online gender based violence

REPORT BY
LAIA SERRA PERELLÓ

DECEMBER 2018

PUBLISHED BY
Pikara online magazine

WITH SUPPORT FROM
Ajuntament de Barcelona

IN COLLABORATION WITH
calala Fondo de Mujeres
FRONT LINE DEFENDERS

CONTENTS

INTRODUCTION

The reach and importance of the Internet in our lives is such that we are starting to consider its use a human right. However, according the **European Institute for Gender Equility** (EIGE), in the context of the current pandemic of violence against women and girls, online gender-based violence is a growing problem of global proportions with major implications. Online violence particularly affects women who fight for their rights, those who belong to vulnerable groups, those who suffer violence offline and activists spearheading feminist demands, challenging gender roles and the violence that sustains male privilege.

In terms of women's rights, it is essential to ensure that the internet, seen as a new public space with an influence that is growing exponentially, is a safe, violence-free and empowering place for all women and girls.

In July 2018, the United Nations Human Rights Council approved a resolution through which it analysed the severity of the situation, the inadequate approach to the matter and the need to change the way State parties respond.

Taking advantage of the publication of this **Resolution**, lawyer and activist Laia Serra Perelló and Pikara Magazine publish this report.

For this project, we been supported by Calala Fondo de Mujeres and Front Line Defenders.

WHAT IS VIOLENCE AGAINST WOMEN?

According to **international definitions**, violence based on the sex/gender system includes:

// violence against women **because they are women.**

// violence that disproportionately affects women.

// any act that results in physical, mental or sexual harm or suffering, including threats to commit such acts, coercion or other forms of deprivation of liberty.

// any fundamental **social**, political and economic milieus that perpetuate inequality between men and women, as well as their stereotypical roles.
violence that is rooted in other spheres, such as the rights ideology that advocates the privileges of men over women, social standards relating to masculinity and the need to affirm masculine control and power.

// violence that seeks to impose assigned gender roles or prevent, discourage or punish anything considered 'unacceptable' behaviour in women. These factors also contribute to the explicit or implicit social acceptance of such violence.

The right of women to a life free of gender-based violence is inseparable from and interdependent on the effectiveness of other human rights.

ONLINE GENDER-BASED VIOLENCE AGAINST WOMEN

ANALYSIS OF THE PHENOMENON

Online gender-based violence against women can be defined as any act of gender-based violence committed, instigated or aggravated, in part or in full by the use of information and communication technology (ICT), through mobile phones, the Internet, social networking platforms or email. This online gender-based violence is another form of violence and discrimination against women and constitutes a violation of their human rights.

At the European level, it still has not been fully conceptualised, nor has it been legislated against. The few studies available claim that a higher proportion of women and girls are the target of certain forms of cyber violence than men, that women and girls face specific threats, and that the effects of such threats are more traumatic for them.

Online gender-based violence is a continuation of the violence that women and girls face outside of the technological environment. The use of the Internet is set within a context of structural gender discrimination. The digital world is crossed by social, economic, cultural and political structures and reproduces the associated forms of gender discrimination and patriarchal patterns that result in gender-based violence offline. On the other hand, ICT has contributed to women's empowerment and the greater fulfilment of their human rights. Nevertheless, this potential continues to be subject to the way in which people access and use ICT. The digital gender gap, or gender inequality in accessing technology, is a multidimensional phenomenon that encompasses questions regarding access to technological equipment, applications or software, connectivity and data, as well as the skills, knowledge and opportunities to develop and make use of ICT and to make a positive and strategic use of it The use of ICT without a human rights-based approach and without prohibiting online gender-based violence has facilitated new types of gender-based violence and this digital divide.

With regard to this, two relevant reports are available:

// **2017 - United Nations Human Rights Council (UNHRC):** THE UNHRC issued a **report** in which it determines that this new global digital space offers great potential for ensuring the promotion and acceleration of human rights, including women's rights. The **UNHRC** highlights the fact that the introduction of the internet has been unequal and has occurred at different rates, thereby exacerbating inequalities between men and women.

// **2018 - UN report on women:** the UN compiled a specific **report** on online gender-based violence. It constitutes a form of discrimination against women and a human rights violation, which fits in with the definitions of international instruments for the protection of women's rights. It shares its cause with other forms of violence against women and should be addressed in the broader context of the elimination of all forms of discrimination against women.

The technological dimension of violence against women and girls brings specific and relevant factors, such as the ease of searching for content, the persistence of the latter on the Internet, along with replicability and scalability. Each time content is disseminated, it promotes and reinforces violence against women and girls, and can give way to further revictimisation and new trauma for victims/survivors, given that a permanent digital record is created that is difficult to remove. A cyber attack against one woman affects all women, who are perceived as potential victims of such attacks. On a policy level, international bodies have recognized the principle that human rights protected offline must also be protected online. However, their reports indicate that many States are failing to fulfil their obligation to adopt appropriate measures, or are using the laws against online gender-based violence as a pretext for restricting liberties, including freedom of expression.

Institutional and structural discrimination against women and girls is embodied in laws, policies and practices that directly or indirectly restrict access, on equal terms, to digital technology. This is detrimental to the empowerment of women and girls and makes them more vulnerable to violence, as well as exacerbating any violence already suffered.

Despite the lack of exhaustive data, given that this is a relatively new phenomenon, the **2014 EU-wide survey** by the European Union Agency for Fundamental Rights (FRA) highlighted that 23% of women had reported that they had suffered abuse or harassment online at least once in their life, and that one in ten women had experienced some kind of cyber violence from the age of 15.

These data indicate that there is an urgent need to combat gender stereotypes and negative social norms that sustain and perpetuate this violence. Without this, it will be difficult for digital technology to be able to contribute to women's empowerment and their full, effective and equal participation in political, economic, cultural and social life and in the innovation, development and application of ICT. To prevent this, a transnational, multidimensional proactive and reactive approach is needed, as well as active cooperation between the State and private sector, given its widespread use and the continuous development of digital technologies.

TYPOLOGIES OF WOMEN ATTACKED AND SUBJECT TO VIOLENCE

In its **2014 report**, the Association for Progressive Communications (APC) highlighted the following trends:

// Young women, between 18 and 30 years of age, are the most vulnerable

// 40% of attacks are committed by someone known and 30% by someone unknown to the woman or girl

// There are three main profiles of women who are attacked:

- women who are in a violent intimate relationship;
- professional women with a public profile who participate in communication spaces (journalists, researchers, activists and artists);
- and female survivors of physical or sexual violence.

In November 2017, the Mexican association Luchadores compiled a **Report** which included a typology of aggressions against women through ICT:

1. Unauthorised access (tapping) and monitoring access
2. Control and manipulation of information
3. Spoofing and identity theft
4. Monitoring and cyberstalking
5. Discriminatory statements
6. Harassment

7. Threats
8. Dissemination of personal or intimate information without consent
9. Blackmail
10. Discrediting
11. Sexual abuse and exploitation associated with technology
12. Attacks on women's channels of expression
13. Oppression by those with regulatory power

As can be seen, several of the above forms of aggression can occur within the same act of violence facilitated by ICT. These forms of violence are often interdependent and mutually reinforcing. Documenting them in such detail enables a better understanding of the complexity of this phenomenon, the analysis of its relationships and the ideation of better strategies to combat them.

The Committee of the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), in its 2017 **Recomendation**, highlighted the crimes committed against female human rights defenders, politicians, activists or journalists, which also constitute forms of gender-based violence due to cultural, ideological or political reasons. Human rights defenders, journalists and politicians in particular are attacked, threatened, harassed or even killed, which demonstrates the undeniably political dimension of online violence against women.

This violence gives rise to and perpetuates the self-censorship of these women. Some resort to using pseudonyms, while others adopt low-level online profiles, a measure which may be detrimental to their professional lives and reputations. Others decide to suspend, deactivate or permanently delete their online accounts, or leave their profession altogether.

Ultimately, online abuse against female communicators and professional journalists is a direct attack on the visibility of women and their full participation in public life. Online gender-based violence also undermines democracy and good governance and, as such, creates a democratic deficit.

