as in the case of religious groups opposing women’s rights or political groups targeting women’s participation. Lastly, individuals and organised groups including sexual predators, traffickers, paedophilic networks and transnational criminal organizations are among the most obvious category of perpetrators. In the case of women human rights defenders and whistle blowers, foreign states or domestic state institutions can fall in the range of online violence perpetrators.

Online VAWG may be most visibly embodied by the figure of the online “troll”: the troll comments or posts often anonymously, with the objective of creating discord and outraged reactions. Even though the troll is sometimes only undermining online debates or conversations, very often however, the use of sexist hate speech is what puts the troll in the category of online harassment perpetrators. Tone-policing, victim blaming, slut-shaming, sexist, racist, classist, ableist and homophobic hate speech, gas lighting, the use of alt-facts and doxxing, all these are techniques used by trolls to expel women from online spaces, making those spaces unwelcoming and threatening.

Internet doesn’t forgive or forget, online, hate and abuse against women can happen 24/7. Online violence against women and girls is still perceived as a sort of reality show. But the highjacking of one’s narrative is a very serious act of violence. It affects every aspects of one’s life.

Karla Mantilla,38 author of *Gendertrolling: How Misogyny Went Viral* (2015), identified several dimensions of what she calls “gender trolling” or online sexual harassment:

- Gender trolling attacks are precipitated by women asserting their opinions online.

---

34 Women Media Center, Op.Cit.
35 Ibid.
37 Ibid.
38 Women Media Center, Op.Cit.
They feature graphic sexualized and gender-based insults.
They include rape and death threats—often credible ones—and frequently involve real-life targeting, which adds to the credibility of the threats.
They cross multiple social media or online platforms.
They occur at unusually high levels of intensity and frequency (numerous threats or messages per day or even per hour).
They are perpetuated for an unusual duration (months or even years).
They involve many attackers in a concerted and often coordinated campaign.

These dimensions of cyber harassment can be summarized in the three pillars of impunity regarding cyber harassment: Mob mentality, Anonymity, Online permanency of outrage.

An example of mob mentality online - Anita Sarkeesian

In a TEDX video[^39], feminist video games critic, Anita Sarkeesian, recalls how she has been targeted by hundreds of perpetrators, reinforcing each other’s hate towards her:

“All my social media sites were flooded with threats of rape, violence, sexual assault, death – and you’ll notice that these threats and comments were all specifically targeting my gender. The Wikipedia article about me was vandalized with sexism, racism and pornographic images. There was a campaign to report all of my social media accounts including my Kickstarter, my YouTube, my Twitter. And they would report them as fraud, spam even as terrorism in an effort to get them suspended. They attempted to knock my website offline, hack into my email and other accounts. They attempted to collect and distribute my personal information including my home address and phone number. There were images made, pornographic images made in my likeness being raped by video game characters and sent to me again and again. There was even a game made where players were invited to “beat the bitch up” in which upon clicking on the screen, an image of me would become increasingly battered and bruised. You get the point, we’ll move on.

What’s even more disturbing, if that’s even possible, than this overt display of misogyny on a grand scale, is that the perpetrators openly referred to this harassment campaign and their abuse as a “Game”. They referred to their abuse as a game. So, in their minds they concocted this grand fiction in which they’re the heroic players of a massively multiplayer online game working together to take down an enemy. And apparently, they cast me in the role of the villain. And what was my big diabolical master plan? To make a series of videos on YouTube about women’s representations in games. Yeah.”

Internet wisdom has it that users are not to “feed the troll”, by not responding to attacks. But this actually has a pervasive effect on women and girls. Its - intended - consequence is to push women out of public spaces and to silence them. Moreover, it allows perpetrators to continue abusing women and girls in impunity. Finally, it contributes to mainstreaming violence against women and girls[^40]. “When women speak up about being attacked online, they are frequently instructed to stop complaining and toughen up. “It’s just words”, they are told. “It’s just the internet”. (...) but gendered hate speech online has significant offline consequences. Female targets suffer socially, psychologically, professionally, financially and politically. Gendered cyberhate is having a chilling effect in that some women are self-censoring, writing anonymously or under pseudonyms or withdrawing partly or completely from the internet. Further, more and more attacks which began exclusively online are spilling into offline domains.”[^41]

[^41]: Emma Jane, Misogyny online, a short (and brutish) history, Sage Swifts, 2017
However, telling women to push back, to toughen up and resist the sexist agenda to hush them up may face a violent backlash that will weigh even more on their social, professional, physical and psychological life. “Talking back” and other individual responses to online abuse promoted by proponents of self-regulation have led certain women into spirals of trolling and threats. In such cases, victims have repeatedly denounced the lack of protection offered them by law enforcement agencies and private tech companies. Policies, legal and law enforcement instruments should take into account the risk of re-victimizing the victims of online abuse. Especially women and girls experiencing male violence at the intersection of several oppressions. Therefore, there is a necessity to acknowledge the impact of violence as to grasp the nature of online VAWG. More, because online attacks are the same everywhere but resilience and mitigation strategies are contextual, there is a crucial need for collective support systems, governmental or not.

It is important to mention here that digital spaces are also spaces where anti feminists and misogynists groups (whether related to political parties/groups or individuals) express their hate of women, in a much more open way than in the offline world. Moreover, on even more hidden places, also on the darkweb, women and girls’ bodies and identities are used and abused.

Here is a list of 12 types of abusers, with their habitat and their tactics, and a proposal of rewording to highlight the type of abuse and violence they perpetrate:

**The troll / the cyber sexual harasser**
Tactics: Attacks women who assert their opinions online
Habitat: Comments sections, forums, chat rooms

**The creepshotter / the digital voyeur and violator**
Tactics: Photographs women and girls without their consent and publishes their photos online
Habitat: Offline public places, Reddit, dedicated websites, social networks

**The revenge pornographer / the digital rapist**
Tactics: Posts private pictures or videos of a sexual nature to shame and humiliate the victim. Extension of intimate partner violence.
Habitat: Social networks

**The online groomer / the child sexual abuser**
Tactics: Builds a relationship with a child via the Internet to bring them into sexual abuse/sex trafficking
Habitat: Social networks, forums

**The cyberstalker / the obsessive abuser**
Tactics: Spies, fixates on and compiles information about women online to scare them and blackmail them
Habitat: Social networks

**The masculinist / the woman hater**
Tactics: Negates and though perpetuates systemic sexism by “defending men’s rights”
Habitat: Dedicated websites, women’s groups’ websites, social networks

---

42 Sandra Laville, Julia Carrie Wong and Elle Hunt, “The women abandoned to their online abusers”, April 11, 2016, available online at https://www.theguardian.com/technology/2016/apr/11/women-online-abuse-threat-racist

43 Interview Alexandra Hache, Tactical Tech, on August 1, 2017
The cyberbully / the humiliator
Tactics: Repeatedly sends hurtful messages and start rumours to shame and humiliate
Habitat: Social networks, communication apps

The dating website manipulator / the sexual predator
Tactics: Seeks power and control over their victim by charming them online and luring them towards a dangerous situation
Habitat: Dating websites, social networks, chat rooms, communication apps

The recruiter / the rape seller aka the trafficker
Tactics: Uses new technologies to lure victims, traffic and sell them and prostitute them
Habitat: Sales websites, dedicated platforms, social media, communication apps

The doxxer / the data thief and criminal shamer
Tactics: Researches and publishes private information online as to publicly expose, out, and shame victims
Habitat: Victim’s social networks profiles, google searches

The malicious distributor / the dangerous defamatory
Tactics: Uses new technologies and a propaganda tool to promote violence against women or women’s rights groups
Habitat: Social networks

The hacker / the invader
Tactics: Intercepts private information and communication, i.e. webcams
Habitat: Can be everywhere

The victims/survivors
As in real life, women and girls are targeted online because of their gender and because of the patriarchal stereotypes underlying gender inequality. Women are attacked because of their identities and their status: among them are self-identified girls and women, female members of LGBTQ+ communities, Women and Girls Of Color, women with economic vulnerabilities, women with disabilities, rural women or women from small communities, migrant women, women with multiple traumas, women with mental health issues, etc. Those identities and/or vulnerabilities or specific visibility, when they intersect, amplify the risks of violence. Women and girls are also targets because of what they do: feminist activists and feminist women and girls, artists, (press) cartoonists, women in male dominated industries, women Human Rights defenders, journalists, NGO activists, lawmakers, members of parliament, academics, bloggers, lawyers, teachers, decision makers, etc.

Here below are examples of how specific groups experience violence by online abusers and criminals.

- Increasingly, women academics are aware of the specific violence they may face online when their publications get widely shared on social media and attracts haters, trolls or groups with a political agenda. Some of them are developing toolkits in order to protect themselves and their peers and are advocating for their institutions to take into consideration the risks they are running44. Others, like Mary Beard, a Cambridge

---

classicist, attacked on Twitter about her research on the ethnic diversity on Roman Britain, respond individually to the attacks\textsuperscript{45}.

- **Women Human Rights Defenders** can experience abuse and violence targeting their intersecting identities and are often victims of sexualised violence, objectifying their bodies and sexualizing them in order to take away their legitimacy\textsuperscript{46}. An Irish Black Woman Human Rights Defender, who has often taken a public stance against racism in her country, says that her interventions in the media are systematically met by insults that target her as a woman and as a black person. “The message it sends is: You’re not supposed to speak out, not supposed to say anything. You should appreciate what you have because you are a foreigner, and a woman.”\textsuperscript{47}

- **Girls and young women and women battling health issues** are particularly at risk. Claire\textsuperscript{48}, a young British woman, had become ill, and her sickness isolated her from her peers. Depressed and vulnerable, she fell prey to an online perpetrator. She was a victim of online sexual assault, commonly called grooming, when she was 15.

---

**Claire’s Testimony - Online child sexual assault**

“I would go to school and come home, that was my daily routine, no socialising, no life outside of school. I was trapped, kept in this bubble that could not be popped. (…) Isolated I began to spend a lot of time in my bedroom alone on social media. It was a way for me to express myself without worrying about my condition. (…) I began to talk to people a lot more online, feeling they accepted me. I started to talk to this one guy in particular, he was so sweet and I felt he really understood me. He made me feel ‘normal’. We spoke for months and I began to really trust him I loved talking to him. He just made me feel brand new (…) I received a message from him one day asking me to send a nude photograph. Although I wasn’t sure at first, he told me that everyone in relationships did it, it was normal. I sent him the photograph and he said it would stay between us and he would delete it. I wasn’t worried, I trusted him. The following day he asked me to send another one but I felt ashamed for sending the first one so I told him I didn’t want too. He got angry and said he would post the picture online and make out I was the biggest slag! (…) The picture was uploaded online and out there for the rest of the world to see! I was so hurt, ashamed, embarrassed and confused. I thought he liked me why would you do that to someone you claim to have fallen for?”

---

- **Female politicians** are also targets of online mobs. In a worldwide survey of violence against female parliamentarians\textsuperscript{49}, the organization IPU reveals how online violence targets women in power, with the objective to silence them and limit their participation: “A European parliamentarian of African origin recounted how a billboard in her country, paid for by far right groups, demanded that she be “whitened with bleach and burned alive”.” Another European parliamentarian said, “I receive emails, sometimes accompanied by pornographic images, and the message ‘get out of politics; get married instead.’” Another Parliamentarian explained that “once, over a period of four days, I received more than 500 threats of rape on Twitter”. In the Netherlands, a broad campaign of advertising boycott, launched by more than 140 high profile women, among them politicians and journalists, hit the online blog GeenStijl. The shock blog was accused of


\textsuperscript{46} Interview with Alexandra Hache, Tactical Tech on August 1, 2017

\textsuperscript{47} Real name withheld. Interview on June 12, 2017

\textsuperscript{48} Real name withheld. Interview on June 12, 2017

denigrating and intimidating women, as well as spreading racist and homophobic hate speech and calling for trolling attacks directed at women\(^{50}\).

- **Female journalists** are at specific risk: two surveys that have been conducted on this topic have indicated that a considerable amount of the work related-threats and intimidation directed at female journalists takes place online (Duggan et al., 2014; Mijatović, 2015). Journalism plays an important role in democracies (watchdog of powerful institutions, stimulation of public debate) and female journalists facing online harassment are also at risk of self-censorship. This has a great impact on freedom of expression/freedom of the press. In the OSCE report, Countering Online Abuse of Female Journalists\(^{51}\), Aina Landsverk Hagen highlights the feeling of shock female journalist experienced when receiving threats “journalists and editors were asked about the first time they experienced being harassed. Some recalled clear death and rape threats; others described milder forms of harassment aimed at their appearance, age or profession. But common to all these stories was that the description of the harassment as a shock.”

- **Feminists** are the “usual” targets of sexism and violent groups online. Moreover, it appears that every women being vocal ends up being called a feminist. In their article Online Abuse of Feminists as an Emerging form of Violence against Women and Girls, describing the results of a survey and the interviews of 226 British feminists, Ruth Lewis, Michael Rowe and Clare Wiper conclude that “40 per cent of (their) sample experienced sexual harassment and 37 per cent experienced threats of sexual violence; high users were more likely to have experienced these. These included rape threats.”\(^{52}\)

- **Women survivors/victims of intimate partner violence.** See below the specific section of this report analysing the link between digital technologies and intimate partner violence.

- Finally, **women in general** are targets for mobs. Facebook groups aiming at humiliating women flourish and allow men to exchange stolen pictures of women and girls for instance: “In December 2016, in Italy, a Facebook group with a vulgar name “Foto di amiche da sborrare” (“Pictures of friends to come on”) was made public when a girl wrote an article about it. She was shocked to discover that some of her male friends were part of the group. People started to report the group but Facebook didn’t close it, saying it did not violate its guidelines. Enrico Mentana and Selvaggia Luarelli, a well-known journalist and a blogger, made the case public and campaigned for it to be shut down. Facebook finally closed this group, but others immediately popped up. It seems they have mirror sites ready to go for the inevitable moment when their site goes down.”\(^{53}\)

---


53 Interview, name withheld
2. Online Violence Against Women and Girls is Part of the Continuum of Male Violence, Impacts all Women and Perpetuates Gender Inequality

The European Women’s Lobby, along with other feminist researchers, organizations and practitioners\textsuperscript{54}, consider digital violence as a reflection of violence against women and girls happening in everyday, offline, life. Online VAWG, such as other forms of violence against women and girls, aims at silencing, scaring, vilifying and banishing women from digital spaces unless they comply to being objectified and treated as inferiors. Perpetrators use the same mechanisms to abuse women and girls, building online landscapes of unsafety where women’s voices and views are considered targets and silenced.

Online violence has a gender

Online violence has persistently been considered gender neutral in the media, and in several national campaigns. Ignoring intersecting discriminations, many actors have preferred to see online violence as a neutral ailment that strikes all users of online platforms and digital technologies, independent of their sex/gender. The internet, we are told, is a place where incivility reigns. Its effects are felt by everyone, regardless of gender.

