Online gender-based violence against women and girls

Guide of basic concepts

OAS | CICTE

OAS | CIM | MESECVI

Credits

Luis Almagro
General Secretary
Organization of American States (OAS)

Arthur Weintraub
Secretary for Multidimensional Security
Organization of American States (OAS)

Alison August Treppel
Executive Secretary
Inter-American Committee Against Terrorism (CICTE)

Alejandra Mora Mora
Executive Secretary
Inter-American Commission of Women (CIM)

OAS Technical Team

Cyber-Security Program
Kerry-Ann Barrett
Mariana Cardona
Gabriela Montes de Oca Fehr

Inter-American Commission of Women /
Follow-up Mechanism of the Convention of Belém do Pará
Luz Patricia Mejía Guerrero
Alejandra Negrete Morayta

Author
Katya N. Vera Morales

Design and Layout
Michelle Felguérez

With the financial support of the Government of Canada Canada

OAS Cataloging-in-Publication Data

Online gender-based violence against women and girls : Practical self-protection handbook: digital security tools and response strategies / [Prepared by the General Secretariat of the Organization of American States].
v. ; cm. (OAS. Official records ; OEA/Ser.D/XXV.25)
ISBN 978-0-8270-7307-4
1. Girls--Violence against. 2. Women--Violence against. 3. Computer security. 4. Computer crimes. 5. Girls--Crimes against. 6. Women--Crimes against. I. Title: Practical self-protection handbook: digital security tools and response strategies. II. Inter-American Commission of Women. III. Inter-American Committee against Terrorism. IV. OAS/CICTE Cyber Security Program. V. Organization of American States. Secretariat for Multidimensional Security. VI. Vera Morales, Katya N. VII. Series.
OEA/Ser.D/XXV.25

Content

This publication was made possible through support provided by the United States Department of State, under the terms of Award No. SLMQM20GR2380. The opinions expressed herein are those of the author(s) and do not necessarily reflect the views of the United States Department of State.

Introduction

Gender-based violence facilitated by new technologies is a phenomenon that increasingly affects the privacy and safety of women and girls in and out of cyberspace. Research on the topic suggested that **women are disproportionately victimized by certain types of cyberviolence compared to men** (UN-SRVW, 2018; EIGE, 2017). According to a study published in 2015 by the United Nations Broadband Commission for Sustainable Development, 73 percent of women had experienced some form of gender-based violence online, while 61 percent of attackers were men (UNBC, 2015). Other sources note that 23 percent of women have experienced online harassment at least once in their life and that an estimated 1 in 10 women has experienced some form of online violence since the age of 15 (UN-SRVW, 2018, para. 16; EIGE, 2017: 3; AI, 2017).

Moreover, as multiple sources have found[1], this violence has been exacerbated by the mobility restrictions and lockdown measures imposed as a result of the COVID-19 pandemic: as more women and girls turn to digital spaces, gender-based cyber-violence against them increases (UN Women; CIM, 2020; Digital Rights, 2020).

This phenomenon is visible in a scenario with multiple challenges. Information on cyberviolence against women is still scarce. Very little is known about the actual percentage of victims and the prevalence of the damage it causes (EIGE, 2017). In addition, to date there is no regionally or internationally agreed definition of online gender-based violence, nor precise terminology[2]. There is significant disparity between the responses of States and international agencies and, in general, a lack of adequate legal frameworks to protect victims.

Bearing this context in mind, the Cybersecurity Program of the Inter-American Committee against Terrorism (CICTE), in partnership with the Inter-American Commission of Women (CIM), has developed this guide aimed at public institutions, professionals, and stakeholders in the cybersecurity sector. It addresses the basic concepts for understanding the characteristics and impact of online gender-based violence (Part 1), a descriptive list of the types of behavior that can be considered manifestations of digital gender-based violence (Part 2), and a brief overview of the latest developments in this regard in the Latin American region, with some reflections on measures that authorities could take to prevent and combat this form of gender-based violence (Part 3).

This guide is part of the publication *Online gender-based violence against women and girls. A guide to basic concepts, digital safety tools and response strategies,* which also provides more information about preventive measures and digital safety tools that can be adopted against attacks and acts of gender-based violence online.

[1] ONU Mujeres (2020). Online and ICT facilitated violence against women and girls during COVID-19. Available at: https://www.unwomen.org/en/digital-library/publications/2020/04/brief-online-and-ict-facilitated-violence-against-women-and-girls-during-covid-19 see also: Inter-American Commission of Women (CIM) (2020), COVID-19 in Women's Lives: Reasons for Acknowledging Differentiated Impacts." Available at: http://www.oas.org/es/cim/docs/ArgumentarioCOVID19-ES.pdf

[2] As noted by the UN Special Rapporteur on violence against women, there is still no consensus on a term for referring to this form of violence. The expressiom "information and communication technology (ICT)-facilitated violence against women" is perhaps the most inclusive, as it encompasses the vast range of behaviors that this form of violence can take. However, in keeping with common usage, the terms "ICT-facilitated violence," "online violence against women," "digital violence," and "cyberviolence against women" will be used interchangeably in this publication.

Part one

Basic concepts:

RECOGNIZING DIGITAL VIOLENCE IS THE FIRST STEP IN COMBATING IT

A

What is online gender-based violence against women?

Basic elements of online violence against women:

01 It is not anything new. It is part of a context of gender-based discrimination and systemic violence against women that appears in all aspects of their lives.

02 It is not disconnected from violence offline: it is part of a continuum of multiple, recurring, and interrelated forms of violence against women and girls that is now flowing in the online-offline world and cuts across it.

03 It entails diverse human rights violations against women and girls.

04 It is a dynamic expression encompassing highly diverse practices of violence facilitated or reconfigured by information and communication technologies (ICTs).

05 It causes victims psychological, physical, sexual and/or economic harm and suffering and affects families, societies and the world at large.

Online violence against women is not an isolated phenomenon but is **situated in a broader social context of gender inequality and discrimination against women and girls.** Therefore, in order to understand digital violence, it is crucial that we first stop to analyze what gender-based violence is, since the assults and attacks that women endure in their online interactions are nothing more than an extension of the violence that has affected them for many years in all spheres of their lives.

What is gender-based violence against women and girls?

The Convention of Belém do Pará defines violence against women as "any act or conduct, based on gender, which causes death or physical, sexual or psychological harm or suffering to women, whether in the public or the private sphere" (Article 1).

Gender-based violence is "**violence that is directed against a woman because she is a woman or that affects women disproportionately**" (CEDAW Committee, General Recommendation 19, para. 6).

Gender-based violence against women is rooted in stereotypes and prejudices about the attributes and characteristics that men and women possess and in expectations of the social roles that both are supposed to play (for example, that women are the only ones who do housework, that they lack sufficient authority to hold managerial positions, or that they are naturally weak. These sociocultural patterns place women in an **inferior or subordinate position with respect to men** and are conducive to their discrimination, which elements are the main drivers of violence directed at them (MESECVI, 2017, para. 37).

It is important to emphasize that violence operates in synergy with gender inequality and not only as a consequence of the latter, but also as a social mechanism that seeks to keep women in a situation of disadvantage. This means that violence is often used to "punish" or "correct" women whose attitudes or activities supposedly go against what society expects of them (MESECVI, 2017, para. 36).

The United Nations has pointed out that violence against women is a pervasive problem in all countries of the world, as well as a widespread, systematic human rights violation that enjoys a high degree of impunity.

Women and girls experience gender-based violence over the years in all offline and online spaces where they are present and participate, whether at home, at school, at work, on public roads, in politics, in the media, in sports, in public institutions, or on social networks (CEDAW Committee, General Recommendation 35). This violence knows no borders; it is directed against all women for the simple fact that they are women and **has a greater impact on certain groups of women because they suffer forms of intersectional discrimination,** as in the case of indigenous, migrant, disabled, lesbian, bisexual and transgender women, among others (MESECVI, 2017).

One of the greatest milestones for women has been to achieve recognition that **violence committed against them is not a private problem**, but a matter of public interest and a violation of human rights recognized in international instruments and national laws that prescribe the obligation for States to prevent, address, investigate, redress, and punish it (Edwards, 2010). In the case of the Inter-American system, the right of women to live a life free of violence is recognized in the Inter-American Convention on the Prevention, Punishment, and Eradication of Violence against Women (Convention of Belém do Pará), the first treaty on the subject that elevated the fight against gender-based violence against women to a problem of regional concern[3].

What is online violence against women?

Although several civil society organizations, academia, and international agencies have made significant efforts to clarify what online gender-based violence against women is, as noted at the beginning, so far no consensus has been reached on its definition, nor is there a consolidated terminology (Van Der Wilk, 2018).

In 2015, the Association for Progressive Communications (APC), which has been working on this issue for over ten years, defined online violence against women as **acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communication technologies** (ICTs), such as mobile phones, the internet, social media platforms, and email (APC, 2017: 3). In addition, the Due Diligence Project noted that these acts have resulted or may result in physical, sexual, psychological or economic harm or suffering (Abdul, 2017).

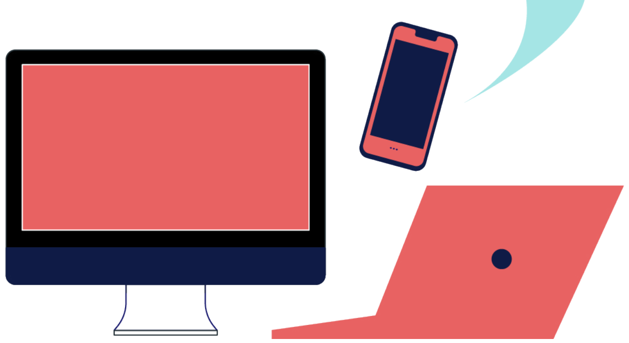
The International Center for Research on Women, for its part, defines technology-facilitated gender-based violence as acts by one or more persons who **harm others on the basis of their sexual or gender identity or by imposing harmful gender norms**. These acts, for which the Internet or mobile technology is used, consist of harassment, intimidation, sexual harassment, defamation, hate speech, and exploitation (Hinson et al., 2018: 1).

Finally, at the United Nations (UN) level, the Special Rapporteur on violence against women defined online violence against women in 2018 as "any act of gender-based violence against women that is **committed, assisted or aggravated in part or fully by the use of ICT,** such as mobile phones and smartphones, the Internet, social media platforms or email, **against a woman because she is a woman, or affects women disproportionately**" (UN-SRVW, 2018, para. 23).

[3] Inter-American Convention on the Prevention, Punishment and Eradication of Violence against Women. Available at: https://www.oas.org/juridico/spanish/tratados/a-61.html

Relevant data and studies have shown that, in most cases, online violence is not a gender-neutral crime (UN-SRVW, 2018).

Online violence against women may be facilitated by algorithms and technological devices such as mobile and smart phones, tablets, computers, geolocation systems, audio devices, cameras, or virtual assistants.



This violence is visible on a large variety of internet platforms; for example, social networks (Facebook, Twitter, Tik Tok), email services, instant messaging applications (WhatsApp), dating applications (Tinder, Grindr, Hinge, Match.com), online video games, content-sharing sites (Reddit), online discussion forums (in the comments sections of newspapers) or user-generated platforms (blogs, image- and video-sharing sites).

Gender-based cyber-violence is a constantly changing concept. As recognized by the UN Special Rapporteur on violence against women, **rapid technological transformations influence online violence**, and new and different manifestations of violence emerge as digital spaces transform and disrupt offline life (UN-SRVW, 2018, para. 24).

Online violence has changed since the early days of the internet, and will surely continue to evolve as digital platforms and technological tools continue to advance and become more and more interrelated in our lives.

The online-offline continuum of violence: new forms of the same violence

Online violence manifests itself in a range of multiple, recurring and interrelated forms of gender-based violence against women (UN-SRVW, 2018).

We should not fall into the error of considering online violence as a separate phenomenon from violence in the "real" world, as it is part of the continuous and interconnected manifestations of violence that women were already experiencing offline.

We are talking about **an old system of gender domination and violence that now uses a new platform to replicate itself.**

In 1989, Liz Kelly first drew attention to the fact that different types of gender-based violence and abuse can be conceptualized as a **continuum of violence in the lives and experiences of women all over the world** (and not just as sporadic or abnormal occurrences), ranging from acts expressly recognized as crimes to behaviors of control and domination that are so common, they have become normalized (Kelly, 1989).

Therefore, in the current context, in which cyberspace and life outside the Internet are increasingly interrelated, violence against women has arrived in the digital world as a further extension of that continuum of violent events that occur in the daily experience of women and girls (Kelly, 1988; Powell, Henry, & Flynn, 2018).

Thus, we observe that in the digital era forms of gender-based violence persist or are amplified with the use of new technologies and that new forms of sexism and misogyny are appearing online, which can emerge from cyberspace in order to become physical attacks on women. Violence against women can, for example, begin as sexual harassment on public streets, as "honor-based" violence in a community, or as physical assaults perpetrated by an intimate partner and relocate through technology and turn into non-consensual distribution of intimate images, cyberharassment, sexist hate speech on social networks, cellphone stalking, etc. Conversely, violence may begin as exchanges on social networks by an underage girl with supposed new friends and culminate in encounters where sexual violence or abductions are committed. All of these new acts impact women's interaction not only online but in all spaces of their offline lives.

In many cases, gender-based violence has intensified as digital spaces offer a very convenient anonymity and abuse can be committed from anywhere, through a wide range of new technologies and platforms that perpetrators of violence have at their fingertips in order to quickly spread permanent digital content.