An addition to the internationally recognized definitions of online gender-based violence is the 2015 definition from the **Internet Governance Forum**:

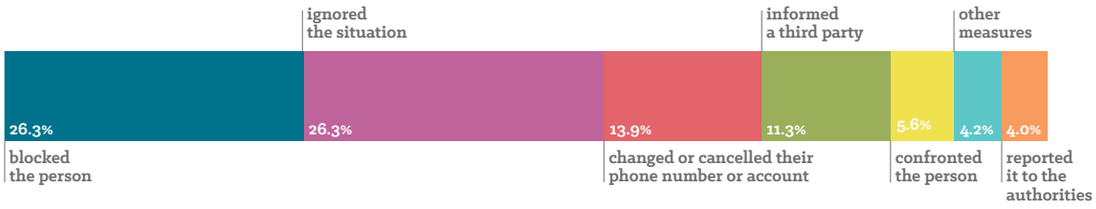
INVASION OF PRIVACY	✕ Accessing, using, manipulating and/or disseminating private data without consent (by cracking personal accounts, stealing passwords, using/stealing identities, using another person's computer to access a user's accounts while he/she is logged in, etc.)..
	✕ Taking, accessing, using, manipulating, and/or disseminating photographs and/or videos without consent.
	✕ Sharing and/or disseminating private information and/or content, including sexualised images, audio clips and/or video clips, without knowledge or consent.
	✕ Doxing: Researching and disseminating personally information that identifies an individual without their consent, sometimes with the intention of providing access to the woman in the 'real' world for harassment and/or other purposes.
	✕ Contacting and/or harassing a user's children, extended family, colleagues, etc., to gain access to her.
SURVEILLANCE AND MONITORING	✕ Monitoring, tracking and/or surveillance of online and offline activities.
	✕ Using spyware or keyboard loggers without a user's consent.
	✕ Using GPS or other geolocation software to track a woman's movements without her consent.
	✕ Cyberstalking

DAMAGING REPUTATION OR CREDIBILITY	✕ Deleting, sending and/or manipulating emails and/or content without her consent.
	✕ Creating and sharing false personal data (such as online accounts, advertisements, or social media accounts) with the intention of damaging a user's reputation.
	✕ Manipulating and/or creating fake photographs and/or videos.
	✕ Identity theft (e.g. pretending to be the person who created an image and posting or sharing it publicly).
	✕ Disclosing private (and/or culturally sensitive/controversial) information for the purpose of damaging someone's reputation.
	✕ Making offensive, disparaging and/or false comments and/or posts online that are intended to tarnish a person's reputation (including defamation).
HARASSMENT (WHICH MAY BE ACCOMPANIED BY OFFLINE HARASSMENT)	✕ 'Cyberbullying' and/or repeated harassment through unwanted messages, attention and/or contact.
	✕ Direct threats of violence, including threats of sexual and/or physical violence (e.g. threats like 'I am going to rape you').
	✕ Abusive comments.
	✕ Unsolicited sending and/or receiving of sexually explicit materials.
	✕ Incitement to physical violence.
	✕ Hate speech, social media posts and/or mail; often targeted at gender and/or sexuality.
	✕ Online content that portrays women as sexual objects.
	✕ Use of sexist and/or gendered comments or insults (e.g. use of terms like 'bitch'/ 'slut').
	✕ Use of violent images to demean women.
	✕ Abusing and/or shaming a woman for expressing unconventional views t, for disagreeing with people (often men) and also for rejecting sexual advances.
	✕ Inducing suicide or advocating femicide.
	✕ Mobbing, including the selection of a target to annoy or harass.
	✕ Mobbing by a group of people rather than an individual and as a practice specifically facilitated by technology.
DIRECT THREATS AND/OR VIOLENCE	✕ Trafficking of women through the use of technology, including the use of technology for victim selection and preparation (planned sexual assault and/or femicide).
	✕ Sexual blackmail and/or extortion.
	✕ Theft of identity, money and/or property.
	✕ Impersonation resulting in a physical attack.

TARGETED ATTACKS ON COMMUNITIES	✕ Cracking websites, social media and/or email accounts of organisations and communities with malicious intent.
	✕ Surveillance and monitoring of activities by members in the community.
	✕ Direct threats of violence to community members.
	✕ Mobbing, specifically when selecting a target for bullying or harassment by a group of people, rather than by an individual, and as a practice specifically facilitated by technology.

According to the **2017 Luchadoras Report**, women who experience cyberbullying took the following decisions:

26.3% blocked the person
26.3% ignored the situation
13.9% changed or cancelled their phone number or account
11.3% informed a third party
5.6% confronted the person
4% reported it to the authorities
4.2% adopted other measures



The Luchadoras report describes four relevant findings:
1. It identifies the multitudinal nature of some attacks by organised groups.
2. It documents the degree to which the mobile phones are used.
3. It analyses the violent nature of public social conversation on social networks, as evidenced by misogynistic and male chauvinistic hashtags that promote violence against women; memes, jokes and taunts; the continued use of the word 'feminazi' to attack feminist activists; in parallel with suggestions to men that they commit corrective rape or images of battered or murdered women, who become targets of attack, mainly as a result of reporting violence or publicly voicing their opinions in support of issues such as abortion.
4. It is noted that only one case of a male victim of bullying or sexual harassment was recorded, compared to rest of the women interviewed.

The report also outlines six prevailing trends:
1. Viral hate: in response to a woman with a public profile on networks, publicly denounces an aggression on social networks, thereby triggering a wave of online violence, revictimising her, blaming her, taunting her or questioning the veracity of her complaint.
2. Exclusion from spaces of expression and" taking down": organised attacks on networks of activists, associations and media outlets that publicly identify themselves as feminist and which represent their main space for expression and influence.
Attacks generally fall into two categories:
i. use of the terms of use of Facebook to report content that the platform considers unlawful;
ii. Denial-of-Service (DoS) attacks.
3. Campaigns of organised attacks by groups with fake accounts.
4. Extortion under the threat of disseminating intimate images without consent.
5. Espionage by the State.
6. Smear campaigns.

All forms of online gender-based violence aim to control and attack women and maintain and reinforce patriarchal norms, roles and structures and an unequal balance of power. This is particularly evident when violence, threats and harassment occur in response to speeches or statements relating to gender equality and feminism, or when defenders of women's rights are those attacked.

ICT can be used as a tool to generate digital threats and to incite acts of gender-based violence. In addition, it is noted that women who speak openly on social networks about the abuse they have suffered are increasingly threatened with having legal defamation proceedings filed against them in order to dissuade them from submitting a complaint.

THE INTERSECTIONALITY PERSPECTIVE

Women experience multiple and interrelated forms of discrimination, each of which affects them differently. Some groups, such as young women, women from ethnic minorities and indigenous and racialised women, lesbians, bisexual and transgender women, non-binary people, women with functional diversity and women from other marginalised groups may be at a **greater risk** and suffer particularly serious forms of online violence. Furthermore, some of these groups use the internet specifically to access information, socialise, build communities and promote their rights, for which they are particularly at risk.

The Brazilian associations Coding Rights and Internet Lab assert the idea of 'digital colonialism' in their **2017 report**. The geopolitical context in which manifestations of online gender-based violence arise means it is harder for those affected in the Global South to obtain unsatisfactory responses from the conglomerate of Internet platforms in the Global North. Their monopoly allows them to establish censoring practices in line with their cultural patterns, which are often more restrictive with the manifestations involving the body as a form of expression, typical of other cultures and feminism.

Access to technology in itself is also affected by intersectional forms of discrimination, based on factors such as skin colour, ethnicity, caste, sexual orientation, gender identity or expression, skills, age, class, income, culture, religion and urban culture versus rural environment.

Any approach to combating online violence and abuse that is not intersectional will continue to increasingly silence women from marginalised communities, who are most affected by violence facilitated by ICT.

IMPACT AND HARM CAUSED BY ONLINE GENDER-BASED VIOLENCE

The harm caused by the various manifestations of online violence especially affects women and girls, who are particularly stigmatised. This violence has an impact on the right of women to self-determination and bodily integrity, on their ability to move around freely without the fear of being monitored. This denies them the opportunity to create their own online identities and to form and participate in social and politically relevant interactions. What is more, women do not even need to use the internet to suffer online gender-based violence. For example, in the case of disseminating videos of sexual assault online without the consent of those affected.

Ther 2017 **APC Report** identifies some of the harm experienced:

// Psychological harm: experiencing depression, anxiety, fear or even suicidal thoughts.
// Social isolation: withdrawal from public life, including contact with family and friends.
// Economic losses: dismissal and loss of sources of income, or difficulty finding employment due to stigma.
// Limitation of mobility: difficulty participating in online and/or offline spaces.
// Self-censorship: limiting activity due to a fear of greater victimisation and the loss of confidence in the safety of using digital technology.

Beyond the individual impact, a significant consequence of online gender-based violence is its social or community impact. It creates a society in which women no longer feel safe on or offline, limiting their ability to benefit from the same online opportunities as men.

The 2017 **Report** released by the Luchadoras Association describes three groups of symptomatic effects of online gender-based violence, and states that violence encountered online is real and transcends the 'virtual environment', impacting victims/survivors on a personal, emotional, professional and life-experience level.

// Physical harm: sweating, nausea, headache, back, stomach and kidney pain, lack or excessive appetite, a feeling of an empty stomach, muscle tension, crying, a sensation of heaviness in the body, self-harm
// Emotional harm: nervous conditions, stress, distress, rage, anger, depression, paranoia, fear, confusion, helplessness
// Other: fear of leaving the house, self-restriction of mobility, abandonment of technology, self-censorship, a feeling of being constantly watched, overall sense of insecurity.

Amnesty International's March 2018 report, **#ToxicTwitter**, points out that the psychological consequences of online violence remain poorly researched and, as a result, are understimated. Nevertheless, almost all of the women interviewed by the organisation reported adverse effects on their mental health: stress, anxiety, panic attacks, helplessness and a loss of self-confidence, sleeping problems and a general sense of loss of power. Some 41% of women interviewed described feeling that their physical integrity was threatened.