But, while it is true that people of all genders report being targets of violence, the figures are clear, women and girls are - compared to men - the main targets of online violence: they suffer the most violent forms of aggression and are the most affected by their consequences.

The “Misogyny on Twitter” report\textsuperscript{55} shows for example that 6 million instances of the words “slut” and “whore” were used on Twitter between December 2013, and February 2014.

Across continents, women are 27 times more likely to be harassed online\textsuperscript{56}. Although women and men between the ages of 18 and 24 were disproportionately at risk of online violence, the Pew Center\textsuperscript{57} found that for some of the most severe forms of violence, women were greatly overrepresented: 1 out of 4 young women reported being stalked or sexually harassed at least once. It has also been shown that women and girls are the primary targets of non-consensual pornography.

<table>
<thead>
<tr>
<th>Children at risk of online violence in Romania</th>
</tr>
</thead>
<tbody>
<tr>
<td>For the sake of this research, the ONG World Vision undertook a survey with high schoolers in both rural and urban areas of Romania\textsuperscript{58}. The sample is small, the results can’t be generalised, but the survey shows that while both these boys and girls are targeted by online violence from a very young age, the girls are feeling more at risk in real life. In a sample of 48 children between 12 and 15 years old, from a rural area in Romania, including 29 girls:</td>
</tr>
<tr>
<td>● 22 of them had already received a mean message on internet, among them, 11 girls and 11 boys;</td>
</tr>
</tbody>
</table>

\textsuperscript{54} Women Media Center, Op. Cit.
\textsuperscript{55} Jamie Bartlett and Richard Norrie and Sofia Patel and Rebekka Rumpel and Simon Wibberley, Demos, “Misogyny on Twitter”, May 2014, available online at \url{https://www.demos.co.uk/files/MISOGYNY_ON_TWITTER.pdf}
\textsuperscript{56} United Nations Broadband Committee, Op. Cit.
\textsuperscript{57} Pew Research Center, “Online Harassment”, 2014, available online at \url{http://www.pewinternet.org/2014/10/22/online-harassment/}
\textsuperscript{58} Survey led by Loredana Giuglea, Project Manager World Vision Romania, table available on demand
● 15 of them had already received a mean comment or message on their phone, among them 8 girls;
● 12 of them had already received pictures or videos they didn’t like and that made them uncomfortable, among them 6 girls and 6 boys;
● 12 children had already feared for their security after using internet, among them 9 girls;
● 26 kids felt they knew how to protect themselves and others on the internet, among them 17 girls.

In a sample of 33 adolescents between 15 and 17, from an urban area in Romania, among them 29 girls:
● 11 of them had ever received a mean message or comment on the internet, among them 9 girls;
● 8 of them had ever received a mean message on their phone, among them, 6 girls;
● 10 of them had already received a video or photo that made them uncomfortable, among them 9 girls;
● 10 of them had already feared for their security after going online, among them 8 girls.

These forms of violence are to be understood as part and parcel of the same violence that occur against women in real life, although they are much too often framed in terms that make the gender dimension invisible. Perpetrators use the internet to stalk, harass, surveil, and control their victims. They use technology to isolate their victims from supportive friends and family, or to damage a victim’s credibility or work-life.

One example of the downplaying of the misogynistic underpinnings of online violence is sexting. Often framed as a problem of « user-naïveté » where the victim allowed the picture to be taken or took it herself and then « lost control of its use », it is very often the result of a pre-existing situation of gender-related violence within a relationship or a group of peers. The image is sent as the result of pressuring from male partners or peers.

For women’s organisations, “All forms of male violence against women are linked and form a continuum of violence, which takes very diverse forms, from obvious violations of women’s rights to subtle or distorted forms of control over women’s lives, bodies, and sexuality.” Crimes such as sextortion, grooming and online recruitment are regarded as being another dimension in the continuum of sex trafficking and sexual exploitation of women and girls. Likewise, cyber bullying, stalking, sexist hate speech and online harassment (including threats, verbal and graphic content) on the internet are understood as the reflection of the violence women experiment in public places.

**Online VAWG is therefore a clear part of the continuum of violence against women and girls** and aims to maintain male domination in the digital sphere. It is another strategy for gender inequality to persist, and must therefore be addressed in any policy aiming to realise gender justice.

Emma Holten’s testimony - Living as a victim – My story, the consequences
Presented at the #HerNetHerRights Online Conference, October, 13th, 2017

A big issue for many victims of revenge porn or non-consensual pornography, is the difficulty they experience in detailing the type of suffering they are enduring. For many, the immediate association is a source of sexual shame, but that is not necessarily the dominant experience for victims, although it of course plays a big part.

Rather, what seems to come up again and again as I speak to people who have experienced this, what they are saying is similar to the sense that I felt myself: a sense of unsafety, coupled with a sense of powerlessness over your own life narrative.

It is very important to understand that the goal of violators is to hijack a victim’s identity. The content of the pictures does not matter much, the thing that matters is that they possess the sense of violation and pain.

---


61 This concept was first outlined by Liz Kelly in Surviving Sexual Violence, John Wiley & Sons, 2013 (1988).
Only through this violation and pain can the power over the victim be exerted. This power takes many different forms, from very concrete (blackmail, harassment), to much more subtle (introducing the violation into public conversations and speaking of the victim as if they were worth less in social settings). The goal of violators and the people propping up the violation is to plant in the victim a constant sense of unease. Of not knowing when the next violation will occur.

(...) Conclusively, sexual violations online are an attack on your identity. It is a way for other people to take control of your life. This attempt is rarely coordinated, but becomes an organising structure through which the victim must navigate at all times. Deciding what your name, life, and self should connote is a right that is taken away from us.

Consequences of male online violence on women’s health and autonomy

Consequences on women are no different from those of harassment, bullying and stalking in real life: stress disorders and trauma, anxiety, sleep-disturbances, depression, and physical pain. In a British study that examined the backlash experienced by self-identified feminists online, 26% of those who had been victims of harassment said: “it was really traumatic and I keep thinking about it even though I don’t want to”.  

The four main symptoms of trauma are:

- Intrusive thoughts such as repeated, involuntary memories; distressing dreams; or flashbacks of the traumatic event. Flashbacks may be so vivid that people feel they are re-living the traumatic experience or seeing it before their eyes;
- Avoiding reminders of the traumatic event may include avoiding people, places, activities, objects and situations that bring on distressing memories. People may try to avoid remembering or thinking about the traumatic event. They may resist talking about what happened or how they feel about it;
- Negative thoughts and feelings may include ongoing and distorted beliefs about oneself or others (e.g., “I am bad,” “No one can be trusted”); ongoing fear, horror, anger, guilt or shame; much less interest in activities previously enjoyed; or feeling detached or estranged from others;
- Arousal and reactive symptoms may include being irritable and having angry outbursts; behaving recklessly or in a self-destructive way; being easily startled; or having problems concentrating or sleeping.  

Moreover, online violence has several real-life implications:

- **Fear for one’s safety when facing methodical, organised harassment**: the Irish woman human rights defender was the target of several online attacks. A survivor of real life hate crimes, she often fears for her safety: “I live in a small town, it is easy to know where people live. In crowds, I check whether I am being followed. At work, I lock the doors, I have seen what real hate looks like. I don’t think they are afraid of anything.”
- **Isolation**: “Cyber-stalking, where men trace the woman’s actions through the use of apps and connected objects in the woman’s home or work space. Because this type of behaviour is not very well known, women can appear paranoid and lose credibility when they report this. As with other forms of psychological abuse, women isolate themselves. They fear using their phone, their computer. All of the objects that empower them on a personal and professional level become off-limits”, says psychologist Karen Sadlier, an expert on domestic abuse.
- **No safe space**: the rapid and uncontrolled diffusion of personal information, malicious content and physical and sexual assaults creates a world where the victims have no possibility of protecting themselves from the abuse. Stolen pictures can reappear on various websites and the law still does not protect women adequately from publishing their private image or information. Tiziana Cantone, an Italian woman, committed suicide in

---

62 Ruth Lewis, Michael Rowe, Clare Wiper; Op.Cit.
63 American Psychiatrist’s Association, “What Is Posttraumatic Stress Disorder?”, available online at [https://www.psychiatry.org/patients-families/ptsd/what-is-ptsd](https://www.psychiatry.org/patients-families/ptsd/what-is-ptsd)
September 2016 after a sexual video she had made landed on several sites. While she won a lawsuit against Facebook, she lost against several other platforms and took her own life, days after the court ordered her to reimburse 20,000 euros in legal costs. The images were still online months after her death.

- **No place to hide, as internet is a crowd**: perpetrators go as far as to broadcast their mistreatment of women online, as these two famous cases of Facebook live gang rape. The one of a 15 years old Chicago girl in march 2017, where at least 40 people watched the rape live and none of them reported it. Or in Sweden in April 2017: “Three people have been jailed for gang raping a woman and broadcasting the horrific attack on Facebook Live. Footage of the rape was posted in a private Facebook group with 60,000 members. The Swedish court heard the prosecuted man had encouraged his friends, and ‘laughed’ while filming the attack on his phone. All three men pleaded not guilty, two of them claimed that the sex was consensual, and they argued that they were unaware that the victim did not want the images to be posted online. But the prosecutors said that the woman was ‘heavily drunk’ and ‘under the influence of drugs’, a situation that the men must have realised. The judge Nils Palbrant said: “It is not possible for a person in such a situation to consent.” The three men were also ordered to pay a total of 335 000 kronor (€34.500) to the victim in damages.”

---

### The impact of online violence on women in Italy

Sodfa Daaji’s perspective at the #HerNetHerRights Online Conference on October 13th, 2017

I would like to bring with me the experience of two young women, killed by the web.

The death of Carolina Picchio brought on the table of the institutions the fact that cyber violence is a reality, that it exists and can’t be treated anymore as a joke. Carolina died at 16 years old, and she was killed multiple times by those who watched and shared the video uploaded by her rapists. Carolina died from suicide and was killed multiple times by those who treated her rape as a joke, as something worth to watch, to share and to comment. The episode was followed by the adoption of a law against any form of cyber violence, including revenge porn, but the law is applied only for victims that are under age.

This law could have helped Tiziana Cantone, 29 years old, who was left without protection and was killed by the multiple jokes made by women and men about her private life. A private video of her intimacy was firstly shared on a whatsapp group, and then widespread on facebook and on porn sites. Tiziana killed herself, and is killed again by those who are still watching her videos, by those who saved the video of her intimacy, of her private life. Tiziana was killed by those who judged her intimacy, who entered without permission in her private life and felt the right to judge her, to joke at her, to follow here and make her life a complete hell.

---

### Impact of male online violence on women’s employment and reputation

A third of women faced with online harassment feel that it has impacted their reputation. In the wake of the publication of the United Nations Broadband Committee Report on Cyberviolence and VAWG, the Under Secretary General of the UN and the Executive Director of UN Women Phumzile Mlambo-Ngcuka, expressed their worry that women would restrict themselves from the Internet, due to the pervasiveness of cyber VAWG: « To be disconnected from technology in the 21st century, it’s like having your freedom disrupted: your right to work, your right to meet people, your right to learn, your freedom of speech. So if women become so intimidated and traumatized from the experiences they may have, it’s a whole world that will be lost to them for the rest of their life. »

---


65 Testimony from the women’s shelter in Sigtuna, Sweden, [http://kvinnojourensigtuna.se](http://kvinnojourensigtuna.se)

Digital technologies and intimate partner violence

Perpetrators of domestic and intimate partner violence are increasingly using sexual imagery as a tool to threaten, harass and/or control both current and former partners. Domestic violence support workers describe cases where perpetrators have recorded intimate partner sexual assaults, where women were coerced into having intimate photos taken, of threats to publicize sexual images or footage if legal action is pursued. Furthermore, the security of women’s shelters and safe houses has become compromised by the use of localisation on cell phones.

A social worker said in an interview with Australian researchers: “I think that the danger (...) is that you’re always there in a sense. It’s not a physical location – it’s accessible and it’s often on our person. So our location follows us instead of us being in the location (...) back in the day, you could only be found at a place if somebody knew your location, so safe houses were safe because you could only be accessed emotionally if you were accessed physically.”

Furthermore, technology enables perpetrators to send a constant barrage of messages to a victim whether by phone, email and text messages, or tweets and posts on Facebook. Whether it is the content of the messages or their frequency, the intent remains the same: to show to the victim that she can be found, that she is not to consider herself at peace.

According to a Women’s Aid survey from 2017,

- 45% of domestic violence victims reported experiencing some form of abuse online during their relationship;
- 48% reported experiencing harassment or abuse online from their ex-partner once they’d left the relationship. 38% reported online stalking once they’d left the relationship;
- 75% reported concerns that the police did not know how best to respond to online abuse or harassment. This includes 12% who had reported abuse to the police and had not been helped.

A good practice: SafetyNed, a Dutch project to protect women victims of domestic violence online and via new technologies

Essa Reijmers, Dutch expert to the EWL’s Observatory on Violence Against Women

SafetyNed stands for the fundamental right of every woman to be safe online in all circumstances whether she is in a women’s shelter, in her own home, at work or elsewhere. The project is an initiative of four women’s shelter organizations that joined forces as they increasingly experienced how abuse of technologies and different forms of online violence impact the lives of survivors of domestic violence. The SafetyNed founders saw the urgency as women arrived in their shelters and were found via their Iphone within the hour upon arrival. They noticed fake accounts on social media, cases of spyware, etc.

They also acknowledged that as frontline organizations, they lacked the proper awareness, tools and knowledge on technology and online media to protect their clients and help them protect themselves. As they did not feel ‘tech savvy’ enough there was a tendency amongst their advocates to shy away from technologies and issues on online violence. But they were convinced that it was absolutely inadmissible to tell women that suffer online abuse to get offline.

---

68 Clare Laxton, Women’s Aid, Virtual World, Real Fear, Women’s Aid report into online abuse, harassment and stalking, 2014, available online at http://bit.ly/2h0W4OX
SafetyNed was launched, in partnership with the United States’ National Network to End Violence against Women’s Safety Net project, a pioneering project in the realm of tech and domestic violence that has existed since 2002.

SafetyNed is a platform and a network organization that integrates, builds and shares knowledge on abuse of digital technologies and online violence.

What has been realised so far:

- The SafetyNed website includes information, tools and survivors’ stories;
- A TechTeam of eight specialists has been recruited and trained. They are the ‘geeks’, the specialists that assist all the front line workers in shelter organizations. They instruct their co-workers, organize training sessions and offer daily support on difficult cases involving technology and online issues;
- The TechTeam also continues to document stories of survivors and their advocates, with a focus on effective strategies to deal with abuse of technology;
- Shelters have included a risk-assessment screening of online violence to the risk-assessment tools that were already in use in their residential and non-residential services;
- SafetyNed also puts an important focus on raising awareness with frontline domestic violence workers, both in shelters and other service providers such as the police, the judiciary etc. Raising awareness with policy-makers and lobbying on this issue will also be a priority for the project.

