

# Online gender-based violence against women and girls

*Practical self-protection handbook: digital security tools and response strategies*



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 

## 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

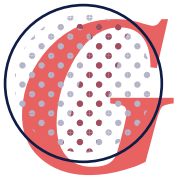
1. Girls--Violence against. 2. Women--Violence against. 3. Computer security. 4. Computer crimes. 5. Girls--Crimes against. 6. Women--Crimes against. I. Title: Practical self-protection handbook: digital security tools and response strategies. II. Inter-American Commission of Women. III. Inter-American 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

<b>Introduction</b>	<b>05</b>
<b>Part 1. Basic concepts: Recognizing digital violence is the first step in combating it</b>	<b>06</b>
A. What is online gender-based violence against women?	07
B. What are the consequences for women and girls who are victims of online violence?	13
C. Who are the aggressors?	15
<b>Part 2. Overview of the types of gender-based violence against women and girls facilitated by new technologies</b>	<b>17</b>
A. Creation, dissemination, distribution, or exchange, online and without consent, of photographs, videos, or audio clips of a sexual or intimate nature	21
B. Unauthorized access, use, control, manipulation, sharing, or publication of private information and personal data	24
C. Identity theft and impersonation	25
D. Actions that damage a person's reputation or credibility	26
E. Surveillance and monitoring of a person	27
F. Cyberstalking or cybermolestation	28
G. Cyber harassment	29
H. Cyberbullying	32
I. Direct threats of harm or violence	33
J. Technology-facilitated physical violence	34
K. Technology-facilitated abuse, exploitation, and/or trafficking of women and girls	35
L. Attacks on women's groups, organizations, or communities	36
<b>Part 3. Self-protection and response handbook: digital security tools and response strategies for online gender violence</b>	<b>37</b>
A. Basic digital security recommendations: preventive measures	38
B. Digital safety tips for women victims of domestic or intimate partner violence	48
C. What can I do if I am a victim of digital violence?	51
D. To learn more	56
<b>Glossary of terms</b>	<b>58</b>
<b>Bibliography</b>	<b>62</b>

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 is increasingly affecting women's privacy and safety both inside and outside of cyberspace. Research indicates that **compared to men, women are disproportionately victimized by certain types of cyberviolence** (UNSRVW, 2018; EIGE, 2017). According to a 2015 study by the United Nations Broadband Commission for Sustainable Development, 73% of women had experienced some form of gender-based violence online, while 61% of their attackers were men (UNBC, 2015). Other sources report that 23% of women have experienced online harassment at least once in their lives, and it is estimated that one in ten women have experienced some form of cyberviolence since the age of 15 (UNSRVW, 2018, para. 16; EIGE, 2017: 3; AI, 2017).

Moreover, as multiple sources have shown<sup>1</sup>, this violence has been exacerbated by the travel and lockdown restrictions imposed on account of the COVID-19 pandemic: as more women and girls turn to digital venues, gender-based cyberviolence against them is increasing (UN-Women; CIM, 2020; Derechos Digitales, 2020).

The scenario surrounding this phenomenon poses multiple challenges. Information on cyberviolence against women remains scarce. Very little is known about the actual percentage of victims and the prevalence of the harm caused (EIGE, 2017). In addition, to date there is no regionally or internationally agreed definition of online gender-based violence and no precise terminology<sup>2</sup>. The responses of states and international agencies vary widely and, in general, adequate legal frameworks for victim protection are not in place.

In light of the need to raise the visibility of this phenomenon and to provide tools to strengthen women's digital security, the Cybersecurity Program of the Inter-American Committee against Terrorism (CICTE), in partnership with the Inter-American Commission of Women (CIM), has developed this practical handbook. It contains basic concepts for understanding online gender-based violence and recommendations, preventive measures, and protection strategies for dealing with it.

As can be seen from its content, this publication aims at the digital empowerment of women and girls. It is based on the premise that they can acquire the skills necessary to protect themselves individually and collectively in their online interactions and to create their own venues in the virtual world where they are free from violence, so that the internet becomes a bridge for them and not a barrier to the development of their life projects.

This manual is a part of the publication *Online gender-based violence against women and girls. Guide to basic concepts, digital security tools, and response strategies*, which should be consulted directly by anyone interested in learning about the latest developments with this issue in the Latin American region and about some of the steps that the authorities can take to prevent and combat this form of violence.