The mental health experts interviewed emphasised that uncertainty over the plausibility of threats means that women are much more cautious in expressing themselves when interacting with their surroundings. Other psychological consequences specific to online gender-based violence include a reduced ability to concentrate and difficulty in making everyday decisions. The persistence of online abuse causes alarm, distress and fear of others.

IMPACT ON FUNDAMENTAL RIGHTS

Measures to protect women online must take into account the various rights at stake, such as safety, mobility, participation in public life, freedom of expression, and privacy. They must also take into account any pre-existing inequality and discrimination.

International organisations describe the tensions between rights (security vs freedom of expression) that the fight against online gender-based violence may cause. But associations such as the APC have countered that the controversy regarding the collision of rights arises because States are responding to interpellations to act against online gender-based violence with conservative measures that are often moralistic and protectionist, which may lead to censorship, limit discourse and even affect other fundamental rights.

When it comes to adopting any restrictions on these rights, States must consider the importance, nature and scope of any proposed limitation, and must always opt for measures that are least restrictive with regard to rights. This is particularly important in a global context of the restriction of arenas of participation by civil society and of the rejection of any progress achieved with respect to women's rights in general.

FREEDOM OF EXPRESSION ON THE INTERNET

In June 2013, the UNHRC adopted a **Resolution** through which it states that the effective exercise of the right to freedom of opinion and expression is essential to the enjoyment of human rights and liberties, and constitutes a cornerstone in the construction of a democratic society.

The internet is a key tool with which people can exercise the right to freedom of opinion and expression, in order to form political communities and questions on related issues. The internet enables women activists to connect with one another and exchange strategies. It also offers them a space to self-organise in exercise of the right to peaceful assembly. The internet can be an important, and sometimes the only way for women to access information and express their views on issues that concern them and that affect their life choices and needs.

Women activists, including human rights defenders, increasingly depend on ICT to access information and promote, communicate, mobilise and obtain visibility. It is precisely groups such as LGTBIQ collectives, organised civil society, human rights defenders, journalists and victims of violence on whom increased online surveillance has been detected. Women who belong to these groups face threats and specific risks that require protection measures with a gender perspective to be taken.

The UN Special Rapporteur on the situation of human rights defenders, in his 2018 **Report**, describes the defamation complaints made against male and female human rights defenders for having published online articles, blog posts or tweets. In addition, the Rapporteur underlines the need to adopt protection measures with a gender perspective and states that their physical security should be interrelated and integrated into their digital security.

Online gender-based violence has an effect of inhibiting women's discourse and, as such, is a key theme with regard to freedom of expression in general. The legal definitions of incitement to hatred vary significantly between different countries. What they do have in common is that legal frameworks often do not consider incitement to gender-based violence and misogynistic content as incitement to hatred.

The UN Special Rapporteur on the freedom of expression, in his **2011 report**, warns that States have adopted a series of unacceptable restrictions on the right to freedom of expression in name of the fight against hate speech. These include blocking or criminalising content related to political debate and discussions regarding governmental policy. Sometimes these restrictions on freedom of expression have been justified on the basis of the fight against gender-based violence.

EDUCATION AND CULTURE

ICT enables greater access to feasible and inclusive educational opportunities for women and girls, as well as to science and culture. The internet is an essential platform for scientific and cultural trends and exchange. The internet can facilitate women's access to and participation in science and culture, giving them opportunities to express themselves and to present discourse and alternative interpretations and encourage their open interaction with people, ideas and activities beyond national and cultural borders.

The freedom to access the internet and maintaining its open structure are important for protecting people's right to participate in cultural life and for enjoying the benefits of scientific progress and its applications.

WOMEN'S POLITICAL PARTICIPATION ONLINE

Feminist groups that work with ICT have been reflecting on the political dimension of the internet, the new digital public forum, and the role of women and activists online.

A 2013 **monograph** by the Asociación para la Cooperación con el Sur (ACSUR)- Las Segovias and Donestech quotes cyberactivist Lara Tíscar of Prag-máTIC@S, who notes that, "somehow, through our digital fragments and fingerprints, we are leaving behind our stories with which our social history will be built in the future".

This monograph focuses on the fact that social networks enable the condemnation of inequalities, organisation of campaigns, the creation of forums for topics that are little discussed and are of public interest. Women are reinterpreting technologies as tools for political organisation and as a means of creating new feminist communities. The reality is that more and more women are logging onto, browsing and contributing to the construction of the internet, making use of its interactive services and opening spaces for communication and action on the web in order to transform the world. Women are taking ownership of technology via the web in order to use it as a basis for a more inclusive and egalitarian society.

The momentum of women's organisations and cyberfeminists in this area is very important, not only because of the number of initiatives recorded but also the innovation of strategic and creative applications of which they make use. In response, these initiatives have been attacked in the form of online violence particularly directed at 'techy' women who attempt to start a debate on sexism and machismo in technology development. One of the unignorable references is the **Feminist Principles of the Internet**, revised in 2016, which laid down a decalogue of the principles on which the internet should be based.

On a State level, we can cite the recent Donestech report, **Redes sociales en perspectiva de género: guía para conocer y contrarrestar las violencias de género on-line** (Social networks from a gender perspective: a guide to understanding and counteracting online gender-based violence), drafted in 2017 on the initiative of the Regional Government of Andalusia, which gave an in-depth analysis of online violence. In this report, they warn of the effect generated by algorithms of 'ideological bubbles. These give rise to an inertia that means we only receive information that has been filtered based on our profile and search history. This inertia creates a harmful effect of self-referencing, which often reproduces power structures and makes it very difficult to achieve social change. Their report echoes the different initiatives of national and international self-defence actions and tools and good digital safety practices with a feminist perspective.

Regarding the incidence of online violence in women's political participation, two reports are of note:

/// **2013 - UNHRC:** notes that stigmatisation, harassment and direct attacks have been used to silence and discredit women who make their voices heard as leaders, community workers, human rights defenders and politicians. The active participation of women, on an equal footing with men, in all areas of decision-making is essential to achieving equality, sustainable development, peace and democracy.

// **2016 - UNHRC:** issued a **Resolution** on enjoyment of human right on the internet, in which it condemns all abuse and violence in the digital space, including exclusion, intimidation and harassment and gender-based violence committed in retaliation for exercising human rights and fundamental freedoms online.

// **2017 - Luchadoras Report:** mentions that the digital space has become an area that complements participation in street protests, assemblies and face-to-face discussions. Due to their significance as a forum for social and political participation, the exercise of rights and the exchange of information and ideas, digital platforms are a battle ground on which freedom of expression is attacked. In this sense, online harassment, particularly by means of threats on social networks, has established itself as a way of intimidating, instilling fear and censuring.

// **2017 - APC report:** mentions that LGTBIQ people, sex workers and others that use the internet to promote the rights of marginalised women are particularly susceptible to risk. Their critical work on matters that are often taboo or controversial and the difficulty of accessing other types of public spaces to facilitate the exchange information and organisation mean that it is essential to respond to the specific risks that they face online. In the digital age, the normalisation of violent behaviour and the culture of tolerance of violence against women that social networks perpetuate and facilitate at great speed, reinforce sexist and violent attitudes and contributes to standards and practices that make online and offline spaces hostile for women and communities at a greater risk of injustice and discrimination.

// **2017 - UNHRC**: in its **Report**, states that without access to the internet, marginalised groups may remain trapped in a disadvantaged position in which inequality is perpetuated; these groups can include women. An internet governance structure based on human rights must ensure that people are able to report violations of their rights and that remedies are accessible and effective. A systematic approach involves addressing the full scope of human rights of women that are affected by ICT.

SECURITY, PRIVACY, ANONYMITY AND DATA PROTECTION

The October 2013 **monograph** by ACSUR - Las Segovias dedicates one section to internet security, and states that the implementation of praxes focused on increasing individual or collective security must be thought of as a multidimensional process. It is affected by operating systems, how we connect, browse and find information on the internet, or even the type of passwords we use. The purposes for which we use these technologies affect the types of security we will need.

Striving to achieve greater security contributes to women's empowerment, as it is based on an affirmation of the value to their digital identities. The monograph claims that the majority of commercial social networks encourage a combination of harmful practices with regard to security. Security levels are low, non-existent or irregular, facilitating the mining and selling of data. Decisions regarding data are taken unilaterally and irrevocably, in the absence of any decision-making machinery based on the direct participation of the community. The terms of use and the configuration of these applications often promote the privacy paradox. This means that most people say they are worried about the confidentiality of their data, but do not take the necessary steps to protect them.

Regrettably, in the name of security, restrictions on copyright are prevalent, freedom of expression is limited for random reasons and moral censorship is practiced, in many cases affecting women, feminist groups and activists in general. Furthermore, it also continuously leads to the privatisation of intelligence and the collective memory.

Anonymity and privacy are essential to exercising the freedom of expression online, but they can also facilitate gender-based violence, by providing those responsible with an invisibility cloak, perceived as impunity. Many governments have argued that waiving or reducing the right to privacy and anonymity is necessary to guarantee security.