Like every innovative project, SafetyNed faces challenges: funding is not easy, the four founding shelter organizations have chosen to invest heavily in this project to make this issue visible. Now that the project is visible, policy-makers and commissioners, such as the Ministry of Safety and Justice and the local authorities have become more aware of the necessity of this work and get interested in the project’s developments. Technologies are moving and developing so quickly that many advocates are afraid they will never be able to keep up. This is why there is the crucial need to partner with other experts and build a community of knowledge and sharing in order to keep on moving forward with reclaiming the right of being safe online.

Facilitating trafficking and prostitution, normalising pornography

The legal voids regarding online publication and anonymity has allowed prostitution to flourish online. On Google, thousands of occurrences of the term « sugar daddy » link to prostitution sites.

In France, where paying for sex has been punishable by law since April 2016, Vivastreet.com - a website best known to the general public for its housing ads - makes profits of up to 10 million euros annually by selling barely disguised ads for sexual exploitation. As a “content host” and not an “editor”, it is not required to check the ads, only to react to eventual complaints. Foreign escort agencies are even more direct. Men discuss the “merits” of the women on separate forums. Seldom do any of these actors of prostitution get prosecuted.

In the United States, however, the fight against sex trafficking has been taken to the courts. Website Backpage.com’s owner and main investors were charged with pimping and money-laundering. The prosecution alleging that the website designed the website specifically to allow for this type of ad, and profited massively from them. While the charges were dismissed on the basis of free speech, lawmakers are aiming to amend the laws.

---

69 https://nnedv.org/content/safety-net/
70 http://safetyned.org/
regulating tech companies, in order to protect victims of sex-trafficking. The Stop protecting Sex Traffickers Act, a bi-partisan law being advance in the US Senate, is currently the subject of a hot public debate. In her research paper about the marketing of Eastern European women as prostitutable bodies on the internet, Karina Beecher connects the “marketing (...) of Eastern European women on the Internet (...) to the broader international sex industry of sex trafficking and mail-order brides or “marriage agencies”. The sex industry generates majority of its profits from sex trafficking and mail-order bride agencies worldwide (Hughes 2002c).”

**Online sexualized violence and pornography are urgent issues to be addressed**

Today, pornography is available in every laptop and smartphone at any time, twenty-four hours a day. Research on pornography shows that mainstream productions almost only contain forms of sexualised violent acts and have very serious consequences both for the girls and women being exploited and abused in the industry, but also on consumers. On the relation between pornography and rape culture, Karina Beecher quotes Rae Langton “We define pornography as the graphic sexually explicit subordination of women through pictures or words that also includes women dehumanized as sexual objects, things, or commodities; enjoying pain or humiliation or rape” (Langton 2009, 138), and Andrea Dworkin “Pornography says that women want to be hurt, forced, and abused, pornography says women want to be humiliated, shamed, defamed; pornography says that women say no, but mean yes—yes to violence, yes to pain” (Dworkin 1993, 23). These images indicate that, “Pornography says that women are sluts, cunts; pornography says that pornographers define women; pornography says that men define women; pornography says that women are what men want women to be” (Dworkin 1993, 24). Pornography sexualizes and dehumanizes women.

Violence in pornography has increased remarkably, while the consumers are getting younger and younger. Research show that pornography normalizes sexual violence against women and girls, and that it limits healthy sexual relationships. Young people and future generations need to be able to develop their own sexuality, free from pornography’s images of sex as connected to violence, humiliation and assaults.

**Online violence and harassment at work and in education**

- More than half of all women in the UK, and nearly two-thirds of women aged 18 to 24, experienced sexual harassment at work.
- 80% of women working in large companies in France state being regularly confronted with sexist attitudes or decisions, having an impact on their self-confidence, their well-being and performance.

The project ‘Safe at Home, Safe at Work’ of the European Trade Union Confederation (ETUC) draws together evidence collected from interviews carried out as part of 11 detailed country case studies of European-level developments on gender-based violence and harassment at work, including domestic violence at work. The report shows how trade unions and/or social partners have approached the issue in negotiations, collective bargaining, union awareness-raising, training and campaigns, and partnerships with women’s organisations working to end gender-based violence.

In the UK The “teaching union carried a survey on online harassment and abuse in 2016 and found that 50% of members were aware of comments or information being posted online about them in relation to their role as a

---

73 Karina Beeche, “The sexual marketing of eastern european women through internet pornography” College of Liberal Arts & Social Sciences Theses and Dissertations. Paper 33, 2010, available online at [http://via.library.depaul.edu/etd/33](http://via.library.depaul.edu/etd/33)
74 ETUC Safe at Home Safe at Work UK country case study, available online at [https://www.tuc.org.uk/sites/default/files/ETUCdomesticviolenceUKdraft.pdf](https://www.tuc.org.uk/sites/default/files/ETUCdomesticviolenceUKdraft.pdf)
76 European Trade Union Confederation : [https://www.etuc.org](https://www.etuc.org)
teacher. Information posted online was often extremely abusive and derogatory, and included sexist comments and sexual harassment. One teacher reported rape threats being posted online. Many also reported online harassment of girls by boys in the school, including circulating naked photographs without consent.”

3. Understanding the Root Causes to Take Action to End Online Violence Against Women and Girls

In order to develop actions to combat and eliminate online violence against women and girls, it is important to understand its root causes.

Several reasons underpin online violence on women and girls. In general, violence against women and girls is rooted in meta-cultural and systemic aspects of society like patriarchy, rape culture, neoliberalism and hyperindividualism as well as political aspects of society like the backlash on progressive ideas e.g. feminism, but also intersecting vulnerabilities.

Like any other form of male violence, online violence against women and girls is ignored, ridiculed or minimised. Victims' experiences are often considered as "incidents" rather than patterns of behaviour, and victims are often blamed for the violence they face.

Several root causes can be identified, some linked directly to the unequal distribution of power and roles between women and men in society, others linked to the structure of the Tech industry and the nature of online spaces.

Rape culture

Rape culture is prevalent in the digital sphere. Rape culture is defined by Emilie Bushwald, author of “Transforming a Rape Culture” as “a complex set of beliefs that encourage male sexual aggression and supports violence against women. It is a society where violence is seen as sexy and sexuality as violent. In a rape culture, women perceive a continuum of threatened violence that ranges from sexual remarks to sexual touching to rape itself. A rape culture condones physical and emotional terrorism against women as the norm... In a rape culture both men and women assume that sexual violence is a fact of life, inevitable.”

Examples of this rape culture are pervasive on the internet and include:

- **Reframing violence to make it sexy and sex to make it violent.** In January 2017, a Belgian blogger discovered that men were sharing images and videos of women they purportedly had had sex with on a private Facebook group called Babylone 2.0. 52,000 men had been part of this private group where one could see images of women, accompanied by degrading, objectifying comments on their looks, their ages, their naïveté.

- **The ongoing promotion of violence and hate towards women through pornography.** 30% of all internet traffic constitutes porn: research also reveals that 88.2% of top rated porn scenes contain aggressive acts and 94% of the time the act is directed towards a woman.

The Women’s Media Center and Marshall University have issued a list of characteristics of rape culture:

- Blaming the victim (“She asked for it!”)
- Trivializing sexual assault (“Boys will be boys!”)
- Sexually explicit jokes

---

78 Emilie Buchwald, Pamela R Fletcher, Martha Roth, Transforming a Rape Culture, Milkweed Editions, Minneapolis, 2005 (1993)
81 Marshall University, Women's Center, “What is Rape Culture”, available online at [http://www.marshall.edu/wcenter/sexual-assault/rape-culture/](http://www.marshall.edu/wcenter/sexual-assault/rape-culture/)
● Tolerance of sexual harassment
● Inflating false rape report statistics
● Publicly scrutinizing a victim’s dress, mental state, motives, and history
● Gratuitous gendered violence in movies and television
● Defining “manhood” as dominant and sexually aggressive
● Defining “womanhood” as submissive and sexually passive
● Pressure on men to “score”
● Pressure on women to not appear “cold”
● Assuming only promiscuous women get raped
● Assuming that men don’t get raped or that only “weak” men get raped
● Refusing to take rape accusations seriously
● Teaching women to avoid getting raped instead of teaching men not to rape

The digital sphere is a male-dominated world

Women in male-dominated areas, especially women in Tech companies, face forms of sexism such as unequal pay, recruitment unbalance and sexual harassment. “The 2016 Women in the Workplace study - a major US national survey - found that 19% of the technology sector’s top executives are women - broadly in line with sectors like banking, media, or professional services. The same study found that, across all industries, 30% of women who negotiated for a promotion or a better salary were told they were “bossy”, “aggressive” or “intimidating”⁸².

According to the EC Advisory Committee for Equal Opportunities:

● Only 9 in 100 European app developers are female;
● Only 19% of ICT managers are women (45% women in other service sectors);
● Only 19% of ICT entrepreneurs are women (54% women in other service sectors);
● Less than 30% of the ICT workforce is female;
● Women represent around 33% of total graduates in science and technology and around 32% of employees of the ICT sector.

The Elephant in the Valley survey, that researched the gender gap in Silicon Valley’s Tech companies found that “90% of the 220 women interviewed had witnessed sexist behaviour at company off-sites and/or industry conferences. About 87% of them had heard demeaning comments from their colleagues.”⁸³ Numbers show that the Tech industry is a male dominated sector. This industry, shaped by and for men, is therefore creating spaces where women’s voices, stories and personas are alien and unwelcome.

Women in Tech: a year of reckoning for women in Silicon Valley

In February 2017, female engineer Susan J. Fowler wrote a long blog post detailing the sexism she had been a victim of at Uber. After reporting the sexual harassment she was being subjected to by her manager in 2014, she wrote, her career mobility had come to a startling stop.⁸⁴ Before her, several women had levelled accusations at leading firms, but this time more women decided to speak out and the companies reacted more strongly than they ever had. In the space of a few months, Uber’s CEO Travis Kalanick was asked to resign. Several leading investors, accused of harassing female entrepreneurs, were forced out of their firms. A ‘star’ engineer was forced to resign from his job after his company found that he had been accused of sexual harassment at his previous

---

⁸⁴ Susan J. Fowler, Reflecting On One Very, Very Strange Year At Uber, February 19, 2017, available online at https://www.susanjfowler.com/blog/2017/2/19/reflecting-on-one-very-strange-year-at-uber
Structure of the Tech industry and nature of online spaces

The power imbalance between the giants of internet, shaping policies and regulations, and unorganized individuals leads to the opportunity for male violence to happen. The lack of political will from governments to interfere has also a role to play.

Online spaces are both vast and very close, and with no borders, where violence can be made invisible, or can be amplified by anonymity. The absence of borders makes it difficult to grasp the phenomenon. Online spaces are still considered as separate spaces from society, as if they are not part of the real world. It creates legal shortcomings like impunity, grey areas, absence of accountability mechanisms, and lack of law enforcement efforts. As an illustration, research reveals that the response of the criminal justice sector to women victims of cyber VAWG is inadequate. For example, of the 1,160 incidents of revenge porn reported during the first six months after its criminalisation in the U.K., 61% resulted in no further action pursued against the alleged perpetrator. Consent is also manipulated in online spaces: it is one thing to consent to publish one’s pictures on one’s personal page, but it is another thing to see one’s pictures shared by others without one’s consent. In the digitalised world of data, what is personal and public data is blurred. Dissemination of personal data, even in the public domain, must be conditioned by consent.

In this context, online spaces are considered spaces where the individual is free from constraints and law, which also leads to situations where many have no information about their rights, and lack self-protection knowledge.

This situation leads directly to the debate around freedom of speech on the internet. The current conversation between stakeholders is all about the complex and tense balance between free speech and its limits when it comes to violations of human rights and violence against women.

We would like to share here the words of the Due Diligence Project, on the definition of and principles behind the concept of freedom of speech:

<table>
<thead>
<tr>
<th>Principle: It is not an exercise of freedom of expression to consciously intimidate women online, express the wish to rape them, threaten to harm them or incite others to do so</th>
</tr>
</thead>
</table>

Human rights are universal, inalienable, interrelated, interdependent and indivisible. An individual’s human rights are not absolute in that it cannot be enjoyed at the expense of the human rights of others. Freedom from gender-based violence against women, freedom of expression and rights to privacy are protected by international human rights law.

The exercise of these rights under international human rights law is not absolute and may be subject to certain restrictions, but these shall only be such as are provided by law and are necessary for respect of the rights of others; and for the protection of national security or of public order. The application of these restrictions by States however, “may not put in jeopardy the right itself”.

This is different from freedom of opinion. The right to hold opinions without interference is an absolute right and “permits no exception or restriction”. However, the expression of an opinion, that is the right to freedom of expression

---

bears “special duties and responsibilities”. The free exchange of and access to information does not equate to unregulated violence. Freedom of expression or access to information cannot be bought at the expense of women’s security and safety.

Dialectics between freedom of speech and protection

Some feminist researchers remind us how complicated the relationship between the protection of privacy and feminism can be. “A great deal of violence, coercion, happens in the privacy of home which has always made it difficult to politicize the personal. So it makes feminists cautious if not reluctant about the protection of privacy online. This can be thought productively as a kind of double bind: privacy on one hand is a privilege, that isn’t afforded equally to all: marginalized groups, especially those who inhabit multiple intersections, are groups whose privacy was never considered on the same level as those of the privileged groups. But we can also think of giving up privacy, consenting to transparency as a privilege that isn’t distributed equally. We all have something to hide, but who’s in the best position to say “I have nothing to hide”? That again is usually the privilege groups. So instead of engaging in these “is privacy good or bad for women” types of debates, it might make more sense to focusing more on highlighting these inequalities: who has access to privacy? Because marginalized groups are exposed to more harassment and persecution without privacy88:.

Demands for a feminist internet

This is why several advocates for women’s human rights on digital platforms have issued demands and principles for a feminist internet89. They ask for a culture of consent to oppose to rape culture, both in policies and in terms of service of internet platforms. They call on States and the private sector to stop using personal data for profit and for manipulating online behaviours. According to them, surveillance is the weapon of patriarchy used to exercise power over women’s bodies and freedom. They raise the topic of memory and the right to access, control and delete one’s personal data. Contrary to many policy makers who push for an instrument such as a RealID on the Internet, many feminists advocate for the right to anonymity as, according to them, anonymity enables freedom of expression particularly when it comes to challenging gender stereotypes and discrimination.

Prevention, Protection and Punishment

In most European countries, Tech companies fall under “service provider” laws that explicitly state that they are not responsible for the content published by their users. While certain countries have begun to enforce stricter laws, Tech companies are mostly required to remove such content “expeditiously”, a rather vague requirement.

In recent developments, the ruling Tech companies have chosen to contribute to the prevention, protection and punishment of women’s human rights violations in the digital sphere by strengthening their voluntary engagements to curb illegal, dangerous and harmful content.