Some aspects of new ICTs that have contributed to the transformation of gender-based violence against women are their rapid expansion, the permanence of online content that leaves an indelible digital record, their replicability and global reach, and the possibility of easily locating people and their information, which facilitates the attackers' contact with the victims and their secondary victimization (UN-SRVW, 2018).

All types of gender-based violence against women have one thing in common: they are forms of coercion, abuse, or aggression that are used to control, limit or constrain women's lives, status, movements and opportunities, and to facilitate and secure men's privileges (Kelly, 1989).

Highlights:

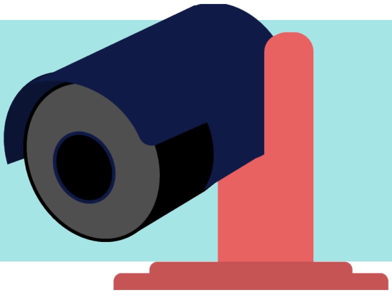
The close relationship between intimate partner violence and new technologies

For several years now, ICTs have been performing a very important role in the upsurge of new strategies of abuse and control used by perpetrators of domestic and partner violence (Dragiewicz, 2019). Diverse studies have revealed that **77% of the victims of online harassment have also sustained some type of physical or sexual violence at the hands of an intimate partner** (FRA, 2014) and that they knew at least half of the aggressors online (APC, 2015).

As new technologies have become incorporated into virtually all people's daily activities, perpetrators have taken advantage, extending and intensifying abusive, possessive, and controlling behaviors that were previously not possible (Woodlock, 2017). As a result, women now experience this violence without boundaries of space and time and with the feeling that the aggressor is omnipresent (Harris, 2018), which has serious effects on their mental health[4].

Although research on the subject is still incipient, several initial studies indicate that some technologies are used more than others to commit abuse and exert cybercontrol in contexts of domestic or intimate partner violence. That is the case with text messages, social networks such as Facebook, or software to monitor the location of victims through their cellphones (Dragiewicz, 2019).

However, the types of digital abuse and surveillance of women and intrusion into their lives are constantly changing and range from incidents of identity theft by a partner or former partner for online shopping to perpetrators' use of smart devices installed in homes, such as thermostats, cameras, microphones, speakers or locks, to generate psychological stress in victims.



New behaviors have also been observed in young couples **that have become normalized in the current online-offline** context, disguised with ideas and myths of romantic love, but which in essence seek to cyber-control and restrict women's digital lives. Some are as follows:

[4] Alexandra Topping (2013). "How domestic violence spreads online: I felt he was watching me." *The Guardian*. Available at: https://www.theguardian.com/society/2013/sep/03/domestic-violence-spreads-online-watching

Demanding the partner's passwords and codes and spying on their cellphone.

Interfering in digital relationships with other people.

Attempting to control interactions on social networks, censoring images or posts, and checking contacts, conversations or online comments.

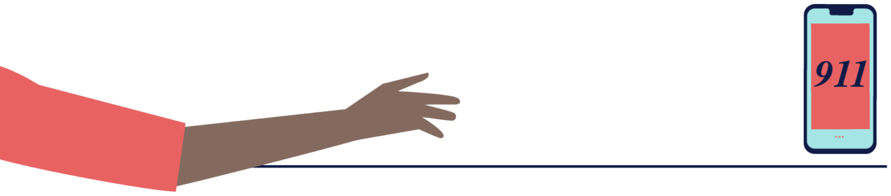
Requiring their partner to display their geolocation constantly.

Forcing them to send intimate images.

In the specific case of victims of domestic and intimate partner violence, online violence can deter them from breaking off the relationship, as they often feel trapped in a situation from which they cannot escape. It has also been documented that digital violence very often intensifies at the time of separation (not only against the victims but also against their children, family members, friends, or intimate partners). It would also appear that abruptly cutting off all communication or digital interaction with certain types of perpetrators may increase the risk to survivors and their family (Dragiewicz, 2019).

This is compounded by the **exponential increase worldwide in physical violence and sexual abuse against women and girls during the COVID-19 pandemic** (UN Women, CIM, 2019). Lockdown meant that they were confined with their aggressors, and for them technology has become an indispensable tool for communicating with the outside world, asking for help, and accessing care services.

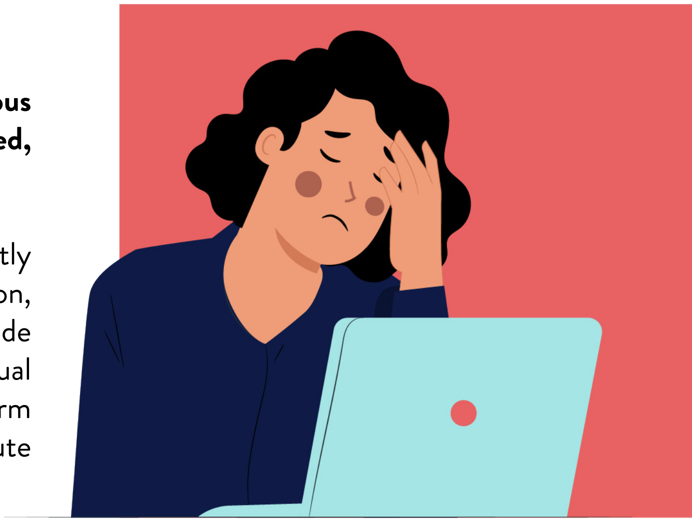
In this context, supporting victims and survivors of domestic and intimate partner violence in recognizing cybercontrol, protecting their digital safety and well-being, and **using technology as a means to break free of the cycle of violence** are essential and must now be part of models of prevention, care and punishment of violence against women, which involve working with families, communities, and institutions.



B

What are the consequences for women and girls who are victims of online violence?

Online violence against women causes real harm



As a consequence of online violence, women and girls suffer serious psychological, physical, sexual, emotional, economic, work-related, family and social harm (UN-SRVAW, 2018).

The manifestations and repercussions of this violence can vary greatly depending on the form it takes; for example, feelings of depression, anxiety, stress, fear or panic attacks in cases of cyberstalking; suicide attempts by women affected by the non-consensual sharing of sexual images; physical harm against victims of doxxing[5], or economic harm as a result of job loss due to online acts that bring them into disrepute (Pew Research Center, 2017; Kwon et al., 2019; AI, 2017).

It has been found that, as part of the continuum of gender-based violence, the harms caused by online acts do not differ from the effects of offline violence; however, they do have short- and long-term impacts on all areas of women's individual development, such as their autonomy, privacy, trust, and integrity (Van Der Wilk, 2018). Unfortunately, there is a persisting lack of proper understanding of the seriousness of the consequences and harm that online violence causes to women, harm that is often considered "not real" because it occurred on the Internet. This reflects a misunderstanding of the online-offline continuum in which our lives now unfold, as well as the characteristics of the series of multiple and interrelated forms of violence experienced by women and girls in their social interactions.

It has also been observed that **the nature of certain technologies causes the magnitude of the harm of some acts of violence to increase exponentially** and extend beyond the original act (such as viralization, reach, anonymity and permanence) (APC, 2017), given that women are judged more harshly than men for their attitudes online. Such is the case of incidents of non-consensual distribution of sexual images, in which women and girls have been stigmatized for exercising their sexuality and, after seeing their images distributed, have to live in a context of permanent humiliation and shame in their social environment, which in many cases has driven them to suicide.

[5] Doxing or doxxing is a cyberattack that consists of obtaining personal information about someone and posting it online.

The women concerned often blame themselves for actions that may have caused the violence and withdraw from digital spaces, self-censor, or cut themselves off socially (Citron, 2014). It is also very common for them to be revictimized by family members, authorities, and the media, which often hold them responsible for protecting themselves, instead of drawing attention to the unlawful conduct of the aggressors, thus normalizing and minimizing such violence (UN-SRVW, 2018, para. 25).

In addition to individual effects, o**nline violence leads to collective and intergenerational harm** and has direct and indirect costs on societies and economies, as victims and survivors not only require medical care and judicial and social services, but their productivity and community interactions may also diminish (UNBC, 2015). Likewise, **this violence has a muzzling effect**, as it is a direct threat to women's freedom of expression (AI, 2017) and affects their online access and participation as active digital citizens, which creates a democratic deficit by preventing women's voices from being heard freely in digital debates (UN-SRVW, 2018, para. 29).

Research on the subject indicates that 28 percent of women who were subjected to violence perpetrated using ICTs have deliberately curtailed their online presence (UN-SRVW, 2018, para. 26) and self-censor for fear that their privacy or security will be breached (AI, 2017). To make matters worse, survivors are often advised to "walk away" or "withdraw" from technologies after an incident of violence.

Finally, we must also not overlook that this violence **contributes to the perpetuation of harmful gender stereotypes and the reproduction of systemic violence** in the new online-offline world, by fostering the development of gender-biased technologies.

Are some women targeted online more than others?

When analyzing digital violence it is important not to fall into generalizations based on an assumed common experience of women. In each case, the specificities of different online experiences lived by women and the diverse identities by which they define themselves must be taken into account.

While online violence is a common phenomenon among women and girls navigating the digital world, the truth is that it also **affects women differently depending on other forms of discrimination** they face in their daily lives on the basis of race, ethnicity, sexual orientation, gender identity, social class or nationality.

According to Amnesty International, women who face discrimination offline due to specific traits of their identity often find that online violence and abuse against them targets those same traits (AI, 2018). These women are particularly vulnerable to victimization through a combination of abuses that reflect racism, sexist beliefs, stereotypes, social prejudices, and notions of a supposed gender order.

The UN Special Rapporteur on violence noted in her 2018 report that certain groups of women are particularly targeted by online violence, such as female parliamentarians, female journalists, young women or women who engage in digital debate, and women from ethnic minorities or the LGBTIQ+ community (UN-SRVW, 2018; Van Der Wilk, 2018; UNBC, 2015; EIGE, 2017; Henry and Powell, 2016). Digital violence against them generally takes the form of attacks on their visibility, sexuality, freedom of expression, and political participation. It is clear that one of the objectives of digital violence is to silence women and keep them in conditions of subordination in society.

Did you know...?

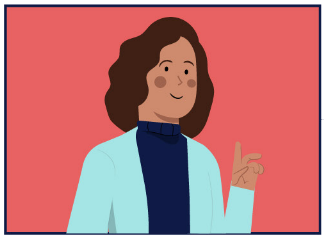
Several reports have found that women aged 18 to 24 are at particular risk of digital violence, with a 27 percent higher likelihood of being victims of cyber abuse compared to men (APC, 2001; UNBC, 2015). The Pew Research Center also reported that such women are particularly vulnerable to cyberharassment (Pew Research Center, 2014 and 2017).

It has been observed that simply being a woman and being a public figure or participating in political life leads to being targeted by extremely misogynistic comments, sexual violence, and threats of physical and femicidal violence online (Rawlison, 2018). Women who participate in public internet discussions or write about gender issues are disproportionately victims of online harassment aimed at silencing and intimidating them; they are also often the target of mass campaigns of abuse and sexualized verbal violence, including hate speech and threats of sexual abuse and rape (UN-SRVW, 2018, para. 25). According to Amnesty International, 88 percent of women experience abuse and cyberharassment after posting feminist content (AI, 2018).

Highlights:

Women likely to be targeted by certain types of digital violence[6]

Women in an intimate relationship or victims of domestic or intimate partner violence.



Women human rights defenders, journalists, women involved in political activities, active participants in online debates, or women with a public profile. These women are frequently subjected to cyberharassment and cyberstalking on the Internet, including online threats and verbal abuse of a misogynistic and sexual nature.

Lesbian, bisexual, transgender, or intersex women; women with disabilities; women from ethnic or racial minorities; indigenous women, or women who belong to marginalized groups. These women are often targets of online hate speech and abuse with homophobic, racist, or sexist overtones.

Young women are also a frequent target of online sexual violence, which reproduces forms of intimidation, harassment, and sexual abuse.

[6] Association for Progressive Communications (APC). *From impunity to justice. Exploring corporate and legal remedies for technology-related violence against women 2012-2015.* Available at: https://genderit.org/onlinevaw/

C

Who are the perpetrators?

It has been found that perpetrators of online gender-based violence against women generally have a male identity (Van Der Wilk, 2018, 34-37). These aggressors may be persons who are unknown to the victim (such as an online sexual harasser who systematically targets several women, or individuals who engage in grooming), a member of the victim's family or professional circle, or even a friend. Studies indicate, for example, that between **40 percent and 50 percent of victims knew their online assailants** (a former partner, family member, friend, or colleague) and that **in one third of cases, the attackers had or had had an intimate relationship with the victim** (Pew Research Center, 2017; APC, 2015).

wo types of perpetrators of online violence against women can be identified (Abdul, 2017):

The original perpetrator:
The person who commits the initial act of digital violence or abuse or who first creates, manipulates or publishes harmful information, personal data, or intimate images without the victim's consent.

Secondary perpetrator(s):
A person or group of persons who participate in the continuation and propagation of an act of online violence by forwarding, downloading, reposting or sharing harmful information, personal data, or intimate images obtained without the victim's consent.

What are perpetrators looking for with online violence against women and girls?
The goal of violence is to create a hostile online environment for women in order to shame, intimidate, denigrate, belittle, or silence them by means of surveillance, theft or manipulation of information, or control of their communication channels (AI, 2018).

Highlights:

Online violence as a violation of women's human rights

As the UN Special Rapporteur on violence against women emphasizes in her 2018 report, women's human rights protected by international treaties must be protected on the internet, "including through the prohibition of gender-based violence in its ICT-facilitated and online forms" (UN-SRVW, 2018, para. 17).