Anonymity is particularly necessary in repressive environments, in which some forms of expression are considered illegal. The ability to remain anonymous online has played an important role for women and other people at risk of discrimination. It enables them to search for information, find solidarity and share opinions without fear of being 'discovered'. According to the APC, in its **2011 Report** on sex and the internet, thanks to interactivity and anonymity facilitated by ICT, people against whom hate speech and online harassment is directed can interact directly with their aggressors, ceasing to be passive victims and proceeding to give effective responses. Anonymity also reduces the risk of arbitrary or illegal interference in women's private lives.

The use of ICT could lead to interference in one's private life through monitoring and control of correspondence and activities, or selective attacks on privacy by publishing personal data and information on the internet (doxing). The collection, storage, exchange and adaptation of large datasets also present a challenge to women's right to privacy.

// **2011 - APC Report**: reflects on the fact that debates surrounding privacy are dominated by the viewpoints of middle-class men. The public and political discourse on privacy is often framed within the context of the same cultural and moral perspectives used to reinforce gender roles and control women's bodies. Privacy violations committed by intimate partners, fathers and brothers are not always interpreted as an invasion of privacy. In many cases, it is the morality of the victim/survivor that ends up being questioned, and the violation of her privacy becomes embarrassing for her.

// **2015 - Report of the UN Special Rapporteur on the freedom of expression:** highlights that people who face discrimination and persecution based on their sexual orientation and gender identity may be forced to rely on encryption and anonymity in order to bypass restrictions and exercise their right to search for, receive and impart information. Anonymity, including the performance and saving of anonymous searches, is essential to fully exercising the right to form and hold opinions.

// **2016 - UNESCO report**: in its Report on Human Rights and encryption, points out that 'much of the debate on encryption to date has been gender blind, or perhaps worse, dominated by men'.

// **2017 - UNHRC report:** reports that privacy is an essential requirement for the full exercise of other rights, particularly the right to freedom of opinion and expression. Women's right to privacy in the context of ICT includes their ability to benefit from data encryption, anonymity or the use of pseudonyms to reduce the risk of interference.

// **2018 - Report of the UN Special Rapporteur on women:** reports that ICT innovations have increased the ability of States and companies to monitor, decipher and compile and use data on a massive scale. Many forms of online gender-based violence are in themselves acts that violate the right of women and girls to privacy.

RESPONSIBILITIES OF INTERNET INTERMEDIARY PLATFORMS

Companies that manage social network platforms, given their ubiquity, growing userbase and the contradictory application of terms of use, play an important role in the permissiveness of certain harmful speeches, the normalisation of gender-based violence and the sexual objectification of women.

In August 2014, the APC published a **Report** on the company policies of Facebook, Twitter and YouTube with regard to online violence against women. The report highlights:

1. The reluctance to make a direct commitment to tackling online gender-based violence, failing to recognise their responsibility in the adoption of measures to eradicate it.
2. The lack of transparency regarding complaint and remedy processes, which is reflected in the lack of information on the procedures available to victims/survivors.
3. The lack of commitment to the perspectives of non-US/non-European women.
4. The lack of public commitment to human rights standards or to the promotion of rights beyond promoting freedom of expression.

Another 2017 APC **Report** shows that inadequate responses by online internet platforms to online gender-based violence contribute to the inhibition of women's freedom of expression. The imposition of certain terms of use may lead to censorship by platforms or other users. In contrast, they do not offer mechanisms to obtain remedies or submit complaints. The APC advocates leaving behind the limited framework of discussion on legal obligations and moving on to focus on the responsibilities, which imply an empowered role, positive action, leadership and accountability. In the European context, the 2011 Istanbul Convention obliges the private communications sector to commit to eliminating both discrimination and gender-based violence against women.

At a time when the efficiency of the capture and analysis of people's data implies a higher advertising income, the right to privacy is particularly affected. In order to operate in different national and regional markets, companies have set up backdoors or applied more restrictive privacy controls in view differing national legislative requirements. Activists in Brazil, in their **2017 Report**, claim that companies are making no effort to adapt to local customs, nor to respect regional anti-discrimination laws.

Activist and feminist groups have seen their communication channels attacked regularly through the complaint mechanisms of social networks, which results in their accounts being temporarily or permanently closed. On the other hand, when women report the avalanche of comments that attack them and stifle their discourse on social networks, they are told that threats and other violent content do not contravene the platform's terms of use. This suggests an inherent sexist bias in both the staff employed and in company policies. Furthermore, any display of naked women's bodies is frequently interpreted from a moralist and heterosexual male standpoint, thereby sexualising the female body. Censoring representations of their bodies denies women the right to political, creative, sexual and other forms of expression through embodiment.

Women who have anonymous online profiles or use pseudonyms are also negatively affected by the anonymity policies of certain intermediary platforms. Women human rights defenders who choose to remain anonymous on websites such as Facebook are often reported by harassers for having 'fake' profiles. Instead of taking action against the harassers, companies sometimes demand that the women affected reveal their identity, which puts them at risk.

The solutions put forward by the companies do not adequately resolve the needs of communities affected by online violence, especially women who do not speak English and groups at risk of exclusion. It is not always easy to know how to activate complaint mechanisms, follow-up on a complaint and, where appropriate, appeal against the company's decision, as there is no 'customer service department'. There is no accountability over the procedures they adopt, the type of content they remove or statistical data, thereby making any external evaluation difficult. There are also very few user awareness campaigns.

The May 2017 **Report** of the UNHRC reminds us that all companies, including those operating in the ICT sector, have a responsibility to respect human rights, in accordance with the **UN's Guiding Principles on Business and Human Rights**. In addition, they must identify, prevent, mitigate and respond to any adverse effect that they cause, contribute to or to which they are directly associated. That includes the obligation to tackle online gender-based violence.
The June 2018 **Report of the UN Special Rapporteur** on women's human rights reports that the role of companies in regulating and governing the internet is increasingly being called into question. The full scope of their specific responsibilities has still not been addressed within the international human rights framework, and even less so under international instruments governing women's rights. Although there has been focus on their commercial responsibility, no attention been paid to how their policies and practices impact on women's rights. Their inadequate responses lead to the self-censorship and censorship of women and there is a lack of effective redress mechanisms for victims/survivors of online gender-based violence.

Preserving the anonymity of users is essential, but establishing mechanisms to identify those responsible is also necessary to address online gender-based violence. Access to justice requires the Judiciary to be able to associate digital identifiers such as an IP address, physical devices those responsible in order to make a judgement.

In order to tackle online violence, companies so far have acted in two ways: reinforcing their terms of use, or automation by means of algorithms. For example, there has been no discussion over the use of hashtags to prevent removed content from reappearing online. Within the European context, in 2014 the European Parliament issued **Recommendation CM/Rec(2014)** entitled 'Guide to human rights for internet users', in which, among other measures, it demands that users be given clear and transparent information on the redress measures on which they can rely.

In 2016, European institutions also succeeded in forcing the internet giants Facebook, YouTube, Twitter, Microsoft, and recently Instagram, to adopt a **Code of Conduct**. This provides for various commitments, including the commitment to have clear and effective procedures for examining complaints regarding hate speech, so that access to such content can be withdrawn or disabled within 24 hours. According to the **third evaluation** of the application of this code in January 2018, its implementation had succeeded in eliminating 70% of content identified as being hate speech.

Another important commitment is that, following a complaint, the evaluation as to whether or not to remove the content will take place in line with internal standards but will also be subject to **Framework Decision 2008/913/JAI** on combating racism and xenophobia through criminal law. The removal of content will follow the regulation set out in the **Electronic Commerce Directive 2000**. The **Audiovisual Media Services Directive 2010**, also contains standards on the removal of discriminatory content.

STATE RESPONSES, LEGAL TOOLS AND PUBLIC POLICIES

GLOBAL TRENDS

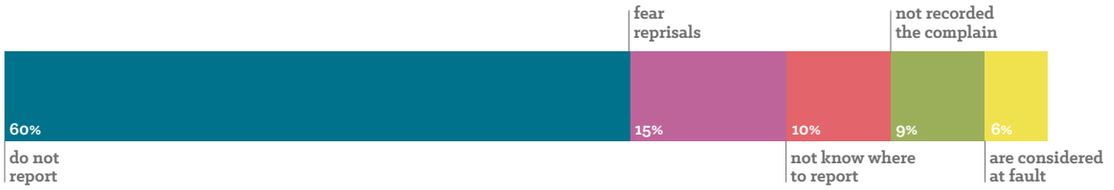
The 2015 APC **Report** on legal mechanisms regarding access to justice for victims/survivors of online gender-based violence examined seven countries. Its research revealed an extremely inadequate but common response by State parties. It also demonstrated the incompetence of authorities, who often trivialised complaints and put the blame on the complainants, did not have sufficient technological knowledge and were slow to investigate. Authorities did not resort to make use of specific existing laws due to indifference or lack of knowledge. In the absence of specific legislation regarding online gender-based violence, they make inflexible interpretations of existing laws on cybercrime, gender-based violence or privacy, thereby hindering the identification of those responsible. This creates a culture of silence that inhibits the reporting of online gender-based violence.