Four major tech corporations signed a Code of Conduct90 countering online hate speech with the European Commission in 2017. In it they commit to “review the majority of valid notifications for removal of illegal hate speech in less than 24 hours and remove or disable access to such content, if necessary”. But a report by the Commission reveals that Twitter removes hate speech from its network less than 40 percent of the time after such content had

---

88 Nicole Shephard, presentation to the #HerNetHerRights online conference on Oct 13th, 2017
been flagged to the company⁹¹. And a German report showed that less than 1 percent had been removed in the first 24 hours⁹².

In May 2017, Facebook’s moderation guidelines were leaked by the Guardian⁹³. They showed that a great amount of verbal and graphic violence against women and girls is tolerated by the platform’s moderators. Despite Facebook’s recent announcement of a new monitoring tool to prevent images posted without consent, experts and civil society agree that big corporations’ community standards do little to prevent the violation of women’s human rights and freedom of expression: “Facebook considers women’s bodies as inherently sexual. Although last year Facebook reiterated that breastfeeding or pictures of mastectomies do not fall under its nudity ban, it still regularly censors news in the public interest, pictures of protests, sex and health educational campaigns, and artistic expression.”⁹⁴ Big internet corporations argue that they are tech companies and not media. They do not recognize that they contribute greatly to shaping and influencing perceptions and behaviours via their community standards and moderating practices. However, women’s and girl’s’ rights to safety and visibility are at stake.

Furthermore, in their attempts for accountability, service providers shall remember they have an immense role to play in providing information on random IPs used by perpetrators of online abuse. Finally, Tech companies should not send the message that victims are to blame. A whole complete cultural shift is needed also for the online world.

Normalisation of male violence in other virtual spaces

Male violence against women and girls is also normalised in other virtual spaces, such as music videos, films, video games, and advertising.

- The **pop music industry**, including rap music, is widely dominated by sexism. Singer Grimes for example “has written about the infantilisation and sexualisation of women in the industry by both the public and those who work within it⁹⁵”. Singer Bjork also highlighted how sexist the music industry is: “After being the only girl in bands for 10 years, I learned – the hard way – that if I was going to get my ideas through, I was going to have to pretend that they – men – had the ideas⁹⁶”. Moreover, many music video clips⁹⁷ emphasize female domination and reinforce harmful stereotypes by mainstreaming pornofication. “Pornofication refers to the notion of mainstream cultural products being imbued with aesthetics of porn⁹⁸”.

- While **sexism in film** has been a topic of discussion for decades, the discussion recently shifted from the number of leading roles for women, and of contracts for women directors, to the way in which a whole industry may have covered a repeat sex offender because of his power in the film industry. After the New York Times⁹⁹ revealed in October 2017 that several women had been victims of sexual violence at the hands of producer Harvey Weinstein, many actresses came forward and recounted stories of harassment, aggression and rape, presented as requirements to obtain parts in hit movies. All of Hollywood knew, the victims say, but no one spoke up.

---

⁹⁴ Erika and Fungai, GenderIT, “Did Facebook Finally Figure Out That Consent is More Important than Nipples?”, May 3, 2017, available online at http://www.genderit.org/articles/facebook-intimate-image-filter
⁹⁵ Heather Saul, Rolling Stone, “Grimes on music industry sexism”, April 15, 2016, available online at http://ind.pn/22zSPfn
The video gaming community has also been denounced for its deep-rooted sexism. Canadian video game critic Anita Sarkeesian payed a hefty prize for announcing the mere intention to examine gender in video game storylines, while American developer Zoe Quinn came under massive attack when a disgruntled ex implied she had used sex to advance her career. In France, gamer mar_lard recounted in 2012 several tales of misogynist insults and rape threats in the gaming community. Sexist representations of women spilling over from virtual life into real life, at gaming events where women are made to feel unwelcome. Her article received widespread attention, both negative and positive.

Sexist advertising is particularly affecting the mental health of young women. In a study conducted by the Swedish Women’s Lobby in 2013, nine out of ten female respondents between 13 and 30 years of age answered that advertising has made them feel bad about their looks and that that it made them want to change something about themselves.

The Harvey Weinstein affair: showing the best and worst of social networks

In the days following the revelations about Harvey Weinstein, several women took to the media and to social networks to denounce what they had gone through at the hands of men like Harvey Weinstein. As the movement became more and more massive on social networks, one of the American producer’s victims, actress Rose McGowan (@rosemcgowan), launched a petition calling for the entire board of Weinstein’s company, Miramax, to resign. She accused them and a number of Hollywood personalities of having known, and covered up, Harvey Weinstein’s behaviour. Twitter’s response came swiftly. On October 12 2017, her account was suspended. Hours later, it was reinstated and Twitter explained a private phone number had been published. Now that it was deleted, the company said, the account was reactivated. Several users reacted with disbelief.

Meanwhile, the uproar over the impunity of perpetrators of sexual violence mounted on several social platforms. And soon, women everywhere were posting using the #MeToo hashtag after a viral post by American actress Alyssa Milano that read: “Me too. If all the women who have been sexually harassed or assaulted wrote #MeToo as a status, we might give people a sense of the magnitude of the problem.”

The sheer number of tweets and posts created a shielding and empowering effect. In the following days and weeks, several women named their attackers and decided to pursue legal action.
4. Taking action: Existing Legislation and Policies in Europe

The new global Agenda2030 includes a specific goal on “achieve gender equality and empower all women and men”. One of the targets of SDG Goal 5 is: “Enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women”, while another one demands the following: “Eliminate all forms of violence against all women and girls in the public and private spheres, including trafficking and sexual and other types of exploitation”. In this context, it is crucial that governments and all actors of civil society and the private sector, take action to end online violence against women and girls.

In July 2017, the Committee on the Elimination of Discrimination against Women (CEDAW Committee) adopted a new General Recommendation, which builds on a previous key document, General Recommendation 19. General Recommendation 35 updates the previous text, and provides a strong reference and tool for advocacy action for women’s organisations. Taking stock of the developments of the last 25 years, GR 35 reaffirms the UN commitment to a world free from violence for all women and girls. GR 35 recognises the new forms of violence against women and girls, redefined “through technology-mediated environments, such as contemporary forms of violence occurring in the Internet and digital spaces”.

Existing EU legislation and policies

The EU recently signed the Istanbul Convention, the first European multi-country legally binding agreement on curbing violence against women and domestic violence. Several articles of the Istanbul Convention can be applied to the specific topic of digital violence. Hence, the Istanbul Convention is an appropriate tool for demanding more visibility and actions against Violence against Women and Girls on the Internet.

<table>
<thead>
<tr>
<th>Council of Europe Convention on preventing and combating violence against women and domestic violence (Istanbul convention)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Chapter V Substantive law</strong></td>
</tr>
<tr>
<td><strong>Article 33 – Psychological violence</strong></td>
</tr>
<tr>
<td>Parties shall take the necessary legislative or other measures to ensure that the intentional conduct of seriously impairing a person’s psychological integrity through coercion or threats is criminalised.</td>
</tr>
<tr>
<td><strong>Article 34 – Stalking</strong></td>
</tr>
<tr>
<td>Parties shall take the necessary legislative or other measures to ensure that the intentional conduct of repeatedly engaging in threatening conduct directed at another person, causing her or him to fear for her or his safety, is criminalised.</td>
</tr>
<tr>
<td><strong>Article 40 – Sexual harassment</strong></td>
</tr>
<tr>
<td>Parties shall take the necessary legislative or other measures to ensure that any form of unwanted verbal, non-verbal or physical conduct of a sexual nature with the purpose or effect of violating the dignity of a person, in particular when creating an intimidating, hostile, degrading, humiliating or offensive environment, is subject to criminal or other legal sanction.</td>
</tr>
</tbody>
</table>

Several European Union directives address aspects of violence against women and assistance to victims of gender based violence. The Victims’ Rights Directive and the Directive on preventing and combating trafficking in human beings and protecting its victims. Experts and the European Parliament have however expressed the need
for a general directive on violence against women, with clear definitions of the different types of violence\textsuperscript{104}. The transnational nature of digital violence against women and girls adds on to the need for an EU wide (at minimum) legally binding instrument that would protect women and girls from such violence.

The 2011 Directive on combating the sexual exploitation of children online and child pornography, addresses online violence against children, such as grooming.


- Article 14 establishes that hosting providers are not responsible for the content they host as long as (1) the acts in question are neutral intermediary acts of a mere technical, automatic and passive capacity; (2) they are not informed of its illegal character, and (3) they act promptly to remove or disable access to the material when informed of it.
- Article 15 precludes member states from imposing general obligations to monitor hosted content for potential illegal activities.

Several \textit{European Parliament resolutions} address the topic of online VAWG. Most of them acknowledge the existence of online violence and urge the Council, the Commission and Member States to develop legal and policy strategies to tackle the phenomenon.

In European Parliament resolution on gender equality and empowering women in the digital age, adopted on April 28th 2016, the EP urges the Commission, the EU and Member states to take action against “\textit{violence against women in a digitalised world}”. Regarding prosecution of digital crimes, it addresses the need for legal instruments to report on, prosecute and punish the perpetrators of digital violence crimes as well as the need for comprehensive strategies to protect and support victims.

In European Parliament resolution of 13 December 2016 on the situation of fundamental rights in the European Union in 2015, the EP acknowledges the role of ICT platforms and new technologies in violence against women and asks for the development of awareness raising campaigns. In this same Resolution, the Parliament addresses the topic of digital rights and insists on the need for protection of personal data and privacy.

In the Resolution of March 12th 2013 on eliminating gender stereotypes in the EU, the EP calls on Member states and the Commission to tackle the root cause of Violence against women by acting against stereotypes and discrimination in the media, while in European Parliament resolution of 3 September 2008 on how marketing and advertising affect equality between women and men, the EP calls on the Council and Commission to implement existing provisions in Community law on fighting sex discrimination and incitement to hatred on the grounds of sex.

The Honeyball resolution of 26 February 2014 on prostitution and sexual exploitation “\textit{Draws attention to the growing role of the internet and social network media in recruiting new and young prostitutes through human trafficking networks}; calls for prevention campaigns also to be conducted on the internet, taking into account the vulnerable groups targeted by these human trafficking networks”. It also “\textit{Draws attention to some of the effects, mostly negative, of mass-media production and pornography, especially online, in creating an unfavourable image of women, which may have the effect of encouraging the human personality of women to be disregarded and of presenting them as a commodity; warns as well that sexual liberty must not be interpreted as a license to disregard women}”.


\textsuperscript{105} \url{http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32000L0031}
In her answer to Barbara Matera’s question to the Commission of 24 January 2017 regarding digital violence against women and the role of the EU on sensitisation, pressure on corporations and legal response, Ms Jourová, Commissioner Justice, Consumers and Gender Equality, stresses that Member States who have ratified the Istanbul Convention “must establish, in their national law, offences on stalking and sexual harassment. The Convention encourages cooperation with the private sector and the media to tackle this problem.”

Finally, several policy documents address the topic of online violence against women and girls

Combating gender-based violence and protecting and supporting victims is one of the 5 priorities in the European Commission’s Strategic Engagement for Gender Equality 2016-2019 under DG Justice.

Among the European Commission’s 16 initiatives towards a Digital Single Market for Europe, initiatives 11, 12 and 13 aim at tackling illegal content on the Internet, protecting privacy and focusing on cyber security. The provisions are not specifically oriented to violence against women and girls but may offer entry points for lobbying.

In the Council’s conclusions on the review of the implementation of the Beijing Platform for Action, the Council calls upon both Member states and the Commission to issue and apply comprehensive policies as to tackle emerging forms of violence linked to digital platforms and new technologies.

The Council conclusions on Preventing and combating all forms of violence against women and girls, including female genital mutilation call on the Commission to carry out specific actions to combat online VAWG, including support to private sector’s initiatives to protect women from online violence and to review legislative frameworks and legal instruments as to combat online violence.

**National pieces of legislation and good practices**

At national level, several pieces of legislation and good practices for law enforcement have emerged, but a great number lack a gender perspective (especially laws on hate speech) and often still fail to address women’s human rights violations in a comprehensive manner. However, some initiatives reveal the growing interest and awareness of national institutions.

In Spain, the Penal Code was reformed in 2015, introducing new types of penalties related to online gender-based violence:

- Harassment and stalking are punishable under article 172 ter.
- Cyberbullying or sexting, consisting of disseminating, revealing or giving a third party images or audio-visual recordings of a person, without their authorization, obtained in a private setting, fall under section 7 of article 197.

In Portugal, criminal laws focus on cybercrime:

- Law n.º 109/2009, 15th September, resulting from signature ratification of the Budapest Convention on Cybercrime and from the transposition to the Portuguese Law of the Framework-Decision n.º 2005/222/JAI, 24th February, from the Council of Europe. The Convention and the Framework-Decision aim at strengthening cooperation between countries to fight the use of new technologies to commit crimes. None of these legal instruments have a gender perspective.
- The additional protocol to the Budapest Convention, adopted in Strasbourg on 28th January of 2003, focuses on racist and xenophobic crimes practiced via ICT channels.
- The Portuguese Criminal Code punishes privacy intrusion (192.º), privacy intrusion by informatic means (193.º), illicit photographs or videos/ illicit recording of voice conversation of photos (199.º); violation of private correspondence or telecommunication/ intercepting/recording conversations, emails, or other private data (194.º/195.º).

---

106 Most legal data collection was made possible by the participation of the national experts of the European Women’s Lobby’s Observatory on Violence against Women.
In Austria, in 2015, the Criminal Code was amended to better include crime online. The amendment included a number of offenses, such as cyber-bullying, cyber-mobbing, online-stalking, insults, hate speech and personal defamation that are now punishable by law. The law also makes it possible to enforce a deletion of comments on social media platforms (especially Facebook). In certain cases, the providers (i.e. social media platforms such as Facebook, Twitter, YouTube etc.) can be held responsible if they refuse to delete the offensive postings after having been informed of their hateful content.

Furthermore, several court decisions have secured information rights to victims of cyber violence. Providers are now obliged to provide courts with the perpetrators’ personal data. In July 2016, the Austrian government decided on an initiative on ending cyber violence (“Initiative gegen Hass im Netz”). The planned measures include, among other things, guidelines and information on the handling of hate postings (including the possibility for compensation under the Austrian Media Act), the instalment of counselling centres with a special focus on cyber violence, the provision of un-bureaucratic possibilities of reporting cyber violence, as well as sensitization and further training of police officers, judges and state prosecutors. In September 2017 the first counselling centre, focusing specifically on cyber violence was opened in Vienna. The counselling centre will help with questions regarding hate postings, cyber mobbing and other forms of cyber violence. The new, state-funded counselling centre can be contacted by phone, via e-mail, chat or an online form, available at the centre’s website. The centre is able to make an initial assessment of the content and can give legal advice to the victims. The centre is run by the NGO ZARA, an organisation that works on combatting racism and promoting civil courage as well as a positive approach to cultural diversity.