[7] Grooming consists of deliberate acts by an adult to approach a child in order to establish a relationship and emotional control that allows them to commit sexual abuse, engage in virtual sex, obtain child pornography, or engage in child trafficking

For its part, the UN Human Rights Council recognized that violence in digital contexts prevents "women and girls from fully enjoying their human rights and fundamental freedoms" as recognized in international law, hindering their full and effective participation in economic, social, cultural and political affairs (HRC, 2018, para. 3).

Some of the human rights of women that online violence may violate include the following (UN-SRVW, 2018; Vela and Smith, 2016; APC, 2017):

- Right to equality and non-discrimination
- Right to a life free of violence
- Right to humane treatment
- Right to self-determination
- Right to freedom of expression, access to information, and effective access to the Internet
- Right to freedom of assembly and association
- Right to privacy and protection of personal data
- Right to protection of honor and reputation
- Women's sexual and reproductive rights

It is important to keep in mind that "the prohibition of gender-based violence has been recognized as a principle of international human rights law" (UN-SRVW, 2018, para. 17). This implies that States have due diligence obligations to prevent and combat online violence against women committed by both state and non-state actors (Abdul, 2017).

Highlights:

The Internet of things (IoT) and domestic violence

The "Internet of things" (IoT) refers to the network of Internet-connected smart devices that can share data with each other. IoT goes beyond connectivity between computers, cell phones and tablets, and includes devices such as televisions, watches, refrigerators, heating systems, cameras, and smart locks.

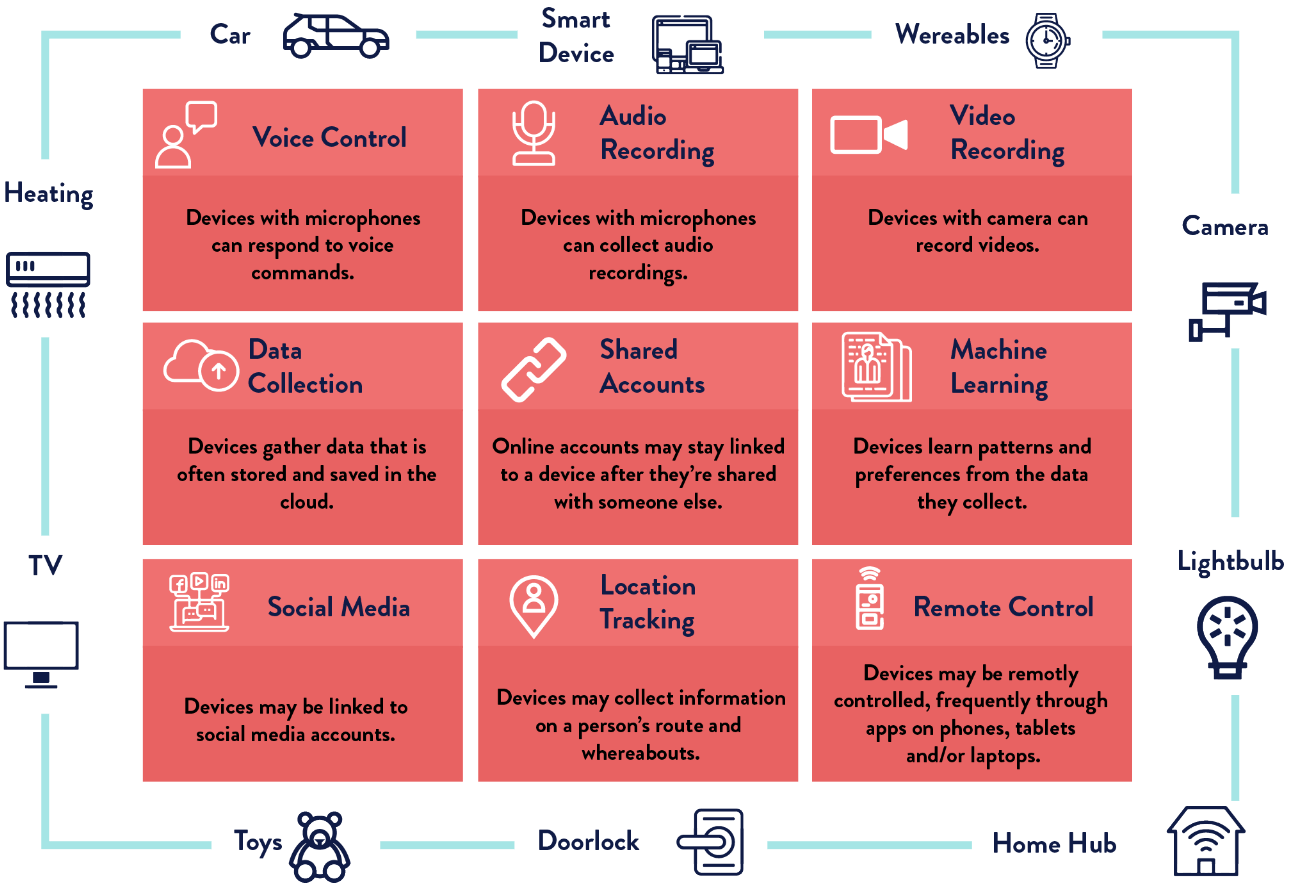
These devices are called "smart" because they can collect and analyze data, communicate with each other, and perform actions without direct human intervention. For example, through IoT, a home security system can be controlled from an application installed on a cell phone, using voice commands directed to virtual assistants, or cameras or lighting systems can be remotely activated or deactivated.

While IoT has many benefits in terms of facilitating practical matters of everyday life, it also entails potential privacy and security risks because the devices assume that all users trust each other. For example, in the case of domestic violence, an abuser can use the IoT to monitor a victim or prevent her from opening the locks to their home, or a hacker can remotely control a security camera to record intimate images or videos directly in a victim's home without their consent.

According to the University College London (UCL) "Gender and Internet of Things" research project, IoT facilitates three forms of online violence:

- Cyberstalking.
- Coercive and controlling behavior, including threats of harm or abuse to frighten a victim; for example, by denying control of heating, lighting or house locks.
- Digital gaslighting, a form of psychological abuse by which the perpetrator manipulates the victim's reality in order to make them question their sanity, memory, or perception.

How IoT can affect victims of domestic violence and sexual violence



Voice Control

Devices with microphones can respond to voice commands.

Audio Recording

Devices with microphones can collect audio recordings.

Video Recording

Devices with camera can record videos.

Data Collection

Devices gather data that is often stored and saved in the cloud.

Shared Accounts

Online accounts may stay linked to a device after they're shared with someone else.

Machine Learning

Devices learn patterns and preferences from the data they collect.

Social Media

Devices may be linked to social media accounts.

Location Tracking

Devices may collect information on a person's route and whereabouts.

Remote Control

Devices may be remotly controlled, frequently through apps on phones, tablets and/or laptops.

Implication:
Perpetrators may exploit IoT's functionalities to monitor, control and/or prevent victims from using devices.

Consideration:
It is important that support services are aware of IoT's functionalities, as they may inform assesments and safetly planning for victims.

Mitigation:
There is no one-size-fits-all mitigation strategy when IoT-enabled tech abuse occurs. Knowing about common IoT functionalities can help when seeking support form professionals such as the police.

Information:
As IoT devices and their funtionalities are constantly evolving, further up-to-date resources and information on the topic are provided on the STEaPP website.

Source: UCL, Gender and IoT Project, How internet-connected devices can affect victims of gender-based domestic and sexual violence and abuse. Available at: https://www.ucl.ac.uk/steapp/research/digital-technologies-policy-laboratory/gender-and-iot

Part two

AN OVERVIEW OF DIFERENT TYPES OF TECHNOLOGY-FACILITATED GENDER-BASED VIOLENCE AGAINST WOMEN AND GIRLS

It is important not to lose sight of the fact that online gender-based violence against women encompasses a wide variety of harmful or offensive practices, behaviors, and online-offline contexts that change as technology progresses.

What we understand as online violence against women are, in fact, very diverse practices and behaviors that may constitute cybercrimes or unlawful acts that engage administrative, civil or criminal liability depending on the law in each country (IGF, 2015; UN-SRVW, 2018; APC, 2017).

At present great disparity persists in terms of the terminology used to refer to the various types of online violence against women and its manifestations, with constant variation between the expressions used by States, international agencies, NGOs, and academia (Van Der Wilk, 2018). Unfortunately, this has led to confusion about the classification of these conducts and, in many cases, resulted in imprecise references in domestic law.

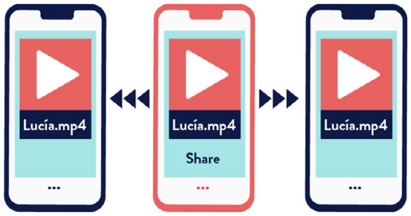
In an effort to clarify this scenario, the **following is a non-exhaustive list with a descriptive guide to behaviors and cyberattacks that can be considered online gender-based violence against women**. The aim is to facilitate the identification of personal experiences and, on that basis, to know what steps can be taken to strengthen the digital safety of victims (see Part 3 of this guide).

This catalog was formed by means of a bibliographic review and should not be regarded as fixed or static, since digital violence is constantly evolving in parallel with technology, and other manifestations of violence emerge as new technological tools appear (UNBC, 2015).

Also, as will be noted in this section, it is important to keep in mind that there may be instances in which two or more forms of digital violence are exercised simultaneously, either interdependently (e.g., online threats followed by non-consensual distribution of intimate images) or accompanied by other forms of violence outside the Internet (as often occurs in cases of domestic violence).

At all events, it should be kept in mind that these cyberattacks and online acts will be considered gender-based violence when directed against a woman simply because she is a woman (i.e., because of her gender identity) or because they disproportionately affect her.

Types of gender-based violence against women and girls facilitated by new technologies:



01

Creation, dissemination, distribution or digital sharing of photographs, videos or audio clips of a sexual or intimate nature without consent.

02

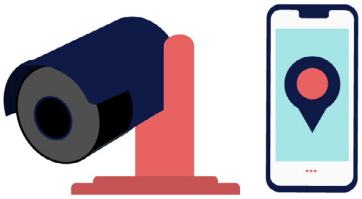
Unauthorized access, use, manipulation, exchange, or distribution of personal data.

03

Impersonation and identity theft.

04

Acts that damage a person's reputation or credibility.

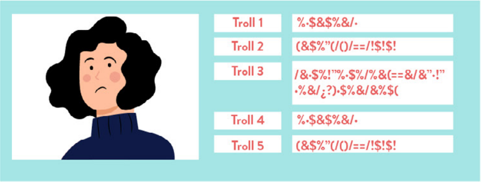


05

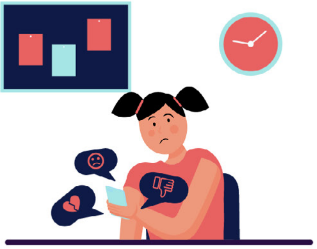
Acts involving surveillance and monitoring of a person.

06

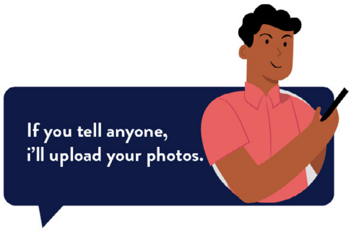
Cyberstalking.



07 Cyberharassment.



08 Cyberbullying.



09 Direct threats of harm.

10 Technology-facilitated physical violence.

11 Abuse and exploitation of women and girls by means of technologies.

12 Attacks on women's groups, organizations, or communities.

A

Non-consensual creation, dissemination, distribution or digital sharing of photographs, videos or audio clips of a sexual or intimate nature

Women are the main victims of this type of digital violence, which affects them disproportionately all over the world. Several studies have found that 90 percent of those affected by digital distribution of intimate images without consent are women (UN-SRVW, 2018; Cyber Civil Rights Initiative).

The **non-consensual** creating, sharing or disseminating online of intimate or sexually explicit material, images or videos obtained with or without consent, for the purpose of shaming, stigmatizing, or harming the victim (UN-SRVW, 2018, para. 41).

This form of violence can occur in a wide variety of contexts and interpersonal relationships: in an intimate and trusting relationship in which these images are sent voluntarily by a person to his or her partner or former partner (perhaps by sexting), as part of cyberstalking or cyberharassment by friends, acquaintances or strangers, or when the material is obtained through hacking or physical access to devices[8].

It also includes the following acts:

01 Recording and distributing images of sexual abuse.

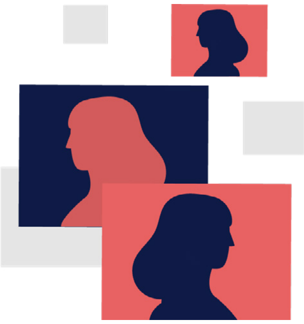
02 Taking, without consent, photographs or videos of intimate parts of women's bodies in public spaces and sharing them online (e.g., photographs taken upskirting, downblousing or creepshots).

03 **Creating sexualized, photomontage-edited images or deepfake videos, where images or videos** of women may be taken from online sites or social media accounts and superimposed on other people's bodies to simulate sexual scenes or pornographic content with the aim of damaging the victim's reputation.

[8] Hacking is the use of techniques and procedures by a hacker to gain unauthorized entry into another's computer system for the purpose of manipulating it, for obtaining information, or for fun. Cracking is a practice related to hacking but involves breaking into other people's systems for criminal purposes in order to violate the privacy of the affected person or the confidentiality of information, or to damage information or hardware.

What is a deepfake video?