The growing pressure on law-makers to draft new legislation based on the approach that adopts this could work against the progress that already been made with significant effort with regards to rights, such as the decriminalisation of defamation. States can use these demands for protection from online gender-based violence, to increase censorship and the invasion of privacy. The APC, for example, has explicitly stated its opposition to the fact that offensive, discriminatory or even violent comments made towards women should carry a prison sentence. The APC warns that given the patriarchal and racist legal systems where impunity is more common than justice, these new laws, designed to protect vulnerable communities, could end up being used against them.

The **Report** drafted by Argentina's Asociación por los Derechos Civiles (Civil Rights Association) in collaboration with the Activismo Feminista Digital (Digital Feminist Activism) foundation in 2017, analyses the reasons for the under-reporting of this violence. This points to the lack of awareness of their own rights among women affected; the difficulty of access to evidence; the lack of confidence in the role of the State (police and judiciary); the financial burden of litigation, the fear and embarrassment of victims/survivors; the impact of further victimisation; the absence or inadequate nature of existing legislation; the difficulty identifying those responsible or the fear of reprisals.

WHY DON'T WOMEN REPORT VIOLENCE?

60% of women do not report violence because they have no faith in justice and to make their case known will result in double victimisation without resolving anything.
15% fear reprisals by the perpetrators and an escalation of digital violence
10% do not know where to report violence
9% found their complaint was not recorded
6% are considered to be at fault for their experience



Another statistic that the report highlights is that in 44% of cases, victims/survivors were in the midst of legal proceedings for previous gender-based violence, which enabled them to benefit from protection orders that also protected them against online violence, and also ensured that such violence be addressed with a gender perspective. The report also notes that the handling of online gender-based violence by the media can be victimising and contain symbolic violence. An example of this is when terms are used such as 'leaking' to refer to the non-consensual and intentional dissemination of intimate images. The report concludes that the rending invisible of these practices by the Argentine State results in their continuation.

The November 2017 **Report** compiled by Brazil's Coding Rights and Internet Lab states that the first challenge in tackling online gender-based violence is recognising that certain actions constitute manifestations of violence. Psychological violence cannot be trivialised, nor can it be believed that it begins and ends in the digital domain or is transient. Blaming the woman undermines her legitimacy and holds her back when it comes to reporting violence.

The 2017 EIGE **Report** notes that the Violence against Women Coalition has found that criminal justice authorities seem to be less effective when it comes to acts of online violence and harassment compared to those committed in the 'real world', creating a false dichotomy. Various studies demonstrate women's frustration with the policy, which tends to treat each attack as an independent act rather than considering the cumulative impact of such violence. Moreover, in a survey conducted in 2014 in the United States, more than half of the victims/survivors of cyberbullying did not identify their own experience as constituting an offence.

The UN Special Rapporteur on women, in her June 2018 **Report**, states that some cases of online gender-based violence that have had a media impact, such as the publication of intimate images that led to girls committing suicide, have prompted important debates on the need for legislative reform, including the approval of specific laws. Given the rate at which acts of online gender-based violence can be committed, victims need agile support and remedial solutions from the authorities. Nevertheless, many States lack a comprehensive legal framework. This generates multiple barriers to female victims accessing justice and a sense of impunity for those responsible.

WHAT LEGAL TOOLS ARE AVAILABLE IN THE SPANISH LEGAL SYSTEM TO TACKLE ONLINE GENDER-BASED VIOLENCE?

A. CRIMINAL LAW

The **Spanish Criminal Code (*Código Penal*)** provides for various crimes that punish some forms of online gender-based violence. Some of these forms of violence are not covered in the Criminal Code, such as impersonation on social networks.

1. Threats (Articles 160 to 171 of the Criminal Code)

2. Coercion (Article 172 of the Criminal Code)

3. Stalking (Article 172. 3 of the Criminal Code)
Statutory Law (Ley Orgánica) 1/2015 of 30 March, reforming the Criminal Code by imposition of the Istanbul Convention, introduced a new crime called stalking in Article 172.3. This article covers various types of behaviour that aims to alter everyday life, resulting in constant unwanted contact.

4. Disclosure of information (Article 197 of the Criminal Code)
Article 197.1 and 197.2 punishes various types of behaviour, including the discovery and disclosure of information, or 'doxing'. Article 197.7 punishes the dissemination of intimate images or videos (badly named 'revenge porn'). This article was also imposed by the Istanbul Convention and incorporated by means of Statutory Law 1/2015 of 30 March amending the Criminal Code.

5. Child grooming (Article 183 of the Criminal Code)
Article 183.3 was introduced by Statutory Law 1/2015 of 30 March amending the Criminal Code, and punishes those that, through the internet, by phone or any other form of ICT, contact a child below the age of 16 years and propose arranging a meeting with the aim of committing any of the offences described in articles 183 and 189, provided such a proposal is accompanied by material acts with the intent of holding such meeting.

6. Defamation and slander (Articles 205 to 208 of the Criminal Code)

7. Computer damage or sabotage (Article 264.2 of the Criminal Code)

8. Crimes against moral integrity (Article 173 of the Criminal Code)
This crime provides for various forms, the first of which is degrading treatment, which involves severely undermining someone's moral integrity. Its second section covers this degrading treatment in the context of an intimate (former) partner. Its fourth section covers minor acts of humiliation, also in the context of an intimate (former) partner. Slander and minor acts of humiliation outside of this intimate context have been removed from the Criminal Code through the amendment implemented by Statutory Law 1/2015, which redirects these to civil legislation.

9. Hate speech (Article 510 and 22.4 of the Criminal Code)
Statutory Law 1/2015 amended Article 510 of the Criminal Code as well as the aggravating circumstances of Article 22.4 through imposition of the Istanbul Convention. The amendment entails the incorporation of gender-based discrimination in both articles. With regard to the aggravating factor of gender, since 2017, some sentences have been starting to apply it in generic offences such as homicide or murder.

With regard to previous offences, some demand a series of requirements in order to instigate a criminal investigation, such as the requirement to file a complaint or even a complaint by the offended party. In the case of defamation and slander, the undertaking of a previous civil conciliation procedure is required, and this increases the financial cost of the dispute. The average processing time of legal proceedings is also a disincentive. Another noteworthy factor is that the new legal provisions introduced through the imposition of the Istanbul Convention, designed to protect women from gender-based violence, have been drafted in a neutral fashion. This implies that men and women can be condemned for such behaviours, an example of this being stalking.

Given that the national law on gender-based on violence is limited to the context of the intimate (former) partner, online violence against other women is not seen as gender-based violence. Going back to the example of stalking, the punishment is increased if it is committed within the context of an intimate partner or former partner, but in all other cases the punishment is the same whether the crime is committed by a man or a woman. This represents a failure to appreciate the gender discrimination factor in online violence that is committed outside of the (former) partner context. Another aspect to consider is that researching the rulings issued to date show that in cases of a conviction, the women affected are rarely awarded damages.

Often, the content is removed at the end of legal proceedings, after having been online for years. Sometimes, the content has been shared so many times it is technically impossible to remove it. An example of this is the case of an Italian girl who took her own life in 2016 as a result of the dissemination of a sex tape by her former partner, which was shared nationally. Today, this content still remains available online.

AND WHAT ABOUT PROTECTION MEASURES?

One of the first laws to consider is **Act 4/2015 on the *Estatuto de la Víctima* (Statute of Victims of Crime)**, which for the first time recognises a series of rights of victims of any crime, and which also applies to women affected by online gender-based violence.

On the other hand, protection measures are governed by the ***Ley de Enjuiciamiento Criminal* (Criminal Procedure Law)**. Article 282 of this law provides that the Judicial Police must verify crimes that are reported and obtain evidence of the crime so that it does not disappear. The specific circumstances of the victims/survivors must also be assessed in order to provisionally determine which protection measures should be adopted in order to ensure they are adequately protected while awaiting the final decision of the judicial authority.

The **Ley de Criminal Procedure Law**, in Article 13, also provides for the undertaking of preliminary enquiries, which involve recording any evidence of the crime that could disappear, identifying the offender and protecting persons affected by the offence, which may including the granting of the precautionary measures set out in Article 544 bis or the protection order described in Article 544 third of this law. Article 544 bis of the Criminal Procedure Law covers protection against any person involved in investigations of certain crimes (those detailed in Article 57 of the Criminal Code). This generic protection can include a restraining order. If the protection of the person's rights or freedoms is not respected, this can be considered a crime of breach of the protection measure. While not specifically covered by the **Criminal Procedure Law**, the Court may be asked to remove or prevent access to digital content as a precautionary measure while the case is being investigated and awaiting trial. The decision as to whether or not to adopt these precautionary measures can be appealed.

Within the scope of intimate (former) partner and domestic (intrafamily) gender-based violence, the protection measure set out in Article 544.3 of the Criminal Procedure Law can be implemented in those cases where the victim/survivor is deemed to be at risk, enabling measures that include restraining orders, among others, to be applied.