<sup>1</sup> UN-Women (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 to Recognize the Differential Impacts*. Available at: <https://www.oas.org/es/cim/docs/ArgumentarioCOVID19-EN.pdf>.

<sup>2</sup> As noted by the United Nations Special Rapporteur on violence against women, there is still no consensus on terminology for this form of violence. "Violence against women facilitated by information and communications technologies (ICTs)" is perhaps the most inclusive, as it encompasses the vast range of behaviors that this form of violence can assume. However, following common usage, the terms "ICT-facilitated violence," "online violence against women," "digital violence," and "cyberviolence against women" will be used interchangeably throughout this publication.

# Part *One*

---

*Basic concepts:*

**RECOGNIZING**

**DIGITAL VIOLENCE**

**IS THE FIRST STEP IN**

**COMBATING IT**





## *What is online gender-based violence against women?*

### Basic elements of online violence against women:

---

01

This is not a new phenomenon: it stems from a context of gender discrimination and systemic violence against women in all areas of their lives.

It is not disconnected from “offline” violence: it is part of the series of multiple, interrelated, and recurring forms of violence against women and girls that now permeate through and across the online and offline worlds.

02

03

It entails various violations of the human rights of women and girls.

It is a dynamic phenomenon that encompasses a wide range of violent practices that are facilitated or reshaped by information and communication technologies (ICTs).

04

05

It causes psychological, physical, sexual, and/or economic harm and suffering to its victims, and it has family, social, and collective repercussions.

Online violence against women is not an isolated phenomenon: **it is an aspect of a broader social context of gender inequality and discrimination against women and girls.** Hence, in order to understand digital violence, the crucial first step is an analysis of what gender-based violence is, since the aggressions and attacks that women experience in their online interactions are nothing more than an extension of the violence that has affected them for years in all aspects of their lives.

## What is gender-based violence against women and girls?

The Convention of Belém do Pará defines violence against women as “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, General Recommendation 19, para. 6).



**Gender-based violence against women stems from stereotypes and prejudices** about the attributes and characteristics of men and women and from expectations of the social roles that both are supposed to play (for example, that women are solely responsible for housework, that they do not have enough 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 lead to discrimination against them, and these elements are the main drivers of violence against women (MESECVI, 2017, para. 37).

Crucially, this violence operates in synergy with gender inequality and not only as a consequence of it, and also as a social mechanism that seeks to keep women in a disadvantaged situation. This means that violence is in many cases used to “punish” or “correct” women whose attitudes or activities are perceived as contrary to society’s expectations of them (MESECVI, 2017, para. 36).

The United Nations has stated that violence against women is a pervasive problem in all the world’s countries and represents a systematic and widespread violation of human rights, with a high degree of impunity.



Women and girls experience gender-based violence over the years in all the offline and online venues they attend and participate in: at home, at school, at work, on public roads, in politics, in the media, in sports, at public institutions, or when surfing social media (CEDAW, General Recommendation 35). This violence, which knows no borders, is directed against all women simply because they are women and **has a greater impact on certain groups of women because they suffer forms of intersectional discrimination**, including indigenous, migrant, disabled, lesbian, bisexual, and transgender women (MESECVI, 2017).

Online violence has changed since the inception of the internet, and it will undoubtedly continue to evolve as digital platforms and technological tools develop and become more and more intertwined in our lives.



One of the most important achievements for women has been the recognition that **violence committed against them is not a private problem**. It is rather a matter of public concern and a violation of human rights recognized in international instruments and in national laws that stipulate the state's obligation to prevent, address, investigate, remedy, and punish it (Edwards, 2010). Within the inter-American system, the right of women to live a life free of violence is enshrined 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 topic that elevated the fight against gender-based violence against women to the level of a problem of regional concern<sup>3</sup>.

## What is online violence against women?



In 2018, the United Nations Special Rapporteur on violence against women defined online violence against women 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**” (UNSRVW, 2018, para. 23).

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

Online violence against women can be facilitated by algorithms and technological devices such as cellphones, smartphones, tablets, computers, geolocation systems, audio devices, cameras, or virtual assistants.



This violence can be seen on a wide variety of internet platforms: for example, social networks (Facebook, Twitter, Tik Tok), email services, instant messaging applications (WhatsApp), dating apps (Tinder, Grindr, Hinge, Match.com), online videogames, content sharing sites (Reddit), online discussion forums (in the comments sections of newspapers), or user-generated platforms (blogs, photo and video sharing sites).