Since 2017, software programs have been available that use machine-learning techniques to swap one person's face for another's (Knight, 2019). These programs are being used to create fake pornographic videos and post them online (Farokhmanesh, 2018). These videos have particularly targeted women involved in political affairs, although their use is expected to increase as this technology has become more accessible to non-expert users (Deeptrace, 2019). Moreover, given that deepfake videos use machine-learning techniques, it could ultimately be difficult to distinguish between a fake video and a real one without the help of forensic tools (Maras and Alexandrou, 2018).



The non-consensual production of intimate photographs or videos **may be accompanied by extortion or threats to distribute them** or take place without the victims' knowledge in closed social networking groups in which several men disseminate images of nude women without their consent for the sexual gratification of the other members, or as part of enrichment schemes in which offenders compile and sell links to files or "packs" (as they have been called in countries such as Mexico and Chile) of sexual images of women obtained in various ways without their consent[9].

It is also **very common to leak personal data of the women who appear in such images or videos**, many of whom are forced to leave school, work, home, and their community to avoid constant humiliation (Henry, Powell, & Flynn, 2017).

As a reminder...

This form of online violence is commonly known as "revenge porn." However, it is not a correct term, and its use is problematic since it does not convey the diversity of perpetrators' motives, which extend beyond vengeance and range from a reaffirmation of their masculinity to economic extortion or sexual gratification. This term also minimizes the harm caused to victims, obscures the non-consensual component of the behavior, and emphasizes the image, rather than the abusive behavior of the perpetrators (Powell, Henry, & Flynn, 2018).

What is sexting?

Sexting is a practice that involves the generation and sharing of sexually explicit material (UNODC, 2019; Interagency Working Group, 2016). It may include consensual creation and sending of images or consensual creation of images that are distributed without consent (Salter, Crofts, & Lee, 2013, p. 302).

Several studies have found that it is a common practice among young men and women using technology as a tool for sexual expression. It has been found, however, that sexting occurs in contexts in which young women and girls are under greater social pressure than young men to share sexual and degrading images of their bodies, while young men and boys are pressured to request images, receive them, and share them with their friends in order to reaffirm their heterosexuality (Walker, Sanci, & Temple, 2013).

[9] Monserrat Peralta (2019). "El oscuro negocio de los packs" [The dark business of packs]. *El Universal*. Available at: https://www.eluniversal.com.mx/nacion/el-oscuro-negocio-de-los-packs-fotos-intimas-desde-un-peso-en-la-red

Highlights:

Some important aspects of sexting and the non-consensual distribution of intimate images and videos:

01

Even if there is consent to share intimate images with someone or to record sexual acts (even in the presence of others), **that consent does not imply permission to store, make public, reproduce or disseminate that content**. Consenting to recording does not mean consenting to another step in the process. Whoever does so violates the privacy of the person who engaged in the sexting. This is a serious form of gender-based violence, a human rights violation, an unlawful act, and it is already criminalized in many countries.

02

The practice of *sexting* should not be stigmatized. We all have the right to use technology to express our sexuality. However, in doing so, it is very important to keep in mind that there are risks, and therefore **digital security needs to be considered.**

03

States have the obligation to adopt appropriate measures to prevent, investigate, punish, and redress harm caused by this form of violence. Likewise, Internet platforms have an obligation to prevent non-consensual dissemination of intimate images and videos, to remove such content, and to reduce or mitigate risks.

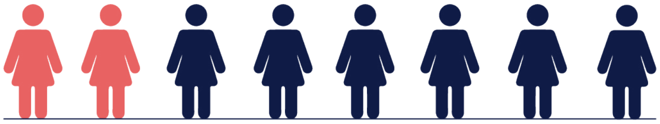
Acoso.online[10] is a site that offers information on this type of digital violence, as well as advice on how to report it to Internet platforms and details about the different laws in Latin American countries on which a complaint can be based. The website of the organization Without my Consent also makes available a wide array of resources to support survivors of this form of violence.

It should be emphasized that the provision of these resources does not constitute an endorsement by the OAS or its member states of the content or organizations named herein. These resources are presented as examples of organizations, guides, tools, etc., that are available in the region, so that readers can obtain more information about the subject matter of this publication.

[10] Acoso.online, *Pornografía no consentida. Cinco claves para denunciar y resistir su publicación* [Nonconsensual pornography: Five key tips for reporting and resisting their posting]. Available at: https://acoso.online/ar; *Without my Consent. Tools to fight online harassment, Resources. Available at*: https://withoutmyconsent.org/resources/

B

Unauthorized access, use, control, manipulation, sharing or publication of private information and personal data



According to Amnesty International, a quarter of women have been victims of doxing at least once in their lifetime (AI, 2017).

This form of violence manifests itself in the form of **attacks on a person's online accounts or devices** (cellphones, computers, tablets, etc.) to obtain, manipulate and/or publish information in an unauthorized manner by stealing passwords, installing spyware, stealing equipment, or keylogging[11] APC, 2017). It may also involve unauthorized access to and full control of a person's accounts or devices.

Doxing or *doxxing*:

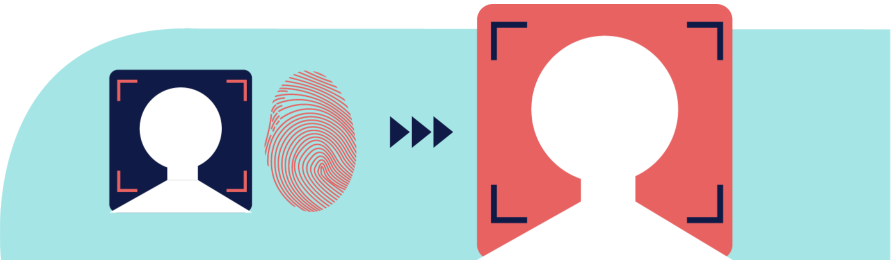
The term comes from the expression "dropping docs" and involves the **unauthorized extraction and publication of personal information**—such as a person's full name, address, telephone numbers, and email addresses; the names of their spouse, family members and children; or financial or work details—as a form of intimidation or with the intent to locate that person in "the real world" in order to harass them (APC, 2017; Women's Media Center, 2019). There have also been cases of personal information being posted on pornographic websites, together with an advertisement that the victim offers sexual services.

[11] A keylogger is a malicious program that installs itself between the keyboard and the operating system to intercept and record information about every key pressed on the device without the user's knowledge.

C

Impersonation and identity theft

Research conducted by the Australian National University revealed that women are 50 percent more likely than men to be victims of identity theft.t[12].



It is a malicious activity that consists of **impersonating another person online and using their personal data in order to threaten or intimidate them** (Women's Media Center, 2019). This can be done by creating fake profiles or accounts on social networks or usurping email accounts or telephone numbers, which can be used to contact friends, family, colleagues or acquaintances of the victim for the purpose of establishing communications and accessing information about them (APC, 2017; Barrera, 2017).

The case of the cyber attacker of a whole family

In a well-known case in Chile, a foreign cyberattacker harassed an entire family and their circle of friends (at least 50 people) for 13 years, stealing personal information and impersonating them, including theft of passwords, e-mails, and social network profiles, as well as personal images to send obscene messages and make large-scale publications on pornographic pages. The aggressor, who is suspected of being the former romantic partner of one of the family members, carried out numerous acts of cyberviolence against anyone related to or in contact with the original victim and their family (Paz Peña, 2017).

In cases of domestic violence, the impersonation and theft of the identity of victims through is often carried out using different mechanisms, such as obtaining their personal data for the illicit use of their credit cards or control of assets, to monitor their communications with other people, or to impersonate family members or friends on social networks in order monitor them through those profiles.

[12] Australian Communications Consumer Action Network, "Identity Theft and Gender." Available at: https://accan.org.au/files/Grants/ANU%20ID%20theft/ANU%20ID%20theft%20infographic_Gender.pdf

D

Acts that damage a person's reputation or credibility

In a UNESCO global survey, 41% of respondents reported being targeted by attacks that appeared to be related to disinformation campaigns specifically aimed at discrediting female journalists.

This form of violence affects women in general. For example, according to the study *Knowing to Resist. Online gender violence in Peru*[13], 15% of the victims interviewed indicated having been affected by the dissemination of false, manipulated or out of context information.

Such acts consist of **creating and sharing false personal information with the intention of damaging a person's reputation,** such as creating fake profiles on social networks or online accounts; making photomontages or manipulated images of a sexual nature from photographs obtained from social networks; posting ads on dating or pornographic sites with intimate photos; disseminating offensive or false comments or posts or memes on discussion forums, social networks or internet pages (including acts of vandalism on Wikipedia), and engaging in acts of slander and manipulation (APC, 2017; Barrera, 2017).

¿?

What is *slutshaming*?

It is a form of violence that consists of publicly pointing out a woman for her alleged sexual activity in order to embarrass her, damage her reputation and regulate her sexuality. It may involve the use of photos and/or videos and demeaning language.

Camila Zuluaga Case

Various civil society organizations have documented an increase throughout the region of online acts that designed to harm the reputation and credibility of women journalists, politicians and human rights defenders (Peña, 2017; Luchadoras, 2017; Cuellar and Chaher, 2020). In a case in Colombia, Camila Zuluaga, a journalist, was the target of a mass coordinated attack in September 2019 after the Los Irreverentes portal claimed without proof that she had received 35 million pesos from someone implicated in a corruption scandal. The attacks concentrated around the hashtags #CamilaEstásPillada and #CamilitaEstásPillada, which at one point reached as many as 10,000 mentions in one day. Research on the subject found evidence of automation in these coordinated attacks and the involvement of a WhatsApp group where instructions were given for carrying out the attacks in order to discredit her work as a journalist (Cuellar and Chaher, 2020).

[13] UNESCO and the International Center for Journalists (ICFJ) (2021). Online Violence: The New Line of Battle for Women Journalists - #JournalistsToo. Available in: https://unesdoc.unesco.org/ark:/48223/pf0000375136_spa; Carlos Guerrero and Miguel Morachimo (2018). Know to resist. Online Gender Violence in Peru. Available in: https://hiperderecho.org/tecnoresistencias/wp-content/uploads/2019/01/violencia_genero_linea_peru_2018.pdf

E

Surveillance and monitoring of a person

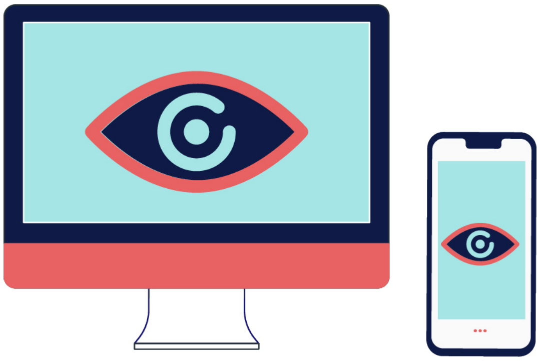
It has been documented that in at least 29 percent of cases of domestic or intimate violence, the partner or ex-partner has used some type of spyware or geolocation equipment installed on the affected women's computers or cell phones (Women's Aid, 2014).

Constant monitoring and surveillance of **a person's online and offline activities** or location constitutes a form of violence (APC, 2017).

- This can be done with *spyware* installed on the victim's cellphone to covertly monitor them or steal their information.
- It is also carried out using geolocation devices located in cars or handbags, toys, surveillance cameras, virtual assistants, or connected smart devices.

¿? What is *spyware*?

It is a type of malware that is installed on a person's devices to record everything they do, including text messages, emails, photos, or even all keystrokes. With certain types of malware, attackers can remotely activate the cellphone's camera or microphone, track the victim's location, monitor application usage, or intercept calls.



F

Cyberstalking

Several studies on the subject have shown that cyberstalking and cyberharassment are cybercrimes with a significant gender connotation and that women and girls are more likely to be victims of such forms of violence (Reyns, Henson, & Fisher, 2011).

To date, there is no single definition of cyberstalking, as it encompasses a wide variety of abusive digital behaviors. In general terms it can be defined as an **intentional and repeated activity** carried out using computers, cellphones and other electronic devices, which may or may not constitute harmless acts separately, but which, taken together, amount to a **pattern of threatening behaviors that undermine a person's sense of security** and cause fear, distress or alarm (EIGE, 2017: 4; PRC, 2018; Maras, 2016). This activity may also be directed against the victim's family members, friends, or romantic partner.

Unlike cyberharassment, cyberstalking involves a pattern in the commission of **more than one incident over a period of time using ICTs,** with the repeated aim of intimidating, stalking, annoying, attacking, humiliating, threatening, frightening or offending a person or verbally abusing them (UNODC, 2015). It may consist of e-mails, calls, text messages, online chat or constantly sending of obscene, vulgar, defamatory, or threatening comments over the Internet. Some of the behaviors that it may include are:

Spying, obsessing, or collecting online information about someone and communicating with them without their consent; constantly sending friend requests on social networks; joining all the online groups they are part of; following up on notes posted by the victim on social networks through acquaintances they have in common, colleagues, or their friends or family members, or constantly viewing their profile for them to notice (UNODC, 2019).

Repeatedly calling or sending emails, text or voice messages, including messages that are threatening or that seek to maintain control over the victim.

Making unwanted and repeated sexual advances, sending unsolicited sexual photos (images of perpetrators' male genitalia), or constantly monitoring and surveilling a person's location or daily activities and communications (Henry and Powell, 2016).