At the end of legal proceedings, upon a final conviction, in addition to the punishments for each offence, for certain crimes (Article 57), the Criminal Code allows the enforcement of a restraining order to be requested as an ancillary penalty for a period no greater than 10 years for serious offences, or 5 years for less serious offenses. Ancillary penalties are compulsory in crimes committed in the context of an intimate (former) partner.

B. CIVIL LAW

The **Statutory Law 1/1982 of 5 May on the civil protection of the right to honour, personal and family privacy and one's own image**, protects against unlawful invasion of privacy. Such invasion is conceived from a 'reputational' and 'individual' perspective, which does not take into account the discriminatory or structural component of gender-based violence. When considering the request for protection, the Court will determine the unlawfulness of the invasion of privacy and the corresponding award for damages. It must also disclose the ruling and remove the unlawful content from the internet.

Article 7 specifies what is considered unlawful invasion of privacy, including but not limited to:

// The disclosure of facts about a person or family's private life that affects their reputation and good name.

// The disclosure of private information about a person or family known through the professional or official activities of the person disclosing it.

// The capture, reproduction or publication of images of a person in places or moments of his private life.

// The use of a person's name, voice or image for advertising or commercial purposes or similar.

// The accusation of facts or passing of value judgements through actions or expressions that in anyway harm the dignity of another person, undermining their reputation.

// The use by the person convicted in the final sentence of the crime to obtain public notoriety or obtain financial gain, or the disclosure of false information regarding criminal acts when doing so undermines the dignity of victims.

Likewise, this law provides for the adoption of urgent precautionary protection measures. It must be taken into consideration that in the event that the ruling refuses the request for the protection of honorary rights, the person who requested it must pay the legal costs to the other party (fees for attorneys, lawyers and any expert witnesses).

WHAT CHANGES DOES THE STATE PACT BRING?

The **June 2017 Pacto de Estado en materia de Violencia de Género (State Pact against Gender Based Violence** has provided for a series of measures that will have an impact on online gender-based violence, such as "to agree, with the National Armed Forces and Security Agencies, telecommunication companies and main digital content providers, a system of coordination, cooperation and co-regulation to remove potentially harmful references online that promote violence against women". This violence includes gender-based, physical, psychological and sexual violence and harassment.

It also envisages 'perfecting the definition of crimes in the digital context', and evaluating the possibility of amending Article 172.3 of the Criminal Code so that it covers behaviours, such as impersonation, that currently are not covered by the Criminal Code. It also provides that 'defamation and slander via social networks will not be considered within the context of gender-based violence, as just a misdemeanour'. On the subject of measures to provide assistance and protection to victims/survivors, it envisages 'facilitating the right of victims to online data expiry'.

OBLIGATIONS OF STATE PARTIES AND THE PRINCIPLE OF 'DUE DILIGENCE'

OBLIGATION TO PREVENT, PROTECT, INVESTIGATE, JUDGE, PUNISH, REMEDY AND OFFER ASSURANCES OF NON-REPITITION.

The **Cedaw Convention** in 1979 coined the basic 'principle of due diligence', which comprises the effective and proactive obligation of the State to adopt measures to prohibit discrimination against women, whether they were enforced by individuals, organisations, companies or the State itself. Its compulsory nature even included the adoption or derogation of discriminatory laws, uses and practices. Another key measure is to support those (wrongly) termed 'positive discrimination' measures.

The CEDAW Committee stipulated the obligations of State parties in a **2017 Recommendation**. This determines accountability for actions and omissions in the public and private sphere, whether committed by the State or individuals, in cases where the State does not adopt all necessary measures to prevent acts of gender-based violence against women; cases where the authorities are aware or should be aware of the risk of such violence; or for the fact that they do not investigate, judge and punish those responsible or offer remedies to victims/survivors of these acts, negligence that constitutes the tacit permission or incitement to commit acts of gender-based violence against women. These shortcomings or negligence constitute violations of women's human rights.

These obligations include legislative, executive and judicial authority and include the obligation to properly investigate and sanction inefficiency, complicity and negligence by public authorities responsible for recording, preventing or investigating this violence or for caring for victims/survivors. The recommendation also calls for the adoption of measures to eradicate customs and practices that constitute discrimination against women. All measures must be applied by focusing on the victim/survivor, recognising women as rights holders and promoting their capacity to act and autonomy.

At the legislative level, it envisages:

// that all forms of gender-based violence against women, which amount to a violation of their physical, sexual or psychological integrity, are criminalised and introduce or reinforce legal sanctions commensurate with the gravity of the offence, as well as civil remedies;
// that legal systems protect victims/survivors and ensure that they have access to justice and to an effective remedy;
// the repeal of all legal provisions that allow, tolerate or condone any form of gender-based violence and prevent or discourage women from reporting such violence.

At the preventive level, it envisages:

// the adoption and implementation of measures to address the underlying causes of gender-based violence, particularly patriarchal attitudes and gender stereotypes, inequality in the family and the neglect or denial of women's rights, and to promote the empowerment, capacity to act and voices of women;
// addressing and eradicating established gender stereotypes, prejudices, customs and practices that condone or promote gender-based violence and underpin the structural inequality between women and men. It also provides for the mandatory, recurrent and effective training for members of the judiciary, lawyers and law enforcement officers, including forensic medical personnel, legislators and healthcare professionals.

At the protection level, it envisages:

// the provision of appropriate and accessible protective mechanisms to prevent further acts of violence, without the precondition that victims/survivors must report it;
// ensuring their privacy and security;
// immediate risk assessment;
// and, where applicable, the granting of protection orders against perpetrators, including sanctions for non-compliance.

At the prosecution and punishment level, it envisages:

// ensuring effective access for victims/survivors to courts and that the authorities adequately respond in a fair, impartial, timely and expeditious manner and impose appropriate penalties. Fees or court charges should not be imposed on victims/survivors. Procedures should empower victims/survivors and the expertise of specially trained professionals should be available.

At the remedial level, it envisages:

// effective reparation to victims/survivors;
// access to health services for a complete recovery and guarantees of non-recurrence;
// that priority should be given to victims'/survivors' capacity to act, wishes, decisions, safety, dignity and integrity.

In the European context, the **2011 Istambul Convention** also provides for the principle of 'due diligence' and similar obligations in order to ensure the right of women to live free from violence in the public and private sphere. Its provisions suggest specific measures that implore the private sector to establish guidelines and self-regulatory standards to prevent gender-based violence.

The general obligations of State parties must take into consideration the relationships between victims/survivors, those responsible for the offences and their broader social context. These will be aimed at avoiding secondary victimisation and empowering and responding to the specific needs of vulnerable people. As with the CEDAW recommendation, a complaint does not need to have been filed in order to access protection measures.

The Convention also requires the Criminal Code to include intentional psychological violence that severely threatens women's psychological integrity by means of coercion or threats. There must also be the crime of harassment, when committed intentionally, by undertaking repeated and threatening behaviour toward the woman which leads her to fear for her safety, and sexual harassment. These crimes will be punished regardless of any existing relationship between the victim and offender.

The Convention also covers obligations, during legal proceedings, based on the human rights and gender perspective, to ensure an effective investigation and proceedings. It provides for a timely and effective response by police forces by offering adequate protection and the gathering of evidence. It also provides for the granting of emergency restraining orders, prioritising the safety of victims/survivors. It also calls for the safeguarding of the rights and interests of victims/survivors in all phases of legal proceedings, thereby protecting them from the risk of intimidation, reprisals and further victimisation.

The UN Special Rapporteur on women, in her **July 2018 report**, notes that although basic women's human rights instruments predate the development of the internet and ICT, they are clearly applicable to digital environments.

The Rapporteur recognises the 'principle of due diligence' and breaks it down into the following key areas:

1. Prevention
Includes measures to raise awareness of the fact that violence against women and girls facilitated by ICT falls under the umbrella of gender-based violence, and provides for the provision of information on the services and legal protection available.

2. Protection
Addresses the removal of harmful content and immediate legal action in the form of court orders and prompt intervention by internet intermediary companies. In addition, it includes the obligation to act, even when no woman has filed a complaint, for example in the case of online forums that promote violence against women.

3. Proceedings
Comprises the investigation and initiation of legal proceedings against offenders. Law enforcement agencies often trivialise the violence and blame victims/survivors, leading to under-reporting. Procedures should empower victims/survivors and the expertise of specially trained professionals should be available.

4. Punishment
Implies the duty to punish those responsible for their crimes, by means of sanctions that are necessary and proportionate to the offense. The certainty of appropriate punishment sends the message that gender-based violence committed via ICT will not be tolerated.

5. Restoration and redress
Include compensation to cover quantifiable losses, damages and non-quantifiable losses. It also includes the immediate removal of harmful content, as well as forms of restoration, rehabilitation, satisfaction assurances of non-recurrence, combining measures that are symbolic, material, individual and collective, depending on the circumstances and demands of the victim/survivor.