While the Austrian law certainly provides an important resource in combatting online VAWG, its implementation is oftentimes lacking: The law isn’t very well-known to the general public. This results in many women not even being aware of the fact that they are protected by it. There is a lack of adequate training of police officers, judges and public prosecutors. Women reporting cases of cyber violence are oftentimes met with insensitive/not specially trained professionals. Counselling centres for women and girls face similar problems: Many social workers lack knowledge in regards to cyber violence (due to a lack of funding for trainings etc.). The implementation of the law is quite complicated; trials can take years – sometimes ending without a positive result for victims of cyber violence. It might take years before the offensive content is deleted.

In Italy, cyberbullying against minors is now illegal. Companies can be prosecuted if they don’t take down content at child or parent’s request.

In France, sextortion is punished since 2014 as a criminal offense with article 222-33-2-2 of the Penal Code.

- Chapter I (Article 1) of the law to strengthen the fight against the prostitution system and accompany the victims of prostitution (Law No. 2016-444 of 13 April 2016) deals with the means of investigation and prosecution of perpetrators of trafficking in human beings and procurement. Article 1 aims at strengthening the fight against networks that use the Internet to organize their activity, proposing, on the one hand, that Internet service providers (ISPs) and web hosts contribute to the fight against the dissemination of offenses involving trafficking in human beings, pimping and related offenses and, on the other hand, that ISPs prevent, at the request of the administrative authority, public access to Internet sites hosted abroad whose content contravenes French legislation.

- In 2016, the Law for a Digital Republic (Loi pour une République Numérique) was adopted and an amendment targets image based sexual abuse (revenge porn): “Words or images of a sexual nature taken in a public or private place”. The penalty incurred is two years of imprisonment and a € 60,000 fine.

- The reporting platform PHAROS, allows citizens to report on abuse suffered online. Reports are processed by police and gendarmes assigned to the platform. If the reported content or behaviour is breaking the law, the report is referred to an investigation service of the National Police, the Gendarmerie Nationale, the

---

Customs or the General Directorate for Competition, Consumer Affairs and Fraud Prevention. A criminal investigation may be initiated, under the authority of a Public Prosecutor. If the reported content is illegal but designed abroad, it is forwarded to Interpol, which directs it to the judicial authorities of the country concerned.

In Germany\(^{108}\), image-based sexual abuse (revenge porn) is punished by law after a 2014 decision of the German High Court. Plus, social media giants including Facebook and Twitter face fines of up to $53 million if they don’t put more effort in removing hate speech from their platforms\(^{109}\). Germany adopted this year a new law on social media (Netzdiffusionsschutzgesetz, known in Germany as NetzDG) which can be used to tackle cases of online violence against women and girls: insults, threats, threats with violence, taking pictures in personal living area, etc. The platform has to erase postings within 24 hours. While the law seems to provide for more protection on the internet, it has been analysed as contradicting the EU laws, especially the EU e-commerce directive which are more liberal.\(^{110}\)

In Poland, cyberstalking is punished by Criminal Code, Article 190 a §1 on stalking since 2011\(^{111}\).

In Czech Republic, the criminal code recognizes cyberstalking and cyber harassment\(^{112}\).

In the Netherlands, “grooming” is punished by article 248e of the Penal Code since 2010, following the Lanzarote Convention.

In the UK, in April 2015 it became a criminal offence with maximum two-years imprisonment to share private sexual photographs or videos without the subject’s consent providing the intent of causing distress to those targeted. In September 2016 it was announced that more than 200 people had been prosecuted since the law came into effect.

In Croatia, hate speech is identified as a crime in criminal law. However, it is not used to stop online violence against women and girls, and is used for political reasons by the government.

In Finland, pieces of existing legislation can be used for combatting online violence such as the legislation on stalking, sexual harassment, spreading information that violates privacy, defamation, identity theft. But specific laws relating to any for online violence do not exist.

---


\(^{109}\) Melissa Eddy and Mark Scott, New York Times, “Facebook and Twitter could face fines in Germany over hate speech posts”, march 14, 2017, available online at http://nyti.ms/2lWXwX6


\(^{111}\) EIGE, Legal Definitions in EU Member States, Poland - Stalking, available online at http://bit.ly/2zBUo66

5. European Women’s Lobby Recommendations and Demands

Digitalisation impacts on the whole society, on women and men. The digital sphere should be a space of equality, justice, respect, rule of law, non-discrimination, freedom of expression and safety.

Online threats to women and their rights are serious, pervasive, and deserving of the same attention as other forms of violence. Participation free of harassment, exclusion, and marginalization is crucial to integrated social change movements in which women feel they can participate - and lead.

Let’s stand in defence of women’s rights, their psychological bandwidth, and their freedom to live online!

Recommendations on ending violence against women

According to the due diligence principle and the international human rights law\(^{113}\), it is a state’s obligation to eliminate all forms of violence against women and girls, online and offline. Such obligation should translate into addressing: prevention, protection, prosecution, punishment, provision of redress and reparation.

In its answer to MEP Matera, the EU Commissioner for gender equality Ms Jourova states that “the Commission recognises cyberviolence as a form of gender-based violence, which it is committed to eliminating as part of its work to promote gender equality in the EU”\(^{114}\).

- **Policy responses should be formulated in recognition of the fact that cyber VAWG is a form of violence against women.** Strategies for addressing cyber VAWG must also include the voices of women who are victims of the phenomenon.
- The EU and the Member States should aim towards agreeing on *definitions of forms of cyber VAWG* and incorporate these forms of violence into EU and national legislation, to ensure that victims of cyber VAWG in Member States have access to justice and specialised support services.
- The EU and its Member States should put their efforts in *designing legal instruments and policy strategies to punish and prevent Online VAWG and protect its victims*, through legal provisions, law enforcement mechanisms, awareness raising campaigns and the diffusion of reporting and self-protection tools.
- The EU institutions should work towards a *Directive* that specifically addresses Violence Against Women and Girls including online violence. The EU institutions shall make sure victims of online violence are protected by all the rights of the Victims’ Rights directive.
- The EU and its member states should *ratify and implement the Council of Europe Convention on preventing and combating violence against women and domestic violence, the Istanbul Convention*\(^{115}\).
- The EU should establish an EU coordinator to end violence against women and girls, within the umbrella of the EU’s work on equality between women and men.
- A priority should be to *improve gender-disaggregated data* at EU and national level on the prevalence and harms of cyber VAWG (including in fields where there lacks a gender perspective, such as Cybercrime and Media), with information on the sex/gender of the victim and the perpetrator and the relationship between them, and to develop indicators to measure the effectiveness of interventions.
- **Specific and trained support lines and services** should be created and funded in a sustainable way in order to support, help and protect women and girls victims of online violence. Whether managed by

---


\(^{115}\) [https://www.coe.int/en/web/portal/home](https://www.coe.int/en/web/portal/home)
govermental services or women’s organisations, they should ensure a deep understanding of the continuum of violence against women and girls.

- **There should be systematic consultation of and sustainable funding** for women’s organisations providing support to women and girls victims, and developing advocacy and awareness raising campaigns, at EU, national and local levels.

### Recommendations to end online violence against women and girls

- **All forms of online violence against women and girls should be criminalized.**
- The provisions of the Council of Europe Convention on preventing and combating violence against women and girls and domestic violence, the Istanbul Convention should apply to cases of **cyberviolence**.
- **The police and justice systems and professionals should be trained** to detect, respond and prosecute such violence.
- The State is responsible to set up an **independent entity** that is authorized to hear and decide on cases involving online violence against women and issue effective remedies for the victim/survivor.
- Both **perpetrators and re-transmitters** should be held responsible for the re-transmission of violating materials.
- States should also set out clearly the expectation that all business enterprises domiciled in their territory and/or jurisdiction protect, **respect and remedy human rights throughout their operations**.
- **Internet intermediaries** should ensure that their platforms are not abused to perpetrate and perpetuate violence against women, and if they are, take immediate action to remedy it. Moderation should have clear guidelines to exclude sexism and racism, and ensure respect for women’s rights.

### Other EU policies dealing with the digital world

While the digital world is addressed or concerned by several areas of policy, there is almost always a systematic lack of gender perspective, including in policies addressing children’s rights. Gender mainstreaming should be systematic in all policies at EU and national level, to ensure that the realities faced by women online and offline are taken into account and that their human rights are protected and promoted.

- The EU should adopt a directive prohibiting sexism and gender inequality in the fields of education and the media, **extending the Equal Treatment Directive**.
- In the immediate future, definitions of cybercrime by the European Commission’s DG Migration and Home Affairs should include forms of **cyber VAWG**, or at the minimum, should include misogyny in the third part of its definition.
- Training on cyber VAWG with a gender perspective should be introduced to **police responses to cybercrime**.
- It is important for EU level institutions and agencies combatting cybercrime to tackle gendered forms of cybercrime; particularly the online luring or ‘recruitment’ of women and girls into harmful situations such as trafficking.
- Prevention measures should be developed that include the **ICT sector**, including adoption of self-regulatory standards to avoid harmful gender stereotyping and the spreading of degrading images of women, or imagery that associates sex with violence.
- The EU institutions should implement a **systematic gender perspective** (gender mainstreaming, including gender budgeting) in the following EU policies and programmes: EU Digital Agenda, Digital Single Market Strategy, Safer Internet Programme, European Safer Internet Centres, EU Cybersecurity Strategy,
Europol Cybercrime Centre, EU Directive on child pornography and sexual exploitation\(^\text{116}\), as well as all policies dealing with trade, competition, ICT and development.

- The **European Code of Good Practices for Women in ICT** should be vitalised, implemented, and completed to include online VAWG and eliminate it\(^\text{117}\).

### Recommendations towards tech companies and internet providers

- All segments of the internet industry, including internet intermediaries and platform providers, **should respect and protect human rights**.
- Tech companies should **recognise online VAWG** and better cooperate with existing law enforcement instruments.
- They should put additional efforts in fully implementing the **EC code of conduct**.
- They should contribute to **producing data** on online VAWG and proof due diligence in responding to it.

### Recommendations regarding Media and Advertisement

- **Annual media barometers** shall be developed, with goals, targets and indicators, based on consistent and comparable data that give tangible proof of the participation of women in the media in terms of recruitment, content, perspective etc.
- It shall be insured that **goals include targets and indicators** on participation in management and decision-making, the working conditions; such as gender equal wages and mechanisms to prevent sexual harassment and other forms of discrimination.
- Policy and law makers shall review how female journalists, elected officials, researchers and culture workers can be offered **improved legal protection**, especially when targeted by organized hate campaigns.
- Public media distributors shall be given the task to **ensure gender equality** by implementing a model for participation and non-stereotypical representation that can also be used by private media actors.
- **Legislative measures shall be implemented against sexist advertising** as well as an obligation for the advertising industry to provide information on any retouching of images.
- Evidence-based research and Civil Society Organization Programs on gender equality in media shall be **supported and funded**.
- **Mandatory gender training** shall be included in programs and courses for journalists.
- **Education on media and ITC literacy** shall be part of the schools curricula. Education should include gender equality awareness and an understanding how gender stereotyping has a negative impact on the achievement of gender equality overall. When people are trained to critically evaluate, use, consume and produce media information, they are empowered to participate effectively in the public debate.

### Recommendations regarding pornography

- **Pornography should be recognised as a form of male violence against women and girls**\(^\text{118}\).
- All internet providers shall install Opt-in filters that block pornographic material as standard. Consumers who want to access pornographic material should actively have to choose to remove the filter (Opt-out).
- Ensure porn-free school environments for children.
- Legislators shall review what measures can limit the distribution of online pornography.

---


\(^{118}\) See EWL position paper “Towards a Europe free from all forms of male violence against women and girls” [https://www.womenlobby.org/Towards-a-Europe-Free-from-All-Forms-of-Male-Violence-against-Women-December](https://www.womenlobby.org/Towards-a-Europe-Free-from-All-Forms-of-Male-Violence-against-Women-December)
We also share here the demands of the Joint statement on Facebook internal guidelines for content moderation\textsuperscript{119}:

1. Provide greater transparency and accountability regarding the following:
   - The implementation of content moderation guidelines;
   - The rejection of reports of online abuse and disaggregated data on reports received;
   - The departments and staff responsible for responding to content and privacy complaints.

2. Provide additional training for moderators that addresses cultural and language barriers, power dynamics, and issues such as gender bias and LGBTQ sensitivity.

3. Hire more speakers of languages that are currently under-represented among content moderators.

4. Improve the reporting mechanism so that it meets the following criteria:
   - Legitimacy: the mechanism is viewed as trustworthy and is accountable to those who use it;
   - Accessibility: the mechanism is easily located, used and understood;
   - Predictability: there is a clear and open procedure with indicative time frames, clarity of process and means of monitoring implementation.
   - Equitable: it provides sufficient information and advice to enable individuals to engage with the mechanism on a fair and informed basis;
   - Transparent: individuals are kept informed about the progress of their matter;
   - Rights-respecting: the outcomes and remedies accord with internationally recognised human rights;
   - Source of continuous learning: the mechanism enables the platform to draw on experiences to identify improvements for the mechanism and to prevent future grievances.