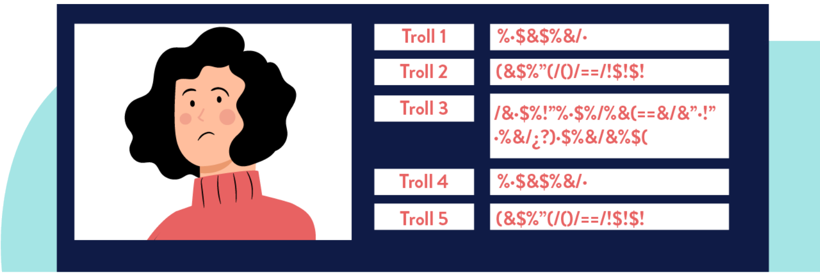
Constantly posting false, malicious or offensive information about a person on their web pages, blogs or social networks.

Perpetrators of cyberstalking can be intimate or sexual partners, former partners, acquaintances, friends, family members or strangers. **This tactic is particularly prevalent in contexts of domestic or intimate partner violence.**

G

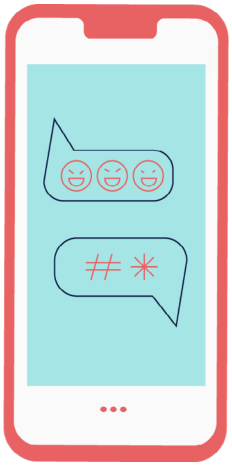
Cyber harassment

A study published in 2018 by Amnesty International noted that 23 % of women surveyed had experienced some form of abuse or harassment on social networks at least once (AI, 2018).



Cyberharassment involves the **use of ICTs to intentionally humiliate, annoy, attack, threaten, alarm, offend or insult a person** (Maras, 2016). Unlike cyberstalking, where there is a pattern of threatening behaviors, in the case of cyberharassment a single incident is sufficient, although it may also involve more than one (UNODC, 2019).

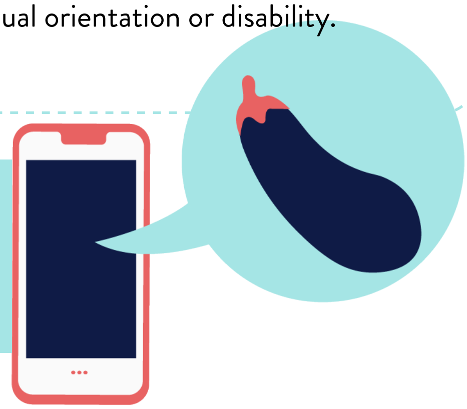
Cyberharassment **can take numerous forms and be associated with other types of online violence.** For example, it can include sending unwanted and intimidating messages via email, text, or social networks; inappropriate or offensive insinuations on social networks or in chat rooms; online verbal violence and threats of physical violence or death; hate speech; theft or publication of personal information, images, and videos; and spreading false information or rumors to tarnish a person's reputation (EIGE, 2017; APC, 2017, UNODC, 2019).



What is hate speech?

It is the use of language that denigrates, insults, threatens, or attacks a person by reason of their identity or other characteristics, such as sexual orientation or disability.

Cyberharassment can also include the disclosure of the victim's personal information (doxing) with invitations to rape her, which has led to situations of revictimization where the harassers and perpetrators go to the home of the woman under attack.

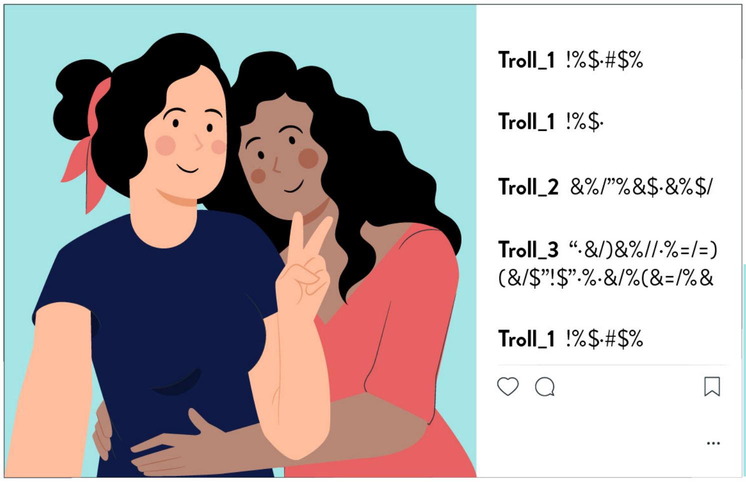


Cyberharassment, which disproportionately affects women worldwide, has sexual connotations (Li, 2006; Henry and Powell, 2017, p. 212). It may involve threats of rape, femicide, sexualized physical violence, or incitement to physical and sexual violence against the victim or her family members, as well as sexist or offensive verbal attacks associated with the gender status or physical appearance of women. It includes sending unwanted sexually explicit material, content that dehumanizes women and presents them as sexual objects, or misogynistic, explicitly sexual, and abusive comments (Jane, 2016).

Did you know...?

Several studies reveal that women are more than twice as likely as men to be targets of sexual cyberharassment (Reid, 2016).

A common form of sexual cyberharassment is cyberflashing or sending obscene photos to a woman without her consent (e.g., pictures of the harasser's genitals) with the intention of annoying, intimidating or embarrassing her.



Troll_1 !%$·#$%

Troll_1 !%$·

Troll_2 &%/"%&$·&%$/

Troll_3 "·&/)&%//·%=/=)(&/$"!$"·%·&/%(&=/%&

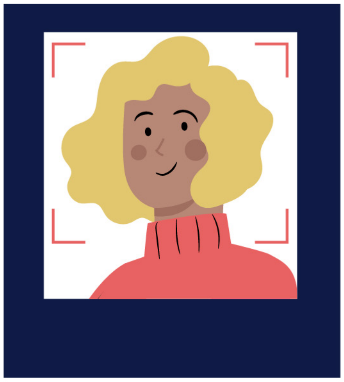
Troll_1 !%$·#$%

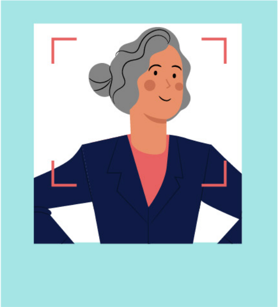
Perpetrators of cyberharassment may be *trolls*, who post extremely offensive and vitriolic comments to provoke an emotional reaction and response from other Internet users. This behavior is known as trolling (Maras, 2016).

Gender *trolling* is the posting of messages, images or videos, as well as the creation of hashtags, with the purpose of annoying women and girls or inciting violence against them (UN-SRVW, 2018; Mantilla, 2013)

Cyberharassment can also be group-based, when two or more people organize and coordinate to repeatedly harass a person online, often in a sustained manner over time and with a particular strategy. These groups may be made up of members of digital communities, forums or alliances (such as Reddit or 4Chan), where certain types of particularly violent masculinities have been found (Jane, 2017).

In Latin America there has been a proliferation of group attacks coordinated by networks of trolls and hacker, such as “Holk Legion” (originating in Colombia and Peru) or “Secta 100tifika,” which carry out mass attacks and harassment in order to generate confrontation and controversy, establish trends, and promote discrimination, racism and misogyny. These groups often target women who are active on social networks, have a public profile, or are feminists. The dissemination of sexualized photomontages, the impersonation of their identities on social networks for defamatory purposes, and circulation of degrading content are common (Peña, 2017; Barrera, 2017).





Some of these attacks have become disproportionate: cybermobs are formed, comprising organized online groups that post offensive or destructive content en masse with the intention of shaming individuals or getting their social network profiles taken down (Citron, 2014).

> **Ana Gabriela Guevara Case**
> An emblematic case of coordinated attacks in Mexico was that on Ana Gabriela Guevara, a former athlete and senator, who, in December 2016, after posting on social networks about physical acts of aggression that she suffered on public roads, was attacked by organized groups of trolls and hackers with fake accounts, who created viral hashtags referencing gender violence. Hashtags such as #MujerGolpeadaEsMujerFeliz or #GolpearMujerEsFelicidad were used and became trending topics in various Spanish-speaking countries (Peña Ochoa, 2017; Barrera, 2017).

H

Ciberbullying

According to a worldwide investigation carried out by IPSOS[15] in 2018, 1 in 5 parents indicated that their daughter / daughter had been a victim of cyberbullying. It was also identified that Peru, Argentina and Mexico were the countries with the highest levels of cyberbullying in social networks.

Cyberbullying involves the use of technologies by children to humiliate, annoy, alarm, insult or attack other children or to spread false information or rumors about the victim, as well as to threaten, isolate, exclude or marginalize them (Maras, 2016; Hinduja and Patchin, 2014; UNODC, 2015).

It can be carried out using text messages, emails, virtual surveys, blogs, social media posts, online video games or virtual reality sites, and can cause very serious harm to the emotional and physical well-being of those under attack, who may even self-harm or commit suicide.

In most countries, it is considered that ***cyberbullying* involves boys and girls as the perpetrators and victims of this form of violence** (Duggan et al., 2015). In others, such as Australia and New Zealand, cyberbullying can involve adults.

Did you know...?

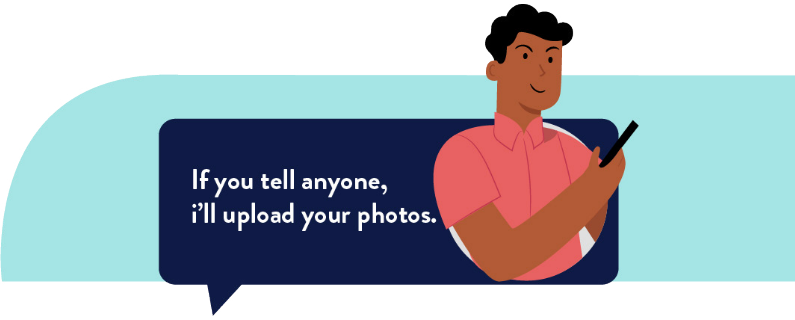
There are diverse opinions as to whether the gender of individuals is a determinant of cyberbullying (Navarro & Jasinski, 2013; Smith, 2012; Fanti, Demetriou, & Hawa, 2012; Livingstone et al., 2011; Calvete et al., 2010). That aside, what is clear is that the harm and consequences suffered by girls and boys differ depending on the gender stereotypes they face: it is common for girls who are victims of cyberbullying to be attacked with offensive and violent comments about their bodies or sexuality.

[15] Ipsos Public Affairs (2018). *Cyberbullying. A Global Advisory Survey.* Available at: https://www.ipsos.com/sites/default/files/ct/news/documents/2018-06/cyberbullying_june2018.pdf

I

Direct threats of harm or violence

In 2019, Amnesty International published the research Green Hearts: Online Violence Against Women during the debate on abortion legislation in Argentina[16], in which it identified that 1 in 3 women surveyed had suffered violence on social networks, of which 26% received direct and / or indirect threats of psychological or sexual violence.



This type of violence consists of using ICT to send or post communications or content (oral or written messages, images, videos) expressing the **intent to commit physical harm or sexual violence** (APC, 2017; Barrera, 2017).

It includes digital extortion, which occurs when one person pressures another person to act in a certain way by means of threats, intimidation or aggression, in order to bend them to their will or control them emotionally. It may take the form of threats to post online or send the victim's acquaintances private sexual or intimate information as sexual blackmail.

¿? What is sextorsion?

Sextortion consists of threatening to disseminate intimate images or videos of a person in order to obtain more material about sexually explicit acts, engage in sexual intercourse, or extort money (UN-SRVW, 2018, para. 32). This form of violence disproportionately affects women and, with a few exceptions, is usually perpetrated by people who identify as men (Kelley, 2019).

This type of violence has grown exponentially in recent years and can be carried out in multiple ways: from hackers who send emails demanding money not to publish intimate images and videos supposedly taken remotely by activating a device's camera, to intimate partners or former partners who engage in sextortion for their own sexual gratification. A 2018 report by the FBI's Internet Crime Complaint Center noted a 242 percent increase in emails threatening extortion, most of which were of a sexual nature (FBI-ICC, 2018).

[16] Amnesty International published the research *Green Hearts: Online Violence Against Women during the debate on abortion legislation in Argentina*. Available at: https://amnistia.org.ar/corazonesverdes/files/2019/11/corazones_verdes_violencia_online.pdf

#GamerGate Case
One of the first mass online targeting campaigns took place in 2014. #GamerGate[17], as it was known, targeted several women in the video game industry—including developers Zoe Quinn and Brianna Wu, as well as journalist Anita Sarkeesian—after they spoke out about sexism and gender inequality in video games. Supporters of #GamerGate voiced their opposition to the influence of feminism in video game culture by organizing on online platforms such as 4Chan, Twitter, and Reddit to launch large-scale coordinated attacks that included acts of cyberharassment, doxing, and rape and death threats. All three women reported doxing attacks with threats that escalated to such a magnitude that they had to flee their homes. In particular, the attacks against Anita Sarkeesian became extremely aggressive, including bomb threats after she was nominated for an award in San Francisco, and terrorist threats when it was announced that she would participate in a conference at the University of Utah.

J

Technology-facilitated physical violence

In the UNESCO and ICFJ research entitled *Online Violence: The New Line of Battle for Women Journalists - # JournalistsToo*[18] it was documented that 20% of surveyed women had been attacked offline in connection with the violence they experienced online.

This form of violence can have various manifestations, such as sexual attacks organized or planned through ICTs or sexual violence following the online publication of the victim's personal data leading to their location (doxing).

It can also occur when a perpetrator befriends a person online to get to know them and then sexually abuse them (as can occur with dating apps), or when a perpetrator forces a person to engage in sexual relations under the threat of publishing intimate or sexual information about them (sextortion) (Henry and Powell, 2018).