ACCESS TO JUSTICE BY WOMEN WHO EXPERIENCE ONLINE GENDER VIOLENCE

The CEDAW Committee, in its **2010 Recommendation**, analyses the performance of the responsibilities of State parties with regard to the provision of protection from discrimination by public authorities, including the judiciary. Its subsequent **2015 Recommendation** on women's access to justice examines the factors that prevent or hinder it. The right of access to justice is multidimensional, and covers the justiciability, availability, access, good quality, provision of legal resources to victims/survivors, and the accountability of justice systems. Barriers to accessing justice are considered to be persistent human rights violations. These include gender stereotypes, discriminatory laws, intersectional procedures, and evidentiary practices and requirements. Also considered a barrier are judicial mechanisms that are not financially, economically, socially and culturally accessible to all women.

State parties are responsible for removing social and cultural barriers, including gender stereotypes, which prevent women from exercising and defending their rights and prevent them from accessing effective legal tools. Human rights defenders and their organisations must also be able to access justice.

With regard to the quality of justice systems, the CEDAW Committee recommends that State parties:

// Ensure that justice systems adhere to international standards as well as to international jurisprudence;
// Adopt indicators to measure women's access to justice;
// Provide a sustainable, gender-sensitive resolution to disputes for all women;
// Ensure that evidentiary rules, investigations and other procedures are impartial and not influenced by gender biases or stereotypes;
// When necessary to protect women's privacy, safety and other human rights, ensure that, in a manner consistent with the principle of a fair trial, testimony can be given remotely. The use of pseudonyms or other measures to protect women's identities should be permitted, and the capture and transmission of images of the women should be prohibited;
// Protect women from threats, harassment and other forms of harm during and after legal proceedings.

With regard to the accountability of justice systems, the CEDAW Committee recommends that State parties:

// Monitor women's access to justice, including the periodic auditing/review of the autonomy, efficiency and transparency of the judicial bodies that take decisions affecting women's rights;
// Ensure that discriminatory practices and acts committed by justice professionals are effectively addressed through disciplinary measures;
// Create a specific entity to receive complaints, petitions and suggestions with regard to all personnel supporting the work of the justice system;
// Conduct and facilitate qualitative studies and critical gender analyses of all justice systems.

Another important section of the Recommendation discusses gender stereotypes and biases within the justice system, which have far-reaching consequences for women's full enjoyment of their human rights. These distort perceptions and give way to decisions based on pre-conceived beliefs and myths, rather than facts. Often, the judiciary adopts rigid standards on what it considers appropriate behaviour by women, and punishes women who do not conform to these stereotypes. The establishment of stereotypes also affects the credibility of women's statements, arguments and witness statements.

These stereotypes may lead to the judicial authority incorrectly interpreting laws, or applying them inadequately. This can result in perpetrators not being held responsible, reinforcing the culture of impunity. In all areas of law, stereotypes compromise the impartiality and integrity of the justice system, which in turn leads to the denial of justice, including the revictimisation of complainants. They exist in all stages of investigations and proceedings, and, lastly, may influence the ruling.

With regard to the criminal justice system, among other points the CEDAW Committee recommends that State parties:

1. Exercise due diligence to prevent, investigate, punish and provide reparation for all crimes committed against women, whether by State or non-State actors;
2. Protect women against secondary victimisation in their interactions with law enforcement and judicial authorities;
3. Create a supportive environment that encourages women to claim their rights, report crimes committed against them and actively participate in criminal justice processes;
4. Use a confidential and gender-sensitive approach to avoid stigmatisation during all legal proceedings;
5. Review rules on evidence and their implementation in cases of violence against women, to ensure that the evidentiary requirements are not overly restrictive, inflexible or influenced by gender stereotypes;
6. Avoid undue delays in applications for protection;
7. Develop protocols for police, for the collection and preservation of forensic evidence, and train sufficient numbers of police and legal and forensic staff to competently conduct criminal investigations;
8. Review and monitor all criminal procedures to ensure that they do not directly or indirectly discriminate against women.

OBLIGATION TO RECORD, STATISTICALLY ANALYSE AND INVESTIGATE ONLINE GENDER-BASED VIOLENCE

One of the priorities regarding online gender-based violence should be its recording and analysis, order to have a deeper understanding of this phenomenon and be able to develop effective public policies in this regard. In Spain, the ***Observatorio Estatal de Violencia sobre la Mujer*** **(National Observatory on Violence against Women)** is the body responsible for compiling reports, studies and action plans concerning gender-based violence. The **Ley para la igualdad efectiva de mujeres y hombres (Gender Equality Law) 2007** obliges public authorities to:

// systematically include the sex variable in statistics, surveys and data collection;
// establish and include new statistical indicators that enable a better understanding of the differences in the values, roles, situations, conditions, aspirations and needs of women and men, their expression and interaction with reality;
// design and introduce the necessary indicators and mechanisms to enable an understanding of the incidence of other variables, the occurrence of which gives rise to instances of multiple discrimination in different areas of intervention.

The recent **State Pact** from June 2017 lays down the legal obligation to regularly collect and provide detailed and secondary statistical data on all forms of violence against women covered in the Pact. With regard to conducting studies, it provides for setting up a shared database and standardising victim data (Ministries of Justice, Internal Affairs, Health, Social Services and Equality). It must be taken into account that the work of the Ministries of Justice and Internal Affairs relates to crime, while that of the Ministry of Health, Social Services and Equality employ sociological concepts.

As can be seen, to date, the way in which online gender-based violence is reflected in statistics is lacking. On the one hand, the existence of general offences is recorded, according to the legal rights affected or the type of offence, while on the other hand, the recording of crimes committed within the context of gender-based violence is limited to that involving an intimate (former) partner. As such, it is not possible to evaluate online gender-based violence against all women or break them down by the type of violence, relationship with the offenders, reporting rates, protection measures, sentences, and any remedies adopted.

By way of example, it is useful to consult the **2015 Macrosurvey on Violence against Women** by the *Delegación Gobierno para la Violencia de Género* (Government Office for Gender Violence), the **2017 Annual Report of the Attorney General's Office**, el **report on *La violencia sobre la mujer en la estadística judicial: primer trimestre de 2018* (Violence against women in judicial statistics: first quarter of 2018)** by the Observatory on domestic and gender-based violence of the *Consejo General del Poder Judicial* (General Council of the Judiciary), or the website of the ***Instituto Nacional de Estadística* (National Statistics Institute)**. Furthermore, risk analyses often do not consider the risk associated with online gender-based violence. In this regard, we can review the **October 2018 report of the *Sistema de Seguimiento Integral en los casos de Violencia de género (Sistema VioGén)* (Comprehensive Monitoring System for Gender-based Violence)** of the State Secretary for Social Security of the Ministry of Internal Affairs.

The CEDAW Committee, in its **Recommendation no. 9 of 1989** on statistics, had already pointed out the importance of understanding the actual situation of women. In its subsequent **2010 Recommendation** on State party obligations, it mentions the responsibility to create and continuously improve its statistical databases and to perform more in-depth analyses of all forms of discrimination against women in general and, in particular, those belonging to certain vulnerable groups.

In its subsequent **2017 Recommendation no. 35** on gender-based violence against women, it envisages the establishment of a system to regularly collect, analyse and publish statistical data on the number of reports of all forms of gender-based violence, including violence committed through the use of ICT, the relationship with the offender, the relationship with other interrelated forms of discrimination, the number and type of protection orders issued, rates of rejection and withdrawal of complaints, proceedings and convictions, and the time needed to resolve the cases. Data analysis should enable the identification of errors in protection and be used to improve prevention measures.

The process for collecting and storing data on gender-based violence should adhere to international standards and assurances, including data protection laws. The use of statistics should adhere to international standards on the protection of human rights and their ethical principles.

In the European context, the 2011 **Istambul Convention** requires Member States to gather detailed statistical data at regular intervals on all forms of violence. It also lays down the requirement to support the investigation into its deeper causes and effects, its frequency and conviction rates, as well as the effectiveness of adopted measures. Member States must commit to making the information obtained available to the Group of Experts on Action against Violence against Women and Domestic Violence (GREVIO) and the general public.

The 2017 **Report of the European Institute for Gender Equility** (EIGE) warns that data on cyber violence against women and girls in the European Union are lacking. The best information available at a European level comes from the **EU-wide survey on violence against women**, conducted in 2014 by the European Union Agency for Fundamental Rights (FRA), which included questions on cyber-harassment and cyberbullying. Given that in most Member States, the different forms of cyber violence against women and girls are not considered offences, data from the police or legal institutions on this phenomenon are scarce. In those Member States where forms of cyber violence are considered an offence, the data collected are not broken down by the gender of the victim/survivor and the perpetrator, nor by their relationship, which limits the use of such data. The EIGE recommends investigation in the following areas:

// Evaluating the severity of the harm suffered by women and girl victims/survivors of various forms of cyber violence, and the repercussions in their daily lives;
// Good practice in the responses of the police and judicial systems to cyber violence against women and girls, including from the perspective of the victims;
// Identification and analysis of risk factors and risk assessment procedures in order to prevent harm and revictimisation.