<sup>3</sup> 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>

Gender-based cyberviolence is a constantly evolving concept. As recognized by the United Nations Special Rapporteur, rapid technological transformations shape online violence, and new and different manifestations of violence emerge as digital spaces transform and disrupt offline life (UNSRVW, 2018, para. 24).

## 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 (UNSRVW, 2018).

Care is needed to avoid the mistake of viewing online violence as a separate phenomenon from violence in the “real” world, since it is a part of the ongoing and interconnected manifestations of violence that women already experience offline.



At play here is **an age-old system of domination and gender violence that is now using 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 seen as a **continuum of violence in the lives and experiences of women around the world** (and not merely as sporadic or abnormal occurrences), ranging from acts expressly recognized as crimes to patterns of control and domination so common that they have become normalized (Kelly, 1989).

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

Thus, in the current context, where cyberspace and offline life are increasingly intertwined, violence against women has arrived in the digital world as an extension of the continuum of violence that is part of the everyday experience of women and girls (Kelly, 1988; Powell, Henry, and Flynn, 2018).

It can be seen that, in the digital era, forms of gender-based violence persist or are amplified through the use of new technologies, and that new forms of online sexism and misogyny that are emerging are capable of escaping the realm of cyberspace and producing physical attacks on women. Violence against women can, for example, begin as sexual harassment on the street, as “honor-based” violence in a community, or as physical aggression perpetrated by an intimate partner, and it can be transformed and relocated through technology into the non-consensual distribution of intimate images, Cyber harassment, sexist hate speech on social networks, cellphone monitoring, etc. Conversely, violence may begin as an underage girl’s exchanges on social networks with supposed new friends and culminate in encounters where sexual violence or abductions are committed. All of these new manifestations impact women’s interactions not only online but in all the venues of their offline lives.

In many cases, gender-based violence has intensified as digital forums offer a very convenient anonymity and abuse can be committed from anywhere, across a wide range of new technologies and platforms that perpetrators of violence have at their fingertips, and with the rapid spread and permanence that characterize digital content.

Some aspects of the new ICTs that have contributed to the transformation of gender-based violence against women are their fast spreading nature, the permanence online of content that leaves an indelible digital record, their replicability and global reach, and the possibility of easily locating people and information about them, which facilitates the aggressors’ contact with the victims and their secondary victimization (UNSRVW, 2018).



Close-up:

## The tight relationship between intimate partner violence and new technologies



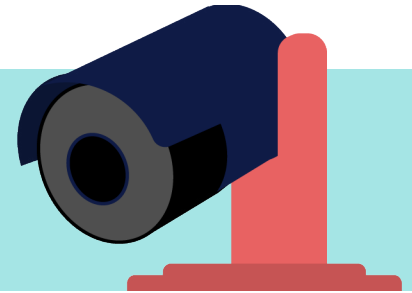
For several years now, ICTs have been playing an important role in the emergence of new strategies through which the perpetrators of domestic and intimate partner violence can abuse and exert control (Dragiewicz, 2019). Different studies have revealed that **77% of cyberharassment victims have also experienced some form of physical or sexual violence at the hands of an intimate partner** (FRA, 2014) and that at least half of them knew their online assailants (APC, 2015).

Abusers have taken advantage of the incorporation of new technologies into virtually all everyday activities, extending and intensifying abusive, possessive, and controlling behaviors in a way that was not previously possible (Woodlock, 2017). As a result, women now experience violence that knows no constraints of space and time and with the feeling that the attackers are omnipresent (Harris, 2018), which has a serious impact on their mental health<sup>4</sup>.

<sup>4</sup> 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>

Although research on the subject is still in its infancy, several early studies indicate that some technologies are used more than others for abuse and cybercontrol in situations of domestic or intimate partner violence: examples include text messages, social networks such as Facebook, or software that monitors victims' locations through their cellphones (Dragiewicz, 2019).

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



Observations of young couples have also revealed **new behaviors that have become normalized in the current online and offline contexts: these are cloaked with ideas and myths of romantic love, but ultimately they seek cybercontrol and to constrain women's digital lives.** Examples include:



Demanding partners' passwords and personal codes and spying on their mobile phones.

Interfering in their digital relationships with other people.



Attempting to control social media interactions, censor photos or posts, and review contacts, conversations, or online comments.



Requiring partners to show their geolocations at all times.



Forcing them to send intimate images.