[17] Eliana Dockterman (2014). "What is #GamerGate and why are women being threatened about video games?" *Time*. Available at: https://time.com/3510381/gamergate-faq/
[18] UNESCO and ICFJ research entitled Online Violence: *The New Line of Battle for Women Journalists - # JournalistsToo*. Available at: https://unesdoc.unesco.org/ark:/48223/pf0000375136_spa

K

Abuse, exploitation, and/or trafficking of women and girls through the use of technology

Some surveys suggest that new technologies provide global human trafficking (whose victims are women in 80 percent of cases and in 95 percent of cases for sexual exploitation) with a new digital modus operandi, in which the Internet is used for the recruitment, sale, advertisement, and exploitation of women and girls (Van Der Wilk, 2018).

This form of online violence involves the use of technology to exert power over a person by sexually exploiting their image or body against their will (Barrera, 2017). Some of the behaviors included in this form of violence are as follows:

- Technologies are used to target and capture women and girls for sexual abuse or trafficking, force them to accept trafficking and sexual abuse situations, exercise power and control over them, and prevent them from freeing themselves from the abuse, including by threatening to disclose private information (UN-SRVW, 2018, para. 32).

- *Grooming* involves deliberate acts by an adult to approach a child (possibly by cultivating a romantic connection) in order to establish a relationship and emotional control that allows them to commit sexual abuse, engage in virtual sex, obtain child pornography, or traffic the child (Women's Media Center, 2019).

- The publication of sexual images without a person's consent for the purpose of commercialization and prostitution.

L

Attacks on women's groups, organizations, or communities

Various studies have documented that among those who face a higher risk of being victims of gender violence online are human rights and gender equality defenders, women identified as feminists and women activists working in the field of sexual health and reproductive (APC, 2017; Barrera, 2018; REVM-ONU, 2018).

They consist of intentional acts to censor and harm women's organizations, including attacks on their channels of expression (Barrera, 2018), such as accessing them without consent or hacking internet sites, social networks, or email accounts to undermine their operation; getting the organization's profile or social networks taken offline by using community standards to denounce content that the platform considers sensitive; denial of service (DoS) attacks[19], domain use restrictions or domain theft, and internet blackouts during a meeting or protest (APC, 2017).

They include surveillance and monitoring of the activities of members of communities or groups, direct threats of violence against them, cyberharassment using sexually explicit content, publication of confidential information (such as addresses of shelters for women survivors of violence), or repeated harassment of an entire group.

Cases of attacks on feminist groups

In Latin America there have been several attacks on websites, profiles or accounts of feminist groups or women's human rights defenders in order to block or have their content taken offline temporarily or permanently. Reported cases include those of Las Hijas de la Violencia, a Mexican feminist collective, or Mujeres Insumisas, a Colombian feminist organization, as well as constant coordinated attacks against activists and groups of black feminist and transfeminist women in Brazil (Lyons et al., 2016; Peña, 2017).

[19] An online attack that consists of mobilizing people to flood a website's server with requests in order to overwhelm it and render it unavailable.

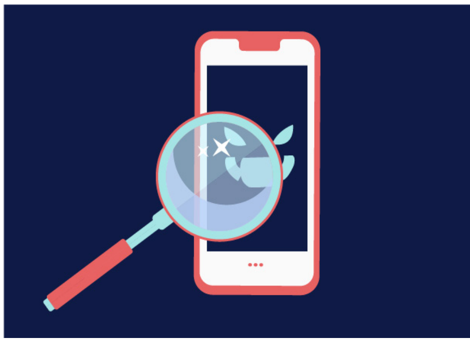
Part three

PREVENTING AND COMBATING ONLINE VIOLENCE AGAINST WOMEN:

The perspective of institutions

A

Interventions to combat online violence against women and girls



Measures to prevent, address, investigate and punish acts of violence against women facilitated by new technologies have received increasing attention at national and international levels. As the extent of this phenomenon and its serious effects on women and girls have become increasingly apparent, different sectors have focused on looking at ways to address the threats to women's safety and well-being that have accompanied rapid technological change.

Some initial studies and testimonies of victims and survivors have disclosed common elements that are undoubtedly a valuable guide for developing institutional capabilities. For example, a widespread lack of information on the characteristics of ICT-facilitated gender-based violence and on online safety practices that women can adopt to protect themselves has been documented; a lack of support services for victims is observed in various countries; a great need persists for training for authorities at all levels to provide adequate guidance; and national legal frameworks remain in place that hinder access to justice for women who suffer this form of violence (Barrera, 2017; APC, 2017; Peña Ochoa, 2017; Van Der Wilk, 2018).

It has also been found that law enforcement bodies often trivialize online violence against women and blame the victims (rather than the perpetrators), which has resulted in a culture of silence, where survivors prefer not to report acts of violence to the authorities rather than risk being ignored or revictimized during the process (Abdul, 2017: p. 7; UN-SRVW, 2018, para. 68).

In her report on digital violence published in 2018, the United Nations Special Rapporteur on Violence against Women took up various proposals from the Internet Governance Forum regarding state measures to address this phenomenon. She underscored the obligation of States to ensure that both State and non-State actors refrain from engaging in online violence against women, as well as to exercise due diligence to prevent, investigate and punish these acts (UN-SRVW, 2018, para. 62). Some of the measures identified by the Special Rapporteur include the following:

- Apply a gender perspective to all online forms of violence.
- Take measures to raise awareness that online violence is a form of violence against women, a form of discrimination, and a violation of human rights.
- Collect and publish sex-disaggregated data on internet access, prevalence of online violence against women, and the harm it causes.
- Provide prompt, adequate and accessible assistance services for women affected by this form of violence, including the establishment of hotlines and specialized care units, and widely disseminate information about these services so that women are aware of their existence.
- Provide victims with appropriate legal assistance.
- Establish legal mechanisms that allow for diligent investigation and punishment of acts of online violence against women, in addition to offering the possibility for victims to obtain protection orders.
- Take effective measures to prevent the publication of harmful gender-based content and to remove it and prevent its distribution.
- Strengthen the technical expertise of law enforcement and justice authorities.
- Adopt clear and specialized intervention models, protocols and codes of conduct so that officials can provide a timely response to this form of violence.
- Combat the culture of impunity of perpetrators by imposing adequate, necessary, and proportional penalties to the criminal act.
- Grant reparations to victims of online violence commensurate with the severity of the harm suffered, financial compensation to cover the costs of material and moral harm, restitution, rehabilitation and satisfaction measures, as well as guarantees of non-recurrence.
- Establish a comprehensive legal framework to combat and prevent ICT-facilitated violence against women and to bring perpetrators to justice for their actions.
- Take measures to eliminate any gender inequality in access to technologies and promote digital literacy.

Similarly, interviews with survivors of new-technology-facilitated domestic violence and with personnel that specialize in addressing violence against women have yielded guidance on other actions that could be taken in this area, including (Dragiewicz, 2019):

- ✓ Increase education and awareness of authorities and first-contact personnel on the characteristics and effects of this violence.
- ✓ Provide adequate training to police on obtaining evidence of online violence against women and on providing guidance to survivors on online safety measures.
- ✓ Recognize and respond to the digital divide that affects many victims of domestic violence.
- ✓ Incorporate training on new-technology-facilitated violence against women into university curricula for law, psychology, and social work degrees.
- ✓ Facilitate the work of technology and security specialists in providing advice and assistance to care centers and shelters for violence survivors (e.g., by analyzing potential threats to the digital integrity of women who turn to such centers).

Undoubtedly, given the novelty of the phenomenon, there is still much to be known about the reality faced daily by victims of gender-based online violence, and new and renewed intervention schemes will surely emerge as women demand justice and as more is known about the links between gender-based violence and new technologies.

In addition, contributions and engagement will be needed, not only from national authorities, but also from internet intermediaries, victims' representatives, civil society, academia and all stakeholders involved in internet governance, as well as in national and regional cybersecurity policies and local strategies to eradicate violence against women.

In this common framework of learning and collaborative work, taking into account the dynamism of this issue and the need to address it adequately, there are some **points that are important to bear in mind in the discussions that are already taking place around digital gender-based violence against women**, as well as for those that will be held in the future.

First, online violence against women, as part of the array of multiple, interrelated and recurrent forms of gender-based violence, is a **complex, multicausal and multidimensional problem** with social roots that go beyond the mere intermediation of technology and for which there is no single solution; rather, a **multidisciplinary approach and the participation of various sectors is required.**

Second, based on national experiences with intervention models to combat gender-based violence outside the Internet, it will be important to **adopt a comprehensive, holistic vision, taking into account the individual, family, community and social planes, as well as the global effects** that gender-based violence has on women's effective access to new technologies and, therefore, on the development of a fairer and more egalitarian Internet that can benefit all societies.

Third, as has been reaffirmed at the international level, it is essential to keep in mind that **women's human rights must be protected both on and off the Internet** and, in particular, to recognize the role that the right of women to equal and non-discriminatory access to the Internet plays in the digital revolution.

Finally, it will be crucial to work with a mindset of advancing **the digital empowerment of women and their online safety** by approaching this issue from standpoint that promotes their digital autonomy, recognizes their diversity, and questions models that treat women as irremediable victims of online aggression and cybercrime, denying them their fundamental right to safety and their freedom to surf the Internet.

Without question, empowering girls and women of all ages to break down the barriers that separate them from technology and to develop strategic thinking about their safety online is a key strategy that should drive collective efforts in the near term. This is precisely the premise under which this guide has been structured and on which basis it is hoped to continue promoting more interventions in this area.

B

What is being done in Latin American and Caribbean countries?

In recent years, several countries in Latin America and the Caribbean have begun to gradually recognize online violence against women and have updated their legal framework to address it, including the enactment of specific laws on cyberstalking, cyberharassment, grooming and cyberbullying.

In particular, largely due to media attention and public demands, there have been significant legislative developments throughout the Americas with regard to the non-consensual distribution of intimate or sexually explicit images (Neris et al., 2018).

In Paraguay, Law 19.580, enacted in 2017, recognized telematic violence, which is defined as the dissemination or publication through ICTs of audiovisual material that adversely affects the dignity or privacy of women. Brazil enacted Law 13.772/2018 in December 2018, criminalizing the unauthorized recording, storage, and exposure of nude or sexual content. According to the law, cases of domestic violence are those in which there was a pre-existing relationship between the victim and the perpetrator. It also has Law 13.718/18, which criminalizes the crime of dissemination of images of sexual violation.

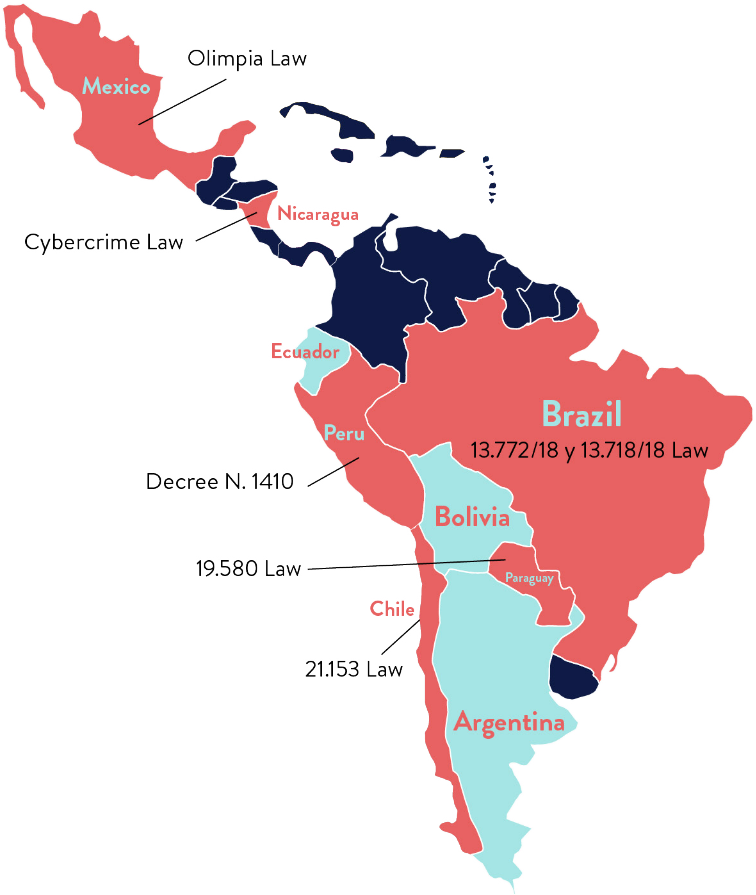
By Legislative Decree No. 1410 of September 2018, Peru incorporated into its Criminal Code the crimes of harassment, sexual harassment, sexual blackmail, and dissemination of images, audiovisual materials, or audios with sexual content by means of ICTs. For its part, Chile adopted in 2019 Law 21.153, criminalizing the unauthorized dissemination of intimate material or images recorded in public places without consent. In October 2020, Nicaragua adopted the Cybercrime Law, which punishes threats and harassment by means of new technologies, as well as the dissemination of sexually explicit material.

In Mexico, 28 local legislatures have already adopted a total of 35 legislative reforms criminalizing non-consensual distribution of intimate images. At the federal level, in April 2021, a series of legislative amendments were approved to the Federal Criminal Code and the General Law on Women's Access to a Life Free from Violence, which recognize digital violence and criminalize the offense of violating the sexual intimacy of individuals through the non-consensual distribution of intimate sexual material. This series of reforms has been dubbed the "Olimpia Law" following the work carried out for the recognition of this form of digital violence by Olimpia Melo Cruz, who in 2014 was the victim of the unauthorized dissemination of a video with sexual content[20].