RECOMMENDATIONS FOR THE DEVELOPMENT OF PUBLIC POLICIES AND LEGISLATIVE MEASURES

Based on the above, and in line with the contributions of various reference groups around the world in tackling online gender-based violence, public policies should focus on the following:

A) DEVELOPMENT OF PUBLIC POLICIES

// Acknowledge the diversity among women (age, culture, sexual orientation), as well as their multiple dimensions;
// Think of online gender-based violence as a continuum of other forms of violence against women, rather than as a separate issue;
// Devise a comprehensive definition of online gender-based violence;
// Consider the specific characteristics that ICT gives to these forms of violence, such as replicability, ease of use of content searches and the impossibility of removing content;
// Foster the adoption of comprehensive tools to ensure women's safety, protect their privacy and enhance their freedom of expression;
// Question an eminently practical approach in the criminal code, and consider other responses, such as administrative processes;
// Legislative measures, whether reformed or new, by themselves, are insufficient. Solutions must have a positive approach and include legal and non-legal measures;
// Anonymity or encryption must not be suppressed or restricted;
// Improve the reporting system for online gender-based violence, which will enable a more in depth understanding of this phenomenon;
// Consider women's access to the internet not only as users, but also as technological innovators;
// Create public campaigns that promote the condemnation of online gender-based violence, particularly directed at the male population, which is largely responsible;
// Support the formation of online feminist networks and digital security strategies for women and other vulnerable groups;
// The effectiveness of the legislative response is not achieved only with specific legislation on online gender-based violence, but also by ensuring the general access to justice for victims/survivors, while at the same time prioritising reparation and restoration over criminalisation;

// Given the particular nature of online gender-based violence, it is necessary to ensure the ability to respond immediately with urgent investigations, as well as the granting of protection orders and the development of emergency protocols for removing content, in line with due process.
// Ensure that existing or new legal frameworks adequately protect women's freedom of expression and privacy. Any restrictions on the freedom of expression should be necessary, concise and proportionate;
// Legislation must take into consideration women's and girls' physical autonomy, self-determination, freedom of expression and the right to participate in public debate;
// The creation or reform of legislation on the internet must involve extensive consultations with civil society organisations that work to promote women's rights;
// Training police forces, the judiciary and other legal practitioners on the gender perspective to be able to measure the severity of online gender-based violence, respond quickly and understand new technologies;
// Explore whether current laws permit interpretations that may extend the guarantees of women who suffer online gender-based violence;
// Evaluate the legal tools available, taking into account their ability to provide immediate protection and consider their cost and average duration;
// Adapt the wording of complaint forms so that they include psychological violence, and risk assessment adapted to online gender-based violence;
// The rapid preservation of technological evidence, including metadata, and the drafting of expert computer forensics reports at no cost to complainants.

C) DEVELOPMENT OF MEASURES TARGETING INTERNET INTERMEDIARY PLATFORMS

// Encourage internet intermediary companies to guarantee data security and privacy, incorporating them as a default setting;
// Companies have the responsibility to respect human rights, including the prevention of gender-based violence. Governmental regulation and the imposition of obligations on companies must also respect the human rights framework by employing necessary and proportionate measures;
// Encourage public debate on the role of companies and their internal policies or terms of use with regard to non-consensual content;
// Ensure the transparency of internal content removal policies and facilitate reporting mechanisms. Users should be able to find out and appeal the decision to remove content.

BIBLIOGRAPHY AND REFERENCES

A) LEGISLATION

1. Spanish Royal Decree of 14 September 1882, of the Criminal Procedure Code
2. Convention on the elimination of all forms of discrimination against women, 1979
3. Statutory Law 1/1982, of 5 May, on civil protection of the right to freedom from injury to honour, personal and family privacy and to self-image
4. Statutory Law 10/1995, of 23 November, on the Criminal Code
5. Directive 2000/31/EC of the European Parliament and of the Council of 8 June
6. Act 34/2002, of 11 July, on services of the information society and electronic commerce
7. Statutory Law 1/2004, of 28 December, on Comprehensive Protection Measures against Gender-based Violence
8. Statutory Law 3/2007, of 22 March, for the effective equality of women and men
9. Council Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia through criminal law
10. Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive)
11. Council of Europe Convention on preventing and combating violence against women and domestic violence
12. Act 4/2015, of 27 April, on the Charter of victim's rights (*Estatuto de la víctima del delito*)
13. Spanish Royal Decree 9/2018, of 3 August, on urgent measures for the implementation of the State Pact against gender-based violence

B) RECOMMENDATIONS AND REPORTS FROM INTERNATIONAL BODIES

14. General Recommendation no. 9, CEDAW, 1989
15. General Recommendation no. 19, CEDAW, 1992
16. Declaration on the Right and Responsibility of Individuals, Groups and Organs of Society to Promote and Protect Universally Recognized Human Rights and Fundamental Freedoms, 1999
17. General Recommendation no. 28, CEDAW, 2010
18. UN Special Rapporteur Report on the Right to Freedom of Opinion and Expression (Frank la Rue), 2011
19. Resolution 17/4 of the United Nations Human Rights Council (UNHRC) on Human rights and transnational corporations and other business enterprises, 16 June 2011
20. United Nations Human Rights Council (UNHRC), Report by the Working Group on the issue of discrimination against women in law and in practice', 2013
21. Resolution of the United Nations Human Rights Council (UNHRC) on the Role of Freedom of Opinion and Expression in Women's Empowerment, 2016
22. Recommendation CM/Rec(2014) of the European Parliament titled 'Guide to human rights for Internet users', 2014
23. UN Special Rapporteur report on the promotion and protection of the right to freedom of opinion and expression, Frank de la Rue, 2011
24. General Recommendation no. 33 of the CEDAW Committee on women's access to justice, 2015
25. Resolution of the United Nations Human Rights Council (UNHRC) on the promotion, protection and enjoyment of human rights on the Internet, 2016
26. General Recommendation no. 35, CEDAW, 2017

27. Report of the United Nations Human Rights Council (UNHRC), "Promotion, protection and enjoyment of human rights on the Internet: ways to bridge the gender digital divide from a human rights perspective", 2017
28. UN Special Rapporteur report on violence against women, its causes and consequences , 'Online violence against woman and girls from a human rights perspective', 2018
29. Resolution of the United Nations Human Rights Council (UNHRC), 'Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts , 2018

C) STUDIES AND REPORTS FROM OTHER ENTITIES

30. Report from the Association for Progressive Communications (APC), 'EROTICS, Sex, Rights and the Internet, 2011
31. ACSUR - Las Segovias Compendium of Monographs in collaboration with Donestech, 'Gender, ICT and activism", 2013
32. Take Back the Tech, Map it!, 2014
33. Report from the Association for Progressive Communications (APC), 'Internet intermediaries and online violence against women: user policies and redress framework of Facebook, Twitter and YouTube', 2014
34. EU-wide survey on violence against women by the European Union Agency for Fundamental Rights, 2014
35. Report of the Association for Progressive Communications (APC), 'End violence: women's rights and safety online from impunity to justice: improving corporate policies to end technology-related violence against women', 2015
36. Report of the Women's Legal and Human Rights Bureau, Inc., 'From impunity to justice: domestic legal remedies for cases of technology-related violence against women', 2015
37. Report of the Association for Progressive Communications (APC), 'End violence: woman's rights and safety online analysis of incidents of technology-related violence against woman reported on the "'Take back the Tech"', 2015
38. Macrosurvey on violence against women, 2015
39. Internet Governance Forum (IGF) 2015: Best Practice Forum (BPF) on Online Abuse and Gender-Based Violence Against Women
40. Feminist Principles of the Internet, 2016
41. UNESCO report, 'Human rights and encryption' , 2016
42. Report of the European Institute for Gender Equality (EIGE), 'Cyber violence against women and girls', 2017
43. Luchadoras compiled a report entitled 'Online violence against women in Mexico', 2017
44. Report of the association Coding Rights and Internet Lab, 'Online gender-based violence: diagnosis, solutions and challenges', 2017
45. Report of the Association for Civil Rights, in collaboration with the Digital Activism Foundation, 'State of online gender-based violence against women in Argentina', 2017
46. Report of the Association for Progressive Communications (APC), 'Online gender-based violence: a submission from the Association for Progressive Communications to the United Nations Special Rapporteur on violence against women, its causes and consequences', 2017
47. Report by Donestech, 'Social networks from a gender perspective: a guide to know and counteract online gender-based violence', 2017
48. Report by Amnesty International '#ToxicTwitter, Violence and abuse against women online', 2018

D) OTHER RELEVANT LINKS

49. **Macro survey on violence against women**, 2015
50. **Annual Report of the Attorney General's Office**, 2017
51. **National Statistics Institute Website**, 2017
52. **State Pact on Gender-based Violence**, 2017
53. **Report by the Comprehensive Monitoring System for Gender-based Violence (Sistema VioGén)**, 2018
54. **Report 'Violence against women in judicial statistics: First quarter of 2018'**