5. Increase diversity at all staff levels and adopt the Women’s Empowerment Principles\textsuperscript{120}.

\textsuperscript{119} Take back the Tech and other signatories, “Joint statement on Facebook’s internal guidelines for content moderation”, available online at https://www.takebackthetech.net/news/joint-statement-facebooks-internal-guidelines-content-moderation

\textsuperscript{120} Women’s Empowerment Principles, available online at http://www.wesprinciples.org
Bibliography

EU documents

Resolutions

European Parliament resolution of 3 September 2008 on how marketing and advertising affect equality between women and men, available online at

European Parliament resolution of 24 November 2016 on the EU accession to the Istanbul Convention on preventing and combating violence against women

European Parliament resolution of 12 March 2013 on eliminating gender stereotypes in the EU, available online at European Parliament resolution of 12 March 2013 on eliminating gender stereotypes in the EU


European Parliament resolution of 28 April 2016 on gender equality and empowering women in the digital age, available online at European Parliament resolution of 28 April 2016 on gender equality and empowering women in the digital age

European Parliament resolution of 24 November 2016 on the EU accession to the Istanbul Convention on preventing and combating violence against women, available online at

European Parliament resolution of 24 November 2016 on the EU accession to the Istanbul Convention on preventing and combating violence against women

European Parliament resolution of 13 December 2016 on the situation of fundamental rights in the European Union in 2015, available online at

European Parliament resolution of 13 December 2016 on the situation of fundamental rights in the European Union in 2015

Directives


Questions

Reports


Press releases


Reports & legal texts


Bartlett, Jamie., and Norrie, Richard and Patel, Sofia., and Rumpel, Rebekka., and Wibberley Simon., Demos, “Misogyny on Twitter”, May 2014, available online at https://www.demos.co.uk/files/MISOGYNY_ON_TWITTER.pdf


Council of Europe, “CoE Factsheet Hate Speech”, 2017, available online at http://www.echr.coe.int/Documents/FS_Hate_speech_ENG.pdf


EIGE, Legal Definitions in EU Member States, Poland - Stalking, available online at http://bit.ly/2zBUo66


Laxton, Claire., Women’s Aid, Virtual World, Real Fear, Women’s Aid report into online abuse, harassment and stalking, 2014, available online at http://bit.ly/2h0W4OX


Books

Buchwald, Emilie., and Fletcher, Pamela R., and Roth, Martha., Transforming a Rape Culture, Milkweed Editions, Minneapolis, 2005 (1993)

Jane, Emma., Misogyny online, a short (and brutish) history, Sage Swifts, 2017


Academic articles & papers
Baker, Daizchane., "Online Sex Slaves: The Internet’s Powerful Role in Sex Trafficking", Senior Honors Theses. 464, 2016, available online at http://commons.emich.edu/honors/464

Beeche, Karina., “The sexual marketing of eastern european women through internet pornography” College of Liberal Arts & Social Sciences Theses and Dissertations. Paper 33, 2010, available online at http://via.library.depaul.edu/etd/33


https://www.academia.edu/31674403/Media_Framing_of_Trolling_and_Online_Abuse_Silencing_Strategies_Symbolic_Violence_and_Victim_Blaming


Pereira, Filipa., and Matos, Marlene., “Cyberstalking entre adolescentes: uma nova forma de assédio e perseguição?”, Escola de Psicologia, Universidade do Minho, Braga, Portugal, Psic., Saúde & Doenças vol.16 no.1 Lisboa mar. 2015, available online at http://dx.doi.org/10.15309/15psd160207

Ringrose, Jessica., UCL Institute of Education, project: “Documenting digital feminist activism: mapping feminist responses to new media misogyny and rape culture.”, available online at http://www.digitalfeminism.co.uk


Verdejo Espinosa, Maria Angeles., “Ciberacoso y violencia de género en redes sociales, Analisis y herramientas de prevencion”. Universidad Internacional de Andalucia, available online at http://dspace.unia.es/handle/10334/3528

Press articles


Citron, Danielle., The Guardian, Op-Ed, We will look back at cyber-harassment as a disgrace – if we act now, April 15,2016, available online at https://www.theguardian.com/commentisfree/2016/apr/15/cyber-harassment-cyberbullying-revenge-porn-education-laws


Eddy, Melissa., and Scott, Mark., New York Times, "Facebook and Twitter could face fines in Germany over hate speech posts", march 14, 2017, available online at http://nyti.ms/2lWXwX6


Laville, Sandra., Wong, Julia Carrie., and Hunt, Elle., “The women abandoned to their online abusers”, April 11, 2016, available online at https://www.theguardian.com/technology/2016/apr/11/women-online-abuse-threat-racist


Mead, Rebecca., The New Yorker, The Troll Slayer, A Cambridge classicist takes on her sexist detractors, September 1, 2014, available online at https://www.newyorker.com/magazine/2014/09/01/troll-slayer


Saul, Heather., Rolling Stone, “Grimes on music industry sexism”, April 15, 2016, available online at http://ind.pn/22zSPfn


Website posts & blogs


Erika and Fungai, GenderIT, “Did Facebook Finally Figure Out That Consent is More Important than Nipples?”, May 3, 2017, available online at http://www.genderit.org/articles/facebook-intimate-image-filter


Internet Signalement, available online at http://bit.ly/2qTfwx3

ItsAllMaya, Gender IT/TacticalTech, The Architectures of Online Harassment (Part 1), February 2017 available online at http://www.genderit.org/feminist-talk/architectures-online-harassment-part-1

Marshall University, Women’s Center, “What is Rape Culture”, available online at http://www.marshall.edu/wcenter/sexual-assault/rape-culture/

NNEDV, Safety Net, available online at https://nnedv.org/content/safety-net/

SafetyNed, available online at http://safetyned.org/


Take back the Tech and other signatories, “Joint statement on Facebook’s internal guidelines for content moderation”, available online at https://www.takebackthetech.net/news/joint-statement-facebooks-internal-guidelines-content-moderation
Women’s Empowerment Principles, available online at [http://www.weprinciples.org](http://www.weprinciples.org)


Women Media Center, “WMC Speech Project, Online Abuse 101”, available online at [http://www.womensmediacenter.com/speech-project/online-abuse-101#mobAttacksCybermobs](http://www.womensmediacenter.com/speech-project/online-abuse-101#mobAttacksCybermobs)
New technologies and digital platforms are also tools for empowerment and are used by women and girls to deploy strategies of resistance and solidarity. Despite the dire consequences described, there is evidence that instead of pushing women out of activism, online VAWG has galvanized women’s advocates. A multitude of responses to violence have emerged, from intergovernmental initiatives like the UN Broadband Commission to informal online networks aimed at giving women the tools they need to be active, visible members of the online community.

Below are examples of support services, campaigns, organisations, social enterprises, programs and projects from all over the European continent, targeting online VAWG. We have chosen to highlight a vast majority of the initiatives we found. However, despite our wish for exhaustivity, we have not been able to explore all the projects, initiatives and campaigns developed at country level, especially those developed in national languages.

**Governmental support services**

- **Better Internet for Kids**
  The European Commission’s Digital Single Market Strategy aims to make every European digital. Its prevention facet encourages self-regulation by the industry. An important part of the programme are the Safer Internet Centres, present in 30 European countries. They give advice and information to children, parents and teachers and serve as hotline to receive reports on online illegal content. The Centres also organise youth panels that are consulted regarding online safety issues and in order to design information material.

- **UK Revenge Porn Helpline**
  Is a government-funded, free of charge phone service to help women who are victims of image based sexual abuse.

- **Child Focus, Belgium**
  This Belgian organisation has created a simple question and answer type Internet platform for children, teenagers, parents and professionals about the opportunities and dangers of the Internet.

- **CEOP**, UK
  Is the British police platform for the digital security of minors.

- **Frauen* beraten Frauen* (Women counselling Women), Austria**
  Founded in 1981 as the first Viennese Women’s Counselling Centre, the offers of ‘Women Counselling Women’ include (among many others) web-based online-counselling via e-Mail and a chat forum.

**Campaigns (governmental and NGOs)**

- **No hate speech movement by the Council of Europe**
  Hate Speech Watch is a user-generated platform used to trace, share and discuss online hate speech contents.

---

121 [https://www.betterinternetforkids.eu](https://www.betterinternetforkids.eu)
122 [https://revengepornhelpline.org.uk](https://revengepornhelpline.org.uk)
124 [https://ceop.police.uk/safety-centre/](https://ceop.police.uk/safety-centre/)
125 [http://www.frauenberatenfrauen.at](http://www.frauenberatenfrauen.at)
126 [https://www.nohatespeechmovement.org](https://www.nohatespeechmovement.org)
Women European Coalition against media sexism (WECAMS)\(^{127}\), Europe wide
WECAMS is a coalition of three European women's organisations set up with the specific aim of bringing an end to sexism in the media and in advertising: **DonneinQuota** in Italy, **Object** in the UK and **Les Chiennes de garde** in France. All three groups campaign against sexist, objectifying and dehumanising representations of women in their respective countries. This coalition has been established to work together in tackling sexist representations of women at the European level and, in doing so, encouraging governments to take decisive action so that they adopt legislation regarding the portrayal of women in the media or in advertising. The Coalition launched a petition calling on the EU to strengthen its laws against sexism in the media.

Recl@im the Internet\(^{128}\), UK
Recl@im the Internet is a UK-based broad campaign for action to challenge online abuse. The campaign draws inspiration from the “Reclaim the Night” marches of the 1979s and 80s when women were warned not to go out after dark because they wouldn't be safe from harassment, abuse or violence. Instead women took to the streets together to demand change.

Stop cybersexisme, Centre Hubertine-Auclert pour l'égalité femmes-hommes\(^{129}\), France
This Paris-based center fighting against gender inequalities led the first large-scale study on cybersexism in France and produced a pedagogical kit. It defines cybersexism as: “acts of violence deployed on the Internet and social networks via insults, harassment, humiliation, rumors and that are defined by their intention to reduce girls to their physical appearance. They aim to control their sexuality and to overvalue virility and men's sexuality”.

#GegenHassImNetz, Austria
In 2016, the Secretary of State for Diversity, Public Service and Digitization, Muna Duzdar launched the campaign #GegenHassImNetz as to respond to the increasing number of hate and hate postings on the Internet. In September 2017 the Ministry of Women’s Affairs, together with the Secretariat of State for Diversity, Public Service and Digitization launched a new campaign focused specifically on cyberviolence against women. Its main focus lies on educating professionals who work with victims of cyber violence. The ministry will fund a research project to collect comprehensive data on cyberviolence against women. The aim of the study is to develop a method box with guidelines and background knowledge for women's counseling centres. Starting at the beginning of 2018, seminars and workshops will be held for consultants working in women's counseling centres.

Osez le féminisme ! (OLF) - Stop agresseurs en ligne\(^{130}\), France
This campaign to raise awareness on image based sexual abuse (revenge porn) also seeks to reframe this violence in clearer terms. "'Revenge porn' is a euphemism that understates its gravity. It is more adapted to designate this violence as a cyber rape, a sexual assault via the distribution of intimate sexual images, or a pornographic predation." While a law against cyber rape exists in France, it is not used often enough, writes OLF.

KlickSafe.de\(^{131}\), Germany
Klicksafe is an awareness campaign promoting media literacy and adequate handling of the internet and new media.

---

127 [https://wecams.wordpress.com](https://wecams.wordpress.com)
128 [http://www.reclaimtheinternet.com/about](http://www.reclaimtheinternet.com/about)
129 [https://www.stop-cybersexisme.com](https://www.stop-cybersexisme.com)
130 [http://stopagresseursenligne.olf.site/](http://stopagresseursenligne.olf.site/)
• CyberVAW\textsuperscript{132}, Slovenia
From July 2017 on, Slovenia will launch the project ‘CYBERVAW’, which aims at developing awareness-raising and education activities that spread a clear message of zero tolerance to VAWG, with a specific focus on prevention of gender-based cyber violence and harassment as a form of VAWG.

Organizations
• Stop violencia de genero digital (\textit{Stop gender-based violence online})\textsuperscript{133}
This Spanish organization provides support to women who experience gender-based violence on the internet, primarily from partners or ex-partners. Its experts include lawyers, computer specialists and psychologists. Its services range from establishing proof of harassment or stalking and detailing it in a preliminary report for the judicial authorities, to teaching women how to best protect themselves from their aggressors. Because some women’s professional insertion may have suffered from their online experiences, the association also helps women get back into the job market.

• Take Back the Tech\textsuperscript{134}
Inspired by « Take Back the Night » movements, Take Back the Tech « is about creating digital spaces that protect everyone’s right to participate freely and equally without harassment or threats to safety ». Launched by the Association for Progressive Communications in 2006, Take Back the Tech campaigns about and maps online VAWG in 25 countries worldwide. Bosnia-Herzegovina’s Take Back the Tech, for instance, has simultaneously networked with various women’s organizations in the region and launched a bootcamp: WomenRockIT\textsuperscript{135}, where young women learned about digital security, shared stories and knowledge, reinforcing their determination to be powerful voices on the Internet\textsuperscript{136}.

• Féministes contre le Cyberharcèlement (Feminists against Cyber Harassment)\textsuperscript{137}
A French network working to raise awareness on VAWG online. Their infographic\textsuperscript{138} on the Iceberg of cyberVAWG has been widely shared.

Programs, Projects and Research
• SRHR and the Internet\textsuperscript{139}. A project by Tactical Tech, Sexuality, Sexual and Reproductive Health and Rights, and the Internet, wished to explore the corporatisation of the internet, collusion between governments and technology companies, censorship, violations of privacy, sexism, and violence, amongst others.

• How can tech help address domestic abuse?\textsuperscript{140} A collaborative research study about the use of digital tools to support people affected by domestic abuse, led between 2016 and 2017 by four organisations working together to find out what role digital technologies can play in helping to support people affected by domestic abuse.

• SafetyNed\textsuperscript{141} is a Dutch national platform launched by a coalition of four women’s shelters on the model of the American SafetyNet\textsuperscript{142} program from NNEDV. SafetyNed claims the right to be safe online for every

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{132} http://bit.ly/2gTbQv4
\item \textsuperscript{133} http://www.stopviolenciadegenerodigital.com
\item \textsuperscript{134} https://www.takebackthetech.net
\item \textsuperscript{135} http://www.genderit.org/node/4832/
\item \textsuperscript{136} https://www.apc.org/en/project/take-back-tech
\item \textsuperscript{137} https://feministesvscyberh.tumblr.com
\item \textsuperscript{138} https://feministesvscyberh.tumblr.com/image/159448703445
\item \textsuperscript{139} https://tacticaltech.org/projects/sexual-and-reproductive-health-and-rights-and-internet
\item \textsuperscript{140} https://www.techvsabuse.info
\item \textsuperscript{141} http://safetyned.org/
\item \textsuperscript{142} http://nnedv.org/projects/safetynet.html
\end{itemize}
\end{footnotesize}
victim of domestic violence. Its objective is to equip both women victims of domestic violence and those caring for them with (self-)protection tools on digital platforms and with new technologies.

- **Digital Feminism**[^143] is a research project which aims were to map, explore and analyze how girls and women use digital media platforms to document experiences of rape culture, harassment, and misogyny. The research team also wanted to understand the experiences of girls and women who participate in this activism and to document these feminist activist practices and experiences through the creation of a living archive of contemporary digital feminist activism.

### Social enterprises

- **Avassa**[^144]
  Avassa is an app and connected ring soon to be released that aims at enhancing women and girls’ sense of safety. When pressed, Avassa’s smart device instantly alerts one’s chosen contacts and community in the event of danger. The application can also connect to local authorities for emergency assistance.

- **Codeworks**[^145]
  In order to combat the gender gap in the tech sector, coding schools like Codeworks Barcelona have implemented affirmative action such as offering a 10% discount to women in order to tackle the unbalance both in applications and in recruitment. They wish to battle the lack of female role models in the Tech sector, especially in Europe.

- **WI-Filles**[^146]
  In France, the organization WI-Filles trains young women and girls from disadvantaged areas to coding and ICT skills. 75% of girls decide to change career after the trainings.

Moreover, adequately contextual resilience and mitigation strategies are emerging, often led with a multi angle and intersectional perspective. Below are listed programs, projects and collective initiatives classified by type of online VAWG:

### Initiatives by type of online VAWG

#### Trolling - Cyberbullying - Online harassment and threats

- **Payeton troll**[^147] Eloïse Bouton, a public feminist figure in France, started a witty and political Tumblr dedicated to trolls. Her website’s name “Paye ton troll” means roughly “Bring on the trolls” and its by-line specifies: “Feminists accounts of unpunished cyber harassment”.