In Argentina, the Commission for the Reform of the new Criminal Code proposed the incorporation of dissemination and recording of sexual content without consent as a cybercrime; this conduct is currently only punishable in the case of minors. The Misdemeanor Code of Buenos Aires already recognizes non-consensual dissemination of intimate images or recordings and digital harassment as offenses.

Other proposed laws related to this form of violence are under consideration in Bolivia, Ecuador, and Chile.

In recent years several countries have seen progress in the formation of police bodies specializing in cybercrime that can investigate acts of online violence against women. **Mexico's Federal Police** has a Scientific Division that investigates domestic cybercrime and handles cases of online violence. Likewise, the Office of the Attorney General of Mexico City established the Gender Violence Cybercrime Unit[21], in addition to an online government portal to raise awareness about cyberharassment. There are also specialized agencies in the **Colombian National Police**, which has a Cyber Police Center, and in **Brazil**, which has an **Office for the Repression of Cybercrime in the Federal Police** (in addition to specialized police departments in some states). **Argentina** has a **Technological Crimes Division in the Federal Police**; **Bolivia** has an **Agency for the Development of the Information Society**, which is the lead agency for managing security issues, and **Paraguay** has a **Specialized Unit for Cybercrimes.** Finally, the **Peruvian Ministry of Women and Vulnerable Populations** has a digital platform for reporting incidents of online harassment[22].



[20] Orden Jurídico. *Ficha Técnica Ley Olimpia* [Fact Sheet on the Olimpia Law]. Available at: http://ordenjuridico.gob.mx/violenciagenero/LEY%20OLIMPIA.pdf

[21] Alejandra Balandrán Olmedo (2020). "Atenderá FGJCDMX ciberdelitos de violencia de género" [FGJCDMX shall tackle crimes of online gender-based violence]. *Diario ContraRéplica*. Available at: https://www.contrareplica.mx/nota-Atendera-FGJCDMX-ciberdelitos-de-violencia-de-genero202028854

[22] Ministry of Women and Vulnerable Populations. *Ponte alerta ante el acoso virtual* [Be alert to online harassment]. Available at: http://www.noalacosovirtual.pe/alerta.html

D

Explore further

The provision of the following resources does not constitute an endorsement by the OAS or its member states of their content or of organizations mentioned. The resources are presented as examples of organizations, guides, tools, etc., that are available in the region, so that readers can obtain more information about the subject matter addressed in this publication.

Organizations, websites and support:

Acoso.online (site that provides useful tools and information for cases of nonconsensual posting of intimate images and videos)

Asociación para el Progreso de las Comunicaciones (APC)

Ciberfeministas Guatemala

Ciber Civil Rights Initiative

Ciberseguras

Cl4ndestina (Brazil)

Coding Rights(Brazil)

Crash Override Network

Datos Protegidos (Chile)

Datysoc (Uruguay)

Derechos Digitales (Latin America)

Dominemos la Tecnología

Feminist Frequency

Frente Nacional para la Sororidad y Defensoras Digitales

Fundación Datos Protegidos

Fundación Activismo Feminista Digital

Fundación InternetBolivia.org (Bolivia)

Fundación Karisma (Colombia)

GenderIT.Org

HeartMob

Hiperderecho (Peru)

Internet es Nuestra

InternetLab (Brazil)

La <clika> libres en línea

Luchadoras (Mexico)

MariaLab (Brazil)

Nodo Común

ONG Amaranta (Chile)

R3D (Mexico)

Safernet (Brazil)

SocialTIC

SOS Digital (Bolivia)

TEDIC (Paraguay)

The Atlas of Online Harassment

Without My Consent

Guides:

A First Look at Digital Security. Access Now.

Alfabetización y Seguridad Digital: La Importancia de Mantenerse Seguro e Informado [Media Literacy and Digital Security: The Importance of Keeping Safe and Informed] (2021). Organization of American States and Twitter.

Alfabetismo y Seguridad Digital. Mejores Prácticas en el uso de Twitter. [Media Literacy and Digital Security: Twitter Best Practices] (2019). Organization of American States and Twitter.

Alza la voz y ten cuidado: Guía para protegerte del acoso online. Speak Up & Stay Safe(r): Guide to Protecting Yourself from Online Harassment (2018). Feminist Frequency.

Ciberseguridad de las mujeres durante la pandemia de COVID-19: Experiencias, riesgos y estrategias de autocuidado en la nueva normalidad digital. [Cybersecurity of women during the COVID-19 pandemic: Experiences, risks, and self-care strategies in the new digital normal]. Organization of American States, 2021.

Cuidados durante la pandemia: ¿Cómo denunciar la violencia doméstica? [Care during the pandemic: How to report domestic violence?] (2020). Derechos Digitales and MaríaLab. .

Cuidar nuestr@ cuerp@ digital. Reflexiones de un equipo virtual. [Taking Care of our Digital Body: Thoughts of a Virtual Team]. Fondo de Acción Urgente [Emergency Action Fund].

Data Detox x Youth. Tactical Tech.

Guía de Seguridad Digital para Feministas Autogestivas. [Digital Security Guide for Self-Managing Feminists].

Guía breve para la cobertura periodística de la violencia de género online (2020). [Brief guide for journalistic coverage of online gender-based violence]. Acoso.online.

Guía práctica para tratar casos de pornografía no consentida en recintos educacionales (2018). [Practical guide for tackling cases of nonconsensual pornography on school premises]. Acoso.online.

Netizens Online Security Guide.

Online Harassment Field Manual. (2019) PEN America.

Security in a Box (2020). Tactical Tech, Front Line Defenders.

Surveillance Self-Defense. Electronic Frontier Foundation.

Reports:

Cyber Violence against Women and Girls. A World-Wide Wake-up Call. United Nations Broadband Commission for Digital Development (UNBC). Working Group on Broadband and Gender (2015).

(In)Seguras Online. Experiencias de niñas, adolescentes y jóvenes en torno al acoso online [Free To Be Online? Girls' and young women's experiences of online harassment] (2020). Plan International.

Informe acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos [Report of online violence against women and girls from a human rights perspective](2018). United Nations Special Rapporteur on violence against women, its causes and consequences.

La ciberviolencia contra mujeres y niñas Cyber violence against women and girls] (2017). European Institute for Gender Equality (EIGE).

Online and ICT facilitated violence against women and girls during COVID-19 (2020). UN Women.

Reporte de la Situación de América Latina sobre la Violencia de Género Ejercida por Medios Electrónicos [Report on the Situation of Latin America regarding Gender-based Violence Inflicted by Electronic Media] (2017). Paz Peña Ochoa (ed).

Ser periodista en Twitter. Violencia de Género digital en América Latina [Being a Journalist on Twitter: Digital Gender Violence in Latin America] (2020). Sentiido-Colombia, Communication for Equality, and the International Programme for the Development of Communication (IPDC) of the United Nations Educational, Scientific and Cultural Organization (UNESCO).

Toxic Twitter - A Toxic Place for Women (2018). Amnesty International.

Violencia en línea: La nueva línea de combate para las mujeres periodistas - #JournalistsToo [Online Violence: The New Line of Battle for Women Journalists - #JournalistsToo] (2021). UNESCO and the International Center for Journalists.

TED events and documentaries:

How Online Abuse of Women Has Spiraled Out of Control. Ashley Judd. TEDTalk, 2016.

Anita Sarkeesian at TEDxWomen 2012.

The problem with "Don't Feed the Trolls". Steph Guthrie, TEDxToronto.

Grooming, el acoso ¿virtual? [Grooming: online harassment?]. Sebastián Bortnik, TEDxRíodelaPlata, 2016.

Netizens. Cynthia Lowen, 2019.

Glossary of Terms

Application (*a.k.a.* app). An app is a computer program created to perform or facilitate a set of specific tasks (professional, leisure-related, educational, etc.) that runs on smartphones, tablets and other mobile devices. There are free and paid applications, and they are generally available on specific distribution platforms or through the companies that own the operating systems of electronic devices.

Internet Blackout. An outage on the Internet caused by an attack on a website, an Internet service provider (ISP) or the Internet's domain naming system (DNS). An outage can also be due to an improper configuration of the Web server infrastructure.

Blog. A website that allows the creation and publication of short articles on specific or off-the-cuff topics.

Chat: Real-time digital communication between two or more users whose computers are connected to a network.

Cybermob**:** An organized online group that posts offensive or destructive content en masse with the intention of shaming individuals or getting their social network profiles taken down.

Creepshot**:** A photo taken by a man of a woman or girl in public without her consent. The photos usually focus on the victim's buttocks, legs or cleavage.

Cyberflashing**:** Sending obscene photos to a woman without her consent with the intention of annoying, intimidating or embarrassing her.

Deepfake video: Artificial intelligence technique that allows the production of phony videos of apparently real people by means of learning algorithms and existing videos or images.

Denial of service attack: A cyberattack that aims to flood a server with service requests in order to prevent legitimate users from being able to use it. A more sophisticated method is the Distributed Denial of Service (DDoS) attack, where requests are sent in a coordinated manner from several computers.

Hate speech: The use of language that denigrates, insults, threatens, or attacks a person because of their identity and/or other characteristics, such as sexual orientation or disability.

Gender-based discrimination: Any distinction made on the basis of sex which has the effect or purpose of impairing or nullifying the recognition, enjoyment or exercise by women, irrespective of their marital status, on a basis of equality of men and women, of human rights and fundamental freedoms in the political, economic, social, cultural, civil or any other field. [Source: Convention on the Elimination of All Forms of Discrimination against Women, Article 1.]

Downblousing**:** The making of unauthorized photographs down the top of a woman's blouse.

Doxing or doxxing: The term comes from the expression "dropping docs" and consists of the unauthorized online extraction and publication of personal information.

Gender stereotypes: A generalized opinion or preconception about attributes or characteristics, or the roles that are or ought to be possessed by, or performed by, women and men. [Source: OHCHR, Gender stereotyping.]

Gaslighting: A form of psychological abuse by which the perpetrator manipulates the victim's reality in order to make them question their sanity, memory, or perception.

Geolocation: The ability to ascertain the geographic location of an object, such as a radar, a cell phone or a computer connected to the Internet.

Gender: refers to the roles, behaviors, activities, and attributes that a given society at a given time considers appropriate for men and women. Gender also refers to relations between women and those between men. These attributes, opportunities, and relationships are socially constructed and are learned through the socialization process [Source: UN Women, *OSAGI Gender Mainstreaming - Concepts and definitions*].

Grooming: Deliberate acts by an adult to approach a child in order to establish a relationship and emotional control that allows them to commit sexual abuse, engage in virtual sex, obtain child pornography, or traffic the child.

Hacking: Techniques and procedures used by a hacker to gain unauthorized entry into another's computer system for the purpose of manipulating it or obtaining information or for fun. *Cracking* is a practice related to *hacking* but involves breaking into other people's systems for criminal purposes in order to violate the privacy of the affected person or the confidentiality of information, or to damage information or hardware.

Hacker: A person who gains unauthorized access to a computer system.

Hashtag: String of characters starting with the "#" symbol. It is used on social networks to indicate the subject of a conversation or message. It also allows the automatic creation of a hyperlink that provides access to all content that includes the *hashtag* in question.

Internet of Things (IoT): Refers to the network of Internet-connected devices and everyday objects that can share data with each other.

Gender equality: The equal rights, responsibilities and opportunities of women and men and girls and boys. [Source: UN Women, *OSAGI Gender Mainstreaming - Concepts and definitions.*]

Keylogger: A malicious software that places itself between the keyboard and the operating system to intercept and record information about every key pressed on the device without the user's knowledge.

Malware: The term comes from the union of the words *malicious software* and refers to a type of *software* designed to infiltrate and/or damage an information system without the user's consent.

Outing: The online disclosure of a person's sexual identity or preference.

Packs: A set of images of women of an intimate or sexual nature obtained and/or distributed without their consent.

Gender perspective: An analysis mechanism that consists of observing the impact of gender on people's opportunities, roles, and social interactions. [Source: UN Women, *OSAGI Gender Mainstreaming - Concepts and definitions.*]

Revenge porn: Term used incorrectly to refer to the non-consensual distribution of intimate images or videos.

Social network: An information-society service that offers users an Internet-based communication platform to generate a profile with their personal data, facilitating the creation of communities based on common criteria and allowing communication whereby users can interact through messages and post information, images or videos that are immediately accessible by all the people in a group.

Gender roles: Social and behavioral norms that, within a specific culture, are widely considered to be socially appropriate for individuals of a specific sex These often determine the traditional responsibilities and tasks assigned to men, women, boys and girls. [Source: UNICEF, UNFPA, UNDP, UN Women. *Gender Equality, UN Coherence and you.*]

Biological sex: Refers to the biological characteristics that define human beings as women and men.

Sexting: A practice that involves the generation and sharing of sexually explicit material between two people. It may include consensual creation and sending of images or consensual creation of images that are distributed without consent.

Sextortion: Consists of threatening to disseminate intimate images or videos of a person in order to obtain more material about sexually explicit acts, engage in sexual intercourse, or obtain money (REVM-UN, 2018).

Software: A set of computer programs, instructions, and rules that enable electronic devices to perform certain tasks.

Spyware: A type of malicious program that infects a device and, without consent, secretly records browsing data, personal information, device location, call or message logs, and other personal data.

Trending topic: Refers to the most repeated word or phrases in social networks at a given time.

Troll: A person with an unknown identity who posts messages online with the intent to annoy, provoke an emotional response, or disrupt online conversations.

Gender trolling: The posting of messages, images or videos, as well as the creation of *hashtags*, with the purpose of annoying women and girls or inciting violence against them.