This is compounded by the **exponential worldwide increase in physical violence and sexual abuse against women and girls during the COVID-19 pandemic** (UN-Women, CIM, 2019). With the lockdown measures imposed, women have been forced to remain confined with their aggressors, and for them technology has become an indispensable tool for communicating with the outside world, seeking help, and accessing care services.

In that context, supporting victims and survivors of domestic and intimate partner violence so they learn to recognize cybercontrol, protect their digital safety and integrity, and **use technology as a means of support to escape from the cycle of violence** is now essential and must be part of ecological models of prevention, care, and punishment of violence against women, involving work with families, communities, and institutions.

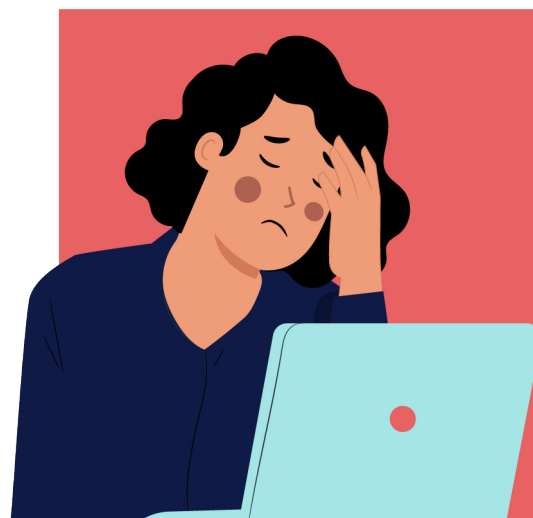


## *What are the consequences for women and girls who are victims of online violence?*

### Online violence against women causes real harm

**As a result of online violence, women and girls suffer serious psychological, physical, sexual, emotional, economic, professional, family, and social harm (UNSRVW, 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 cybermolestation, suicide attempts by women affected by the non-consensual distribution of sexual images, physical harm against victims of doxing<sup>5</sup>, or economic harm from loss of employment as a result of online acts that denigrate them (Pew Research Center, 2017; Kwon et al., 2019; Al, 2017).



It has been determined that, as part of the continuum of gender-based violence, the harm caused by online acts does not differ from the effects of offline violence: it has short- and long-term impacts on all areas of women's individual development, such as agency, privacy, trust, and integrity (Van Der Wilk, 2018).

Unfortunately, the seriousness of the consequences and harm that online violence causes to women remains inadequately understood, and that harm is often considered “not real” because it takes place 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 multiple and interrelated forms of violence that women and girls experience in their social interactions.

It has also been established that **the characteristics of certain technologies exponentially increase the magnitude of the harm caused by some acts of violence** and cause them to extend beyond the original act (such as their rapid spread, reach, anonymity, and permanence) (APC, 2017), since women are judged more harshly than men for their online activities. This is the case with the non-consensual distribution of sexual images, in which women and girls have been stigmatized for the exercise of their sexuality and, after seeing their images distributed, have been forced to live in permanent humiliation and shame in their social environment or, in extreme cases, have been driven to suicide.

<sup>5</sup> “Doxing” (or “doxing”) is a cyberattack that involves obtaining personal information about someone and making it public online.

The affected women often blame themselves for actions that may have caused the violence and withdraw from digital venues, self-censor their activities, or socially isolate themselves (Citron, 2014). In addition, it is very common for them to be revictimized by family members, authorities, and the media, who often underscore their responsibility to protect themselves instead of highlighting the aggressors' illegal conduct, thus normalizing and minimizing this violence (UNSRVW, 2018, para. 25).



In addition to its individual effects, **online violence inflicts collective and intergenerational harm** and has direct and indirect costs for societies and economies, as victims and survivors not only require medical care and legal and social services, but may also see their productivity and community interactions diminished (UNBC, 2015). Furthermore, **this violence has a silencing effect**, as it is a direct threat to women's freedom of expression (AI, 2017) and affects their online access and engagement as active digital citizens; this creates a democratic deficit by preventing women's voices from being heard freely in digital discussions (UNSRVW, 2018, para. 29).

Research into the topic indicates that 28% of women who were subjected to violence through ICTs have deliberately reduced their online presence (UNSRVW, 2018, para. 26) and self-censored for fear of violations of their privacy or safety (AI, 2017). To make matters worse, survivors are often advised to “stay away” or “withdraw” from technology after a violent incident.

Finally, this violence **contributes to the perpetuation of harmful gender stereotypes and the reproduction of systemic violence** in the new online-offline world by encouraging the development of technologies with gender bias.