- **Hatr.org**[^148] German feminists have decided to make money off of trolls. Their website is a compendium of sexist, homophobic, racist (and other hate-inspired) comments. It seeks to both empower women by showing the sheer absurdity of these comments, but also to raise money for feminist causes via advertising’s user-generated income.

- **HeartMob**[^149] is a platform that provides real-time support to individuals experiencing online harassment. With reporting and urgent action and support tools, this initiative builds on a community of helpers.

[^143]: [http://www.digitalfeminism.co.uk/](http://www.digitalfeminism.co.uk/)
[^144]: [http://avassa.com](http://avassa.com)
[^145]: [https://codeworks.me](https://codeworks.me)
[^146]: [http://wifilles.org](http://wifilles.org)
[^147]: [https://payeton troll.tumblr.com](https://payeton troll.tumblr.com)
[^148]: [http://hatr.org](http://hatr.org)
[^149]: [https://iheartmob.org](https://iheartmob.org)
• CrashOverride\textsuperscript{150} Founded by two survivors of online violence, one of them Zoe Quinn, a gamer and video game creator, and main target of the famous Gamergate, Crash Override Network is an online abuse hotline and a toolbox for victims of online violence.

• Blocking lists on Twitter and/or the App “Blocktogether”\textsuperscript{151} Block Together is designed to reduce the burden of blocking when many accounts are attacking a person, or when a few accounts are attacking many people in a user’s community.

• Trollbusters\textsuperscript{152} TrollBusters provides rescue services to support women journalists, bloggers and publishers who are targets of cyber harassment. They have an S.O.S. team who sends positive memes, endorsements and testimonials into online feeds at the point of attack.

General DIY digital security guidelines

• #Digilantism\textsuperscript{153} The term, coined by Australian researcher Emma A. Jane, describes the way in which some women have chosen to take the law in their hands, using “name and shame” and various mob tactics to « take down » online abusers.

• Surf Smart initiative aimed at Girls Guides and Girls Scouts led by WAGGGS\textsuperscript{154}

• DIY digital security toolkit by SafeHub Collective\textsuperscript{155}

• DIY online harassment protection kit by Feminist Frequency

• Toolkit designed by Chayn\textsuperscript{156}

• Cyber hate quiz designed by Stop Cyber Hate Belgium\textsuperscript{157}

Doxing - spoofing accounts and fake identities

• Zen Manual\textsuperscript{158} The Zen Manual is Tactical Tech’s exhaustive guidebook on digital safety and managing identities online. It equips the user with knowledge and tools on how to stay safe and control one’s data online.

• MyShadow\textsuperscript{159} My Shadow project has the objective to help the user control their data traces, understand how one’s being tracked, and learn more about the data industry.

Cyber Stalking

• Online safety manual (Feminist Frequency)\textsuperscript{160} The guide, initiated by Anita Sarkeesian, the director of Feminist Frequency, Jaclyn Friedman, anti-rape activist and founder of Women, Action & the Media (WAM!) and Renee Bracey Sherman, reproductive justice activist and author of Saying Abortion Aloud. This guide is designed for people who may be

\textsuperscript{150}http://www.crashoverridenetwork.com
\textsuperscript{151}https://twitter.com/blocktogether
\textsuperscript{152}http://www.troll-busters.com
\textsuperscript{154}https://www.wagggs.org/en/what-we-do/surf-smart/
\textsuperscript{155}https://hackblossom.org/cybersecurity/
\textsuperscript{156}http://chayn.co/safety/
\textsuperscript{157}http://www.stopcyberhate.be/quiz-fr/
\textsuperscript{158}https://gendersec.tacticaltech.org/wiki/index.php/Complete_manual
\textsuperscript{159}https://myshadow.org/about
\textsuperscript{160}https://feministfrequency.com/2015/12/08/speak-up-stay-safer-a-guide-to-protecting-yourself-from-online-harassment/
experiencing fear or trauma. It details best security practices for social media, email, online gaming, website platforms, and ensuring privacy of personal information online, as well as the documentation and reporting of harassment, and caring for oneself emotionally during an online attack.

Informal networks on the web

Facebook groups, Twitter hashtags and fluid solidarity. These networks are in part hidden from public view, because of the threat of online violence. They can however become very powerful relays when a member of the feminist community online falls prey to online aggression.
Here below are listed the outputs of the October 13th, 2017 Online Conference

- The video recording of the Online Conference Online Conference - #HerNetHerRights - October 13th 2017
- The conference's storify Storify - #HerNetHerRights
- The collection of speakers’ presentations

Here below is the collection of the speakers’ presentations at the Online Conference. These are not a publication of articles, but more of a digest of the content of the conference.

Emma Holten’s presentation

Living as a victim – My story, the consequences

As big issue for many victims of revenge porn or non-consensual pornography, is the difficulty they experience in detailing the type of suffering they are enduring. For many, the immediate association is a source of sexual shame, but that is not necessarily the dominant experience for victims, although it of course plays a big part.

Rather, what seems to come up again and again as I speak to people who have experienced this, what they are saying is similar to the sense that I felt myself: a sense of unsafety, coupled with a sense of powerlessness over your own life narrative.

It is very important to understand that the goal of violators is to hijack a victim’s identity. The content of the pictures does not matter much, the thing that matters is that they possess the sense of violation and pain.

Only through this violation and pain can the power over the victim be exerted. This power takes many different forms, from very concrete (blackmail, harassment), to much more subtle (introducing the violation into public conversations and speaking of the victim as if they were worth less in social settings). The goal of violators and the people propping up the violation is to plant in the victim a constant sense of unease. Of not knowing when the next violation will occur.

Another aspect of this crime that seems to not come up much, is that of keeping the violation a secret. Just a LGBTQ people do not ‘come out of the closet’ once, but many times over their lifetime, and are in a constant danger of being ‘outed’, non-consensual pornography victims live a life of constant assessment and vigilance. How will I be treated now? Do these people know? Will they respect me? Are they ridiculing me? A sense of paranoia and of not wanting to leave the house is extremely common. Every day is a measuring up of the risks vs. the gains of associating with other people. Applying for jobs, going on dates, attending parties, is of course a minefield (more so in more conservative societies, but the structure remains the same).

Conclusively, sexual violations online are an attack on your identity. It is a way for other people to take control of your life. This attempt is rarely co-ordinated, but becomes an organising structure through which the victim must navigate at all times. Deciding what your name, life, and self should connote is a right that is taken away from us.

– Intentions and violators

While the above is a fair place to start in terms of understanding the day-to-day lives of survivors, it does not even begin to give us an understanding of perpetrators. Through my work, I have the odd privilege of meeting every day the young men and women who participate in the sexual humiliation of others. The conversations around revenge porn have thus far been heavily – and rightly! - focussed on the initial sharer of material. The wronged ex-spouse as well as the serial offender who violates for profit are the most salient in literature. However, these are not the people who prop up this crime. It is the sharers who do not know the victim, nor gain anything material or economical from their victimization. It is people who humiliate for entertainment. I suspect that the reason these people have been excluded from the conversation is that their motives are much harder to talk about.
Misogyny just simply does not cut it. Because while many of the people who harass the victim directly are men, when these things happen in high schools and institutions of higher education, many participants are women.

Rather, I think we must look closer at the culture of “humiliation-cum-entertainment”. Because while the initial breach of privacy might share traits with rape or assault, the further violations much more take on the nature of reality show. People revel in the humiliation of others to raise up themselves. Gathering around in what seems like a schoolyard for the whole world, the lowest common denominator - that of ganging up on the weak and vulnerable - takes over. The young people that I speak with, who have contributed with comments or further ridicule, do not (not even close!) see themselves as sexual violators. They do know, though, that the behaviour is not commendable, when asked. Just as we all know that laughing at a fat person, a handicapped person, an ugly person, an unskilled or stupid person is not commendable. Yet, millions of people everywhere do it, and do not consider themselves bad or evil for that reason.

- My activism

The work that I have done upon getting this information is towards radically humanizing victims. In order to violate and humiliate a person, I am of the understanding that you must first dehumanize them. This process is of course much easier when it comes to historically and currently oppressed groups such as women, LGBTQ and minority persons. While I have serious doubts we will ever fully stop the initial spread, spreading awareness about one’s responsibility towards people one does not know seems to me key in this work. My project CONSENT attempted to, by casting me as an actor with agency, underscore my right to choice in what happens to my body and how it is portrayed publicly. By far, the strongest response has been that of surprise: that revenge porn victims even have feelings, even have basic humanity, seems to strike many as a surprise. The response “She was stupid to take naked pictures”, is to me only an attempt to alleviate one’s own responsibility by not granting the victim basic human rights. Thus, one does not have to look at them as one sees oneself. Full. A human. But this dehumanization can not be isolated. It must be seen in the bigger context of a society where the ridicule of regular people is the most popular form of entertainment. Older generations created reality television with the explicit goal of abusing and shaming regular people for fun. Now, young people are doing the same.

Sodfa Daaji’s Presentation

Thank you for inviting me, it is a pleasure to talk about the young women on internet and the Italian experience about cyber violence.

As you can see, internet is giving us the opportunity to gather here and to share our experiences and to hear what happens in the different parts of the world.

Few days ago, as you have probably heard, a woman in Congo was raped publicly by rebels and internet gave us the opportunity to learn that, unfortunately, in some parts of the world women are still the primary victims during conflicts, and targeted by men to show their strength and domination to their enemies.

Internet is the reflex of our society and shows how women are perceived in real life, and how men feel the right to objectify and sexualize women and their bodies. I have really appreciated the intervention of Emma, her personal experience and she highlighted something important: for men, this is an entertainment, and they don’t think about the on-line and off-line implications.

That is why I would like to bring with me the experience of two young women, killed by the web.

The death of Carolina Picchio brought on the table of the institutions the fact that cyber violence is reality, exists, and can’t be treated anymore as a joke. Carolina died at 16 years old, and killed multiple times by those who watched and shared the video uploaded by her rapists. Carolina died suicide and killed multiple times by those who treated her rape as a joke, as something worth to watch, to share and to comment. The episode was followed
by the adoption of a law against any form of cyber violence, included revenge porn, but is applied just to victims that are under age.

The following law could have helped Tiziana Cantone, 29 years old, who was left without under protection and killed by the multiple jokes made by women and men about her private life. A private video of her intimacy was firstly shared on a whatsapp group, and then widespread on facebook and on porn sites. Tiziana killed herself, and is killed by those who are still watching her videos, by those who saved a video of her intimacy, of her private life. Tiziana was killed by those who judged her intimacy, who entered without permission in her private life and felt the right to judge her, to joke at her, to follow here and make her life a complete hell.

The sad part is that internet is a reflection of the society, and is giving to men the opportunity to sexualize us, to virtually rape us and to take our contents without any permission. I was so shocked and outraged when I’ve heard the first time that on Facebook there are secret groups in which strangers gather together and rape virtually women. Those users upload pictures of their female friends, female workers or just strangers and start a virtual rape group, comment after comment. Just imagine how brutal it is to imagine a group of men, comment after comment, stating this such ‘I would do to her this and this and this’.

No matter how many times those groups were closed, because it is that easy to create a new group, to change a name, to create a new profile and to continue what is, for them, a form of entertainment and joke. What is virtual for them, it is reality a violence toward us and a reflection of the male dominant attitude.

Women are everyday covered with sexist comments, and their pictures are stolen without thinking that, as Pierrette said, the fact that by uploading a picture on social medias, does not give them the right and the consent to take it.

The positive said is that Internet is giving to us the opportunity to gather from different parts of Europe and to debate about the issue. And we can take the chance to use internet as the tool to lead our fight against cyber violence. If we want, we can unify our strength and let this be added on the list of fights that we are already doing, as feminists.

Thank you.

Nicole Shephard’s presentation

The feminist implications of big data and privacy

We’ve come quite a long way since they the early days of the big data hype. After initial hyperbolic claims that data will solve all our problems, answer all the questions we never had, and replace theory and the social sciences, a lot of critical work has appeared and toned the narrative down by a few notches. A couple of things are quite clear by now:

- Even the biggest dataset is only ever a sample and never a whole population;
- Who is included in that sample isn’t only geographically specific but also gendered, raced, and classed;
- Data as such is never neutral, objectivity is a very persistent myth (in data as elsewhere), and algorithms don’t emerge from some kind of egalitarian vacuum;
- Technology is embedded in the same kinds of unequal power relations as everything else;
- And (almost) anyone can become a data point in one way or another but only few can collect data on a large scale and an even smaller elite can process and analyse that data.

My worry around contemporary data practices is that the feminist tools we have at our disposal to think about data, about knowledge production and research methods are underused. Here I have in mind things like
intersectionality or reflexivity, but also concepts like situated knowledges, strong objectivity, epistemic violence, or all the feminist work around agency and consent.

On that note, I turn to a couple of somewhat disjointed tensions around the feminist politics of data and privacy in relation to online harassment.

**Feminism & privacy**

Feminism has a fairly complicated relationship with privacy. A great deal of exploitation, violence and coercion takes place in the privacy of the home, which has made it difficult to politicise the personal. That history and decades worth of feminist debate around the public/private divide makes many a feminist cautious, if not reluctant, around the protection of privacy online.

We might productively think of this as a kind of double-bind:

Privacy on the one hand is a privilege that isn’t afforded equally to all. Women, queers, trans people, people of colour, disabled people, poor people, recipients of state benefits, refugees and others – particularly those inhabiting multiple intersections – are groups whose privacy was never considered on an equal level with that of privileged groups.

But turning this argument on its head, we can also think of giving up privacy, of consenting to transparency as a privilege that isn’t distributed equally either. We all have something to hide, of course, but who’s in the best position to reveal as good as everything without having to fear the consequences? Here, again, we’d have to list the most privileged groups, perhaps headed by the figurative heterosexual white cis man.

Instead of engaging in good privacy vs. bad privacy debates – is privacy good for women or is privacy bad for women – we may choose to focus on highlighting these inequalities in access to privacy and on making its protection online more widely accessible.

There is a good feminist argument to be made for the protection of online privacy. Such an argument would, at a bare minimum, reference how marginalised groups are exposed to even more harassment and persecution without privacy. Or that the freedom to creatively experiment with gender, sexuality, and coming to one’s identity more broadly relies on privacy and anonymity. And how, for feminist activists, researchers or journalists, a lack of privacy can lead to exposure and harassment – not only of themselves, but also of the often marginalised people they work with.

**A feminist politics of data**

The politics of data affect a wide range of people, but not all in the same ways. That includes big data and surveillance, questions around privacy and anonymity as well as online harassment and other forms of technology-related violence.

The response to online harassment as a social problem are often calls for more research, bigger data = better data. I too recall complaining that particularly on the European level we don’t have enough data on online harassment, that more research is necessary. While in some ways certainly a reasonable objective, the desire/need for more data also seems at odds with feminist concerns about the complicity of big data in surveillance and control, the epistemic violence that comes with the counting, sorting, and managing of populations, and the struggle against non-consensual and disempowering uses of data.