Upskirting: The making of unauthorized photographs beneath a woman's or girl's skirt.

Violence against Women: Any act or conduct, based on gender, which causes death or physical, sexual or psychological harm or suffering to women, whether in the public or the private sphere. [Source: Inter-American Convention on the Prevention, Punishment, and Eradication of Violence against Women, Article 1.]

Online gender-based violence or gender-based cyber-violence against women: Any act of gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of information and communication technologies, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately. [Source: United Nations Special Rapporteur on violence.]

Bibliografía

Abdul Aziz, Z (2017). Due Diligence and Accountability for Online Violence against Women. APC Issue Papers, Consultado el 9 de septiembre de 2020.

Agencia de los Derechos Fundamentales de la Unión Europea (FRA) (2014). Violencia de género contra las mujeres: una encuesta a escala de la UE. Consultado el 9 de septiembre de 2020.

Amnesty International (2018). Toxic Twitter-A Toxic Place for Women. Consultado el 9 de septiembre de 2020.

--- (2017). *Amnistía revela alarmante impacto de los abusos contra las mujeres en Internet.* Consultado el 9 de septiembre de 2020.

Amnistía Internacional (2019). Corazones Verdes. Violencia online contra las mujeres durante el debate por la legalización del aborto en Argentina. Disponible en: https://amnistia.org.ar/corazonesverdes/files/2019/11/corazones_verdes_violencia_online.pdf

Association of Progressive Communications (APC) (2017). *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.*

--- (2015). Briefing paper on VAW. APC Women's Rights Programme. Consultado el 9 de septiembre de 2020.

Barrera, L. (coord) (2017). *La Violencia en Línea contra las Mujeres en México.* Informe para la Relatora Especial sobre la violencia contra la mujer. Luchadoras, México.

Citron, D. (2014). *Hate Crimes in Cyberspace.* Massachusetts: Harvard University Press.

Comité para la Eliminación de la Discriminación contra la Mujer de las Naciones Unidas (Comité CEDAW) (2017). CEDAW/C/GC/35. Recomendación general núm. 35 sobre la violencia por razón de género contra la mujer, por la que se actualiza la recomendación general núm. 19. Consultado el 9 de septiembre de 2020.

--- (1992). A/47/38. Recomendación General No. 19. La Violencia contra la Mujer. Consultado el 9 de septiembre de 2020.

Comisión Interamericana de Mujeres (CIM) (2020). COVID-19 en la vida de las mujeres. Razones para reconocer los impactos diferenciados. Consultado el 9 de septiembre de 2020.

Cuellar, L y Sandra Chaher (2020). *Ser periodista en Twitter. Violencia de género digital en América Latina.* Fundación Sentiido, Comunicación para la Igualdad Ediciones, UNESCO.

Deeptrace (2019). The State of Deepfakes: Landscape, Threats and Impact. Consultado el 9 de septiembre de 2020.

Derechos Digitales América Latina (2020). *COVID-10 and the increase of domestic violence against women in Latin America: A digital rights perspective.* Documento presentado por Derechos Digitales a la Relatora Especial de las Naciones Unidas sobre la violencia contra la mujer, sus causas y consecuencias.

Dragiewicz, H., Woodlock et. al (2019) *Domestic violence and communication technology: Survivor experiences of intrusion, surveillance, and identity crime.* Brisbane: Queensland University of Technology.

Edwards, A. (2010). "Feminist Theories on International Law and Human Rights". En *Violence against Women under International Human Rights Law*, 36-87. Cambridge: Cambridge University Press.

Fanti K., A. G. Demetriou, y V. Hawa. (2012). "A longitudinal study of cyberbullying: Examining risk and protective factors". En *European Journal of Developmental Psychology*, Vol. 9(2), 168-181.

Federal Bureau of Investigation. Internet Crime Complaint Center (FBI-ICC) (2018). Internet Crime Report. Consultado el 9 de septiembre de 2020.

Fondo de las Naciones Unidas para la Infancia (UNICEF) (2017). Access to the Internet and Digital Literacy. Consultado el 9 de septiembre de 2020.

Freed, D., J, Palmer, D. Minchala, et al. (2017). "Digital technologies and intimate partner violence: a qualitative analysis with multiple stakeholders". En *Proceedings ACM Human-Computer Interaction*, Vol. 1, 46:1- 46:22.

Goldsman, F. y G. Natansohn (2020). *Cuidados durante la pandemia: ¿Cómo denunciar la violencia Doméstica?* Derechos Digitales y María Lab.

Henry, N. y A. Powell (2018). "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research". En *Trauma, Violence, & Abuse*, Vol. 19 (2), 195-208.

Henry, N. y A. Powell (2017). "Sexual Violence and Harassment in the Digital Era". En Antje Deckert y Rick Sarre (eds.). *The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice.* Palgrave Macmillan.

Henry, N. y A. Powell (2016). "Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law". En *Social & Legal Studies*, Vol. 25 (4), 397-418.

Henry, N., A. Powell y F., Asher (2018). *"AI can now create fake porn, making revenge porn even more complicated"*. En *The Conversation*.

--- (2017). Not just "revenge pornography": Australians' experiences of image-based abuse: A summary report. Gender Violence and Abuse Research Alliance (GeVARA). Centre for Global Research, Centre for Applied Social Research.

Harris, B. (2018). "Spacelessness, spatiality and intimate partner violence: Technology-facilitated abuse, stalking and justice". En K. Fitz-Gibbon, S. Walklate, J. McCullough, y J. Maher (eds.), *Intimate partner violence, risk and security: Securing women's lives in a global world* (pp. 52–70). Londres: Routledge.

Hinduja, S., y J. W. Patchin (2014). *Bullying Beyond the Schoolyard: Preventing and Responding to Cyberbullying* (Second edition). Thousand Oaks, California: Corwin.

Hinson L., J. Mueller, L. O'Brienn-Milne, N. Wandera (2018). *Technology-facilitated gender-based-violence: What is it, and how to we measure it?* Washington D.C., International Center for Research on Women.

Interagency Working Group (2016). "Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse". En *ECPAT International and ECPAT Luxembourg*, Luxemburgo. Consultado el 9 de septiembre de 2020.

Internet Governance Forum (IGF) (2015). 2015: Best Practice Forum (BPF) on Online Abuse and Gender-Based Violence against Women. Consultado el 9 de septiembre de 2020.

Instituto Europeo de la Igualdad de Género (EIGE) (2017). La ciberviolencia contra mujeres y niñas. Consultado el 9 de septiembre de 2020.

Jane, E. (2017). *Misogyny Online*. A Short (and Brutish) History. Londres: Sage Publications.

Jane E. (2016). "Online Misogyny and Feminist Digilantism". En *Continuum. Journal of Media & Cultural Studies*, Vol. 30 (3), 284-297.

Kelly, L. (1988) *Surviving Sexual Violence*. Cambridge: Polity.

Knight, W. (2018). "The Defense Department has produced the first tools for catching deepfakes". En *MIT Technology Review*. Consultado el 9 de septiembre de 2020.

Kwon, M., Y. S. Seo, S. S. Dickerson, E. Park, y J. A. Livingston (2019). "Cyber Victimization and Depressive Symptoms: A Mediation Model Involving Sleep Quality". En *Sleep*, 42(Supplement_1), A322–A322.

Qing Li (2006). "Cyberbullying in schools: a research of gender differences". En *School Psychology International*, Vol. 27(2), 157-170.

Mantilla. K. (2013). "Gendertrolling: misogyny adapts to new media". En *Feminist Studies*, Vol. 39(2), 563–570.

Maras, M. (2016). *Cybercriminology*. Oxford University Press.

Maras, M., y A.Alexandrou (2018). "Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deepfake Videos". En *International Journal of Evidence and Proof*, Vol. 23(3), 255-262.

Mecanismo de Seguimiento de la Convención de Belém do Pará (MESECVI). Comisión Interamericana de Mujeres (2017). Tercer Informe Hemisférico sobre la Implementación de la Convención de Belém do Pará. Consultado el 9 de septiembre de 2020.

Salter M., T. Crofts y M. Lee (2013). "Beyond Criminalisation and Responsibilisation: Sexting, Gender and Young People". En *Current Issues in Criminal Justice*, Vol. 24 (3), 301-316.

Navarro, J. y J. L. Jasinski (2012). “Going Cyber: Using Routine Activities Theory to Predict Cyberbullying Experiences”. En *Sociological Spectrum*, Vol. 32(1), 81-94.

Neris, N., J. Ruiz y M. Valente (2018). Enfrentando Disseminação Não Consentida de Imagens Íntimas: Uma análise comparada. InternetLab. Consultado el 9 de septiembre de 2020.

Oficina de Naciones Unidas para la Droga y el Delito (UNODC) (2015). Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children. Consultado el 9 de septiembre de 2020.

--- (2019). University Module Series. Cybercrime. Module 12. Interpersonal Crime.
Organización de las Naciones Unidas. Asamblea General (2018). Intensificación de los esfuerzos para prevenir y eliminar todas las formas de violencia contra las mujeres y las niñas: el acoso sexual. A/C.3/73/L.21/Rev.1. Consultado el 9 de septiembre de 2020.

---. Consejo de Derechos Humanos (2018). Acelerar los esfuerzos para eliminar la violencia contra las mujeres y las niñas: prevención de la violencia contra las mujeres y las niñas en los contextos digitales. A/HRC/38/L.6. Consultado el 9 de septiembre de 2020.

---. Comisión de la Banda Ancha para el Desarrollo Sostenible (UNBC-UN) (2015). Working Group on Broadband and Gender. Cyber Violence against Women and Girls. A World-Wide Wake-up Call. Consultado el 9 de septiembre de 2020.

Organización de Estados Americanos (OEA) (2019). Media Literacy and Digital Security: Twitter Best Practices. Consultado el 9 de septiembre de 2020.

Peña Ochoa, P. (ed) (2017). *Reporte de la Situación de América Latina sobre la Violencia de Género Ejercida por Medios Electrónicos.* Presentación para la Relatora Especial sobre la violencia contra la mujer.

Pew Research Center (2014). Online Harassment 2014. Consultado el 9 de septiembre de 2020.

--- (2017). Online Harassment 2017. Consultado el 9 de septiembre de 2020.

Powell, A., N. Henry, y F. Asher (2018). “Image-based Sexual Abuse”. En Walter DeKeseredy and Molly Dragiewicz (eds.) *Handbook of Critical Criminology.* Nueva York: Routledge.

Relatora Especial de las Naciones Unidas sobre la Violencia contra la Mujer, sus Causas y Consecuencias (REVM-ONU) (2018). A/HRC/38/47. *Informe acerca de la violencia en línea contra las mujeres y las niñas desde la perspectiva de los derechos humanos.* Consultado el 9 de septiembre de 2020. https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session38/Documents/A_HRC_38_47_EN.docx

Relator Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (RELE) (2018). *Mujeres periodistas y libertad de expresión: Discriminación y violencia basada en el género contra las mujeres periodistas por el ejercicio de su profesión* (OEA/Ser.L/V/II), párr. 48. Disponible en: http://www.oas.org/es/cidh/expresion/docs/informes/MujeresPeriodistas.pdf

Reyns, Bradford, Billy Henson y Bonnie S. Fisher (2011). “Being pursued online. Applying Cyberlifestyle-Routine activities theory to cyberstalking victimization”. En *Criminal Justice and Behavior*, Vol. 38(11), 1149-1169.

Salter, M. y T. Crofts y M. Lee (2013). “Beyond Criminalisation and Responsibilisation: Sexting, Gender and Young People”. En *Current Issues in Criminal Justice*, Sydney Law School Research Paper No. 13/38, Vol. 24(3), 301-316.

Segrave, M., y L. Vitis (2017), *Gender, Technology and Violence.* Oxon y Nueva York: Routledge.

Smith, Peter K. (2012). “Cyberbullying and cyber aggression”. En S.R. Jimerson, A.B. Nickerson, M.J. Mayer, y M.J. Furlong. (eds). *Handbook of school violence and school safety: International research and practice* (pp. 93-103). Routledge.

Van Der Wilk, A. (2018). *Cyber violence and hate speech online against women.* Estudio encargado por el Departamento Temático de Derechos de los Ciudadanos y Asuntos Constitucionales del Parlamento Europeo. Bruselas: Parlamento Europeo.

Vela, E. y E. Smith. “La violencia de género en México y las tecnologías de la información”. En *Internet en México: Derechos Humanos en el entorno digital.* Ed. Juan Carlos Lara. México: Derechos Digitales, 2016. Consultado el 9 de septiembre de 2020.

Walker, Shelley, Sanci, Lena y Temple-Smith Meredith (2013). “Sexting: Young women’s and men’s views on its nature and origins”. En *Journal of Adolescent Health*, Vol. 52, 697-701.

Web Foundation (2018a). Advancing Women's Rights Online: Gaps and Opportunities in Research and Advocacy. Consultado el 9 de septiembre de 2020.

Web Foundation (2018b). *Measuring the digital divide: Why we should be using a women-centered analysis.* Consultado el 9 de septiembre de 2020.

Women's Aid (2014). *Virtual World, Real Fear. Women's Aid report into online abuse, harassment and stalking.*

Women's Media Center (2019). *Online Abuse 101.* Consultado el 9 de septiembre de 2020,

Woodlock D (2017). "The abuse of technology in domestic violence and stalking". En *Violence Against Women*, Vol. 23(5, 584-602.

Online gender-based violence against women and girls

Guide of basic concepts

ISBN 978-0-8270-7306-7

OAS | CICTE

OAS | CIM | MESECVI