Is there such a thing as feminist data? I don’t know. But some data practices are definitely more in line with a feminist ethics than others. That includes for example thinking carefully about agency and consent in relation to data. That includes questioning the power relations behind who gets to collect data and who becomes a data point. That includes questioning and critiquing not only the data practices of governments and large corporations, but also our own research and activism with data.
● It’s important to always question what is being left out of the frame.
● Which questions do we ask, and don’t we ask of our data?
● What silences might the missing data reveal?
● Which outliers in the data might reveal discrimination and exclusions?
● But also, who gets to do the definitional work, who decides what counts as harassment in the data and what doesn’t?
● Is our approach intersectional enough to capture the ways in which harassment affects different people differently?

These and similar questions apply to human and algorithmic efforts to stop online harassment by the means of data and technology. But they also refer to our own understanding of online harassment and to our research and efforts to get bigger and better data about online harassment.

A fairly recent large-scale European study, for example, interviewed 42,000 women across all EU countries, published a report of almost 200 pages but failed to mention race even a single time. That still feels symptomatic for the European context. In the small section that dealt with online harassment specifically, it was also quite narrow in what counted as harassment, reduced it to 2-3 items, which meant it reported much lower numbers of women affected by online harassment than other recent studies that operationalised harassment in more nuanced ways, but that’s a different story.

It makes sense, of course, to talk about the online harassment of women and girls. Research shows that they are indeed disproportionately targeted by online abuse. But it is also worth keeping in mind that not all online violence is gender-based. And that, in turn, we can only have a very partial understanding of online violence against women if we neglect the intersections between gender, race, religion or sexuality. Producing data that further conflates online harassment with gender and women is too narrow.

A feminist politics of data has to go further than simply adding women to data or generating more data about women. At a minimum, it should be intersectional enough to capture how race, sexuality, or religion factor into the online harassment of women. But, ideally, it would capture the issue more broadly and work towards data that includes women, men, trans and non-binary people to examine how gendered and sexualised harassment, racist harassment, Islamophobic and anti-Semitic harassment etc., intersect and affect different groups of people differently.

**Feminisms vs. online harassment**

I conclude by highlighting one more tension we encounter in figuring out what to do against online harassment. That is, we need to be a little bit careful what we wish for in two related ways.

First, some methods to eliminate online abusive content and users can be counterproductive. That’s the case when such methods are easily turned against those they are built to protect, or when they almost by definition exclude the more vulnerable groups among our own ranks. Algorithmic filtering and blocking of abusive language to get rid of harassing content, for example, silences resistance and counter-speech that uses similar language, but also simple profanity, slang, and regional differences in what terms are used in what context and so on. Machines are still terrible at filtering nuance, context, meaning, irony, reclaimed or repurposed language.

Or, forcing real-names may curb some forms of harassment, i.e. get rid of some harassers. But it also further silences and excludes those who rely on anonymity for their feminist work, or for their personal safety. Similarly, mechanisms designed to identify and/or report abusers are at risk of being turned against those abused, i.e. “troll” is seldom a self-designation. Body shaming and transphobia under guise of Facebook’s community guidelines about nudity is just one example that comes to mind.
Long story short: no measure, even if it promises an interim solution to some aspect of the problem, is a feminist measure if it also holds the potential to further silence and put at risk women, communities of colour, queers, and other groups who get marginalised online.

And second, when we wish for such “quick fixes”, we delegate a complex social problem that crosses online/offline boundaries, geopolitical contexts, as well as platforms, to companies that are often confined to particular geographical and legal contexts, that are often not particularly diverse or inclusive in their workforce, and that have a somewhat abysmal track record in doing justice to such issues in the past.

Holding platforms accountable for the harassment they enable is reasonable – not least because that’s where the potential lies for measures to reduce harm by design and for giving users some agency over what content and other users they engage with in what ways. But we also need to be very aware of the power relations these solutions are embedded in. The tech sector is ill-equipped to apply a feminist politics of data. Many technologists working on new features for these platforms simply lack the background in feminist theory and practice to adequately frame and address online harassment.

By delegating the problem, we give already powerful private sector corporations even more power, and discursive control over online harassment and what should be done against it. If I were to pointedly exaggerate here, I might ask, are we comfortable to delegate “fixing” the online harassment of women, queers, people of colour and trans people to a majority of white SV bros? Speaking of “the master’s tools…”. My tentative final words here might be that working towards solving a complex social problem like online harassment requires us to work together, to build coalitions across disciplines, across industries, and across platforms rather than point fingers, attribute blame and demand others fix “it” (be that tech companies, legislators, ...).

**European Institute for Gender Equality (EIGE) presentation**

**#HerNetHerRights – Online violence against women and girls**

Digitalization provides not only a vehicle for new forms of violence such as image-based sexual abuse (otherwise known as non-consensual pornography) or ‘recruitment’ but a platform in which existent forms can manifest and be further facilitated.

In order to better understand the nature and prevalence of cyber violence against women and girls (VAWG), the European Institute for Gender Equality (EIGE) conducted desk research that aimed to identify and analyse the existing research on different forms of cyber VAWG and assess the availability of survey and administrative data on the phenomenon. Despite indications of increasing severity, EIGE found that to date, cyber violence against women and girls has not been fully conceptualised or legislated against at EU level and many questions remain as to its current scope and impact, or indeed that of the future.

EIGE’s analysis bolsters findings which view online violence as not necessarily distinct from violence experienced in the ‘real world’ but rather a continuum. For example, cyber stalking by a partner or ex-partner often follows the same patterns as offline stalking and can therefore be seen as intimate partner violence that is simply facilitated by technology. EIGE’s breakdown of data from the 2014 European Agency for Fundamental Rights’ (FRA) Survey on Violence Against Women found that **70 and 77 percent of women (aged over 15) who had experienced cyber stalking and cyber harassment respectively** had also experienced at least one form of physical and/or sexual violence by an intimate partner. However the stark lack of data available overall at EU level hampers the ability to conduct a gendered analysis of cyber violence as well as a comparison of online and offline VAWG or a tracing of the evolution of the phenomena and trends in numbers of those affected over time.
When considering **challenges vis-à-vis response** to cyberVAWG, it is necessary to reflect *inter-alia* on the following:

- **What is the responsibility of internet intermediaries?**
  
  From ‘cloud’ storage technologies to social media platforms where contact is user-generated, internet intermediaries represent a **heterogeneous group**, rendering it complex to discern to what extent they can be held accountable for cyberVAWG. As opposed to states (who must also take steps to prevent violence from occurring in the first place), the **human rights obligations of the information communication technology (ICT) sector** are limited to their respective platforms, e.g. the duty to ensure the immediate cessation of violence by removal of abusive content.

  One positive example of an initiative to tackle cyberVAWG (in part) in this instance is the introduction of Facebook’s recent photo-matching technology which prevents people re-sharing images previously reported and tagged as non-consensual pornography.

  However, it can be argued that internet intermediaries also have a social responsibility to ensure their services do not bring about harm to users; one precarious example is the introduction of Snapchat’s ‘Snapmap,’ function which allows for tracking of users down to the exact street address, a technology which could prove particularly threatening for those in abusive intimate partner relationships. The ICT sector, including app developers should **assess risk from a gender perceptive in the formulation of novel functions or settings.**

- **How can we tackle the issue of enhanced anonymity** offered by digital and virtual spaces, which provides particular challenges in identifying perpetrators of online violence against women and magnifies impunity?

  It is imperative that governments work with the ICT sector to this end, in order consider how (and in what circumstances) the latter can help to make the identify of perpetrators known. In doing so however, anonymity must not be viewed as a threat to be eradicated in and of itself as, for many, e.g. survivors of abuse, anonymity online can offer safety and re-entry to online space via the use of pseudonyms etc.

- **How can secondary transmitters be held accountable?**

  The actions of those who like, share, download or in some other way disseminate harmful content can contribute significantly to the secondary traumatization of those affected by cyberVAWG in the first instance. Further reflection on what should be the appropriate legal framework under which to hold secondary perpetrators of violence to account is needed.

  Noteworthy, is the recent adoption of **legislation targeting forms of cyber VAWG** by several Member States, among them;

  - **France**, whose ‘**Law of the digital republic**’ carries a €60,000 fine or two year prison sentence for perpetrators of image-based sexual abuse.
  - **Germany**, which mandates the deletion of imitate photographs when requested by person depicted.
  - **Italy**, whose new law on ‘**cyberbulismo**’ requires education on cyber-bullying in schools and allows victims or their parents to call for the removal of abusive content on hosting websites within 48 hours.
  - **Denmark**, whose programme entitled ‘**Stepping up initiatives against digital sexual abuse,**’ increases the penalty for circulation of non-consensual pornography from six months to two years and shall entail a survey of legislation and legal practice concerning digital abuse in a Nordic Context.
  - **United Kingdom**, who in 2015 introduced a criminal offence (and guidelines) with maximum two-years imprisonment for image based-abuse under which 200 people prosecuted within its first year. A helpline for victims of abuse was also established at this time, which received almost 2000 calls within its first six months in operation. The recent introduction of Guidelines on prosecuting cases involving
communications sent via social media constitutes a further step forward. The Guidelines, *inter-alia* include specific mention of VAWG and related issues, and can apply, in instances, to the re-sending of communications. Furthermore, they allow for the possibility to adduce evidence from social media for the prosecution of coercive and controlling behaviour.

However though laudable steps have been made to address cyber VAWG in many EU member states there is, to put it lightly, **still a ways to go.** Even where legislation exists, the criminal justice response has been found to be inadequate: For example, in the UK, of 1,160 reported incidents of non-consensual pornography between April and December 2015, **61% resulted in no action being taken against the alleged perpetrator.** The false dichotomy between online and offline violence, compounded by victim-blaming attitudes and lack of understanding of this new phenomenon, are among the factors that EIGE attributes to the inadequate response on part of the criminal justice sector thus far.

What are **EIGE’s recommendations** towards tackling cyber violence against women and girls?

- **Specialised training for police and judiciary, especially for first responders** (law enforcement, helpline operators).
- **Policy responses** should be formulated in recognition of the fact that cyber VAWG is a form of VAW. Strategies for addressing cyber VAWG must also include the **voices of women who are victims of the phenomenon.**
- The EU should aim towards agreeing on **definitions** of forms of cyber VAWG and incorporate these forms of violence into EU legislation, to ensure that victims of cyber VAWG in Member States have access to justice and specialised support services.
- In the immediate future, **definitions of cybercrime on the Migration and Home Affairs website should be updated to include forms of cyber VAWG,** or at the minimum, should **include misogyny in the third part of its definition.**
- A substantial aim of online abuse, whether misogynistic, racialized, xenophobic, homophobic, or an amalgam of myriad forms of discrimination, is to make its targets feel unwelcome, and thus retreat from the cyber sphere. In this sense, there are similar power dynamics at play as to the restriction of exercising freedom of movement in public space that many women experience on a daily basis (and can manifest differently for women with multiple identities). The upcoming EU-wide Survey on GBV (following from that of FRA in 2014) should **include a question about whether women have avoided online spaces for fear of experiencing cyber VAWG.** This will better enable us to examine the extent to which freedom of expression is hampered by cyberVAWG.
- **Quantitative and qualitative research** that examines **system responses,** based on survivors’ perspective.
- Entrenched commitment from ICT sector including **development of self-regulatory standards** and awareness raising on respective platforms.

If you found this interesting, you may like to look out for EIGE’s study on ‘Youth, digitalisation and gender equality,’ available in the latter half of 2018.

In the meantime, EIGE’s paper on ‘Cyber violence against women and girls’ can be accessed [here](#).
Essa Reijmers’ presentation (member European Women’s Lobby Observatory on Violence Against Women, representing the Netherlands)

Reclaiming the right to be safe online for every woman: the Dutch safetyNed project

safetyNed stands for the fundamental right of every woman to be safe online in ALL circumstances whether she is in a women’s shelter, in her own home, at work or elsewhere.

safetyNed is an initiative of 4 women’s shelter organizations that joined forces as we increasingly experience how abuse of technologies and different forms of online violence impact the lives of survivors of domestic violence. We saw the urgency as women arrived in our shelters and were found through “find my I-phone” within the hour upon arrival, so to speak… We saw fake accounts on social media, saw cases of spyware…

We also acknowledged that as frontline organizations, we lacked the proper awareness, tools and knowledge on technology and online media to protect our clients and help them protect themselves. As we did not feel ‘tech savvy’ enough there was a tendency amongst our advocates to shy away from technologies and issues on online violence. At the same time we are convinced that it is absolutely inadmissible to tell the women that suffer online abuse to get offline. We just had to turn things around: let the technology work for us, not against us and reclaim the right to be safe online.

So we started safetyNed, based on the vast experience of our American partners who started Safety Net (https://nnedv.org/content/safety-net/) in 2000.

safetyNed as we have developed it over the year is a platform and a network organization that integrates, builds and shares knowledge on abuse of digital technologies and online violence. We partnered with the experts of the American Safety Net project from the National Network to End domestic violence. They have a tremendous experience in this area; we are working closely with them on adapting their tools for our specific Dutch context. We also benefit greatly from their support, knowledge and networks with tech companies.

What we have accomplished so far is:

- We have created the safetyNed website which includes tools, stories of survivors and lots of information (http://safetyned.org/)
- We have formed and trained a specialist TechTeam of 8 advocates: all 8 of them practitioners that come from our shelter organizations. The TechTeam are our ‘geeks’, our specialists that assist all the front line workers in our shelter organizations.
- The TechTeam has started to instruct their co-workers, are organizing training sessions and offer daily support on difficult cases involving technology and online issues;
- The TechTeam also continues to document stories of survivors and their advocates, with a focus on effective strategies to deal with abuse of technology
- We have integrated a specialized risk-assessment screening on online violence in the risk-assessment tools that were already in use in the shelters, as well as for our non-residential services.

A lot of focus has been - and will continue to be - on raising awareness with front line domestic violence workers, both in shelters and other service providers such as the police, the judiciary etc. Raising awareness with policy-makers and lobbying on this issue has just begun and will become more and more important as we go on.

Let me finish by highlighting two of the challenges in our journey so far:

- It has not been easy to raise funds and get the money to do this important work: the four founding shelter organizations have chosen to invest heavily in this project to make this issue visible: now that we are becoming visible policy-makers and commissioners, such as the Ministry of Safety and Justice and the local
authorities where we hope to raise funds for this project, have become more aware of the necessity of this work and get interested in these developments.

- Technologies are moving and developing so quickly that many advocates are afraid they will never be able to keep up and to fully grasp what is happening.... At one point we just had to decide: we cannot wait until we know enough of all technologies, we will have to partner with other experts and build a community of knowledge and sharing and keep on moving forward with these coalition partners as we go along.... That also is a way of reclaiming the right of being safe online. And that is in a nutshell what the Dutch safetyNed project is all about....