## Who are the aggressors?

Observations reveal that the perpetrators of online gender-based violence against women generally identify as male (Van Der Wilk, 2018, pp. 34-37). These assailants may be someone the victim does not know (such as an online sexual harasser who systematically targets women, or individuals who practice grooming or cyberstalking<sup>6</sup>) or a member of the victim's family, professional circle, or friend group. Some studies indicate, for example, that between **40% and 50% of victims know their online attackers** (a former partner, family member, friend, or colleague) and that, **in one third of cases, the attackers have or have had an intimate relationship with the victim** (Pew Research Center, 2017; APC, 2015).

Two 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.

### The secondary perpetrator(s):

A person or group of persons who participate in the continuation and spread 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 do the perpetrators of online violence against women and girls want?

The goal of violence is to create a hostile online environment for women in order to shame, intimidate, denigrate, belittle, or silence them through surveillance, information theft or manipulation, or control of their communications channels (Al, 2018).



### Close-up:

## Online violence as a violation of women's human rights

As the United Nations Special Rapporteur on violence against women highlighted 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" (UNSRVW, 2018, para. 17).

<sup>6</sup> Cyber grooming by pedophiles consists of deliberate acts by an adult to approach a minor in order to establish a relationship and forge emotional control, allowing the adult to commit sexual abuse, engage in virtual relationships, obtain child pornography, or engage in child trafficking.

For its part, the United Nations Human Rights Council has recognized that violence in digital contexts prevents “women and girls from fully enjoying their human rights and fundamental freedoms” recognized in international law, which hinders 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 can violate include the following: (UNSRVW, 2018; Vela and Smith, 2016; APC, 2017):**

- **Right to equality and non-discrimination.**
- **Right to a life without 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 the protection of honor and reputation.**
- **Women’s sexual and reproductive rights.**

It is significant that “the prohibition of gender-based violence has been recognized as a principle of international human rights law” (UNSRVW, 2018, para. 17). This means that states have an obligation of due diligence to prevent and combat online violence against women committed by both state and non-state actors (Abdul, 2017).



# Part *two*

---

OVERVIEW OF THE TYPES OF

# GENDER-BASED VIOLENCE

AGAINST WOMEN AND GIRLS  
FACILITATED BY NEW  
TECHNOLOGIES





Online gender-based violence against women is a phenomenon that encompasses a wide variety of harmful or offensive practices and behaviors and online and offline contexts, and these undergo transformations as technology advances.

**What we understand as online violence against women in fact covers a range of very diverse practices and behaviors** that may constitute cybercrimes or unlawful acts triggering administrative, civil, or criminal liability according to the laws of each country (IGF, 2015; UNSRVW, 2018; APC, 2017).

To date, there remains a wide disparity in the terminology used to typify the various manifestations of online violence against women, with constant variations in the terms used by states, international agencies, non-governmental organizations, and academics (Van Der Wilk, 2018). This has unfortunately fueled confusion about the classification of those actions and, in many cases, has resulted in imprecise definitions in national legislation.

In an effort to clarify this scenario, **the following paragraphs present a non-exhaustive, descriptive list of behaviors and cyberattacks that can be considered online gender-based violence against women.** This is intended to facilitate the identification of personal experiences and, on that basis, to determine what measures can be taken to strengthen the victims' digital security (see part four of this Handbook).

This catalogue was compiled from a review of the literature and should not be considered fixed or static: digital violence is constantly changing in parallel to technology, and other manifestations of violence emerge as new technological tools appear (UNBC, 2015).

Furthermore, as will be noted in this section, some cases may simultaneously entail two or more forms of violence, be they interdependent (e.g., online threats followed by the non-consensual distribution of intimate images) or accompanied by other forms of offline violence (as is often the case in domestic violence cases).

In any event, such cyberattacks and online acts must be considered gender-based violence if they are directed against a victim simply because she is a woman (i.e., because of her gender identity) or if they affect her disproportionately.



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

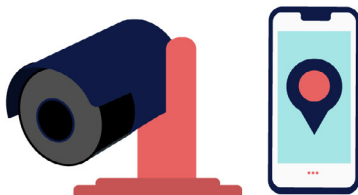
---



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



Actions that damage a person's reputation or credibility



Cyberstalking or cybermolestation.

01

Creation, dissemination, distribution, or exchange, online and without consent, of photographs, videos, or audio clips of a sexual or intimate nature.

02



03

Identity theft and impersonation.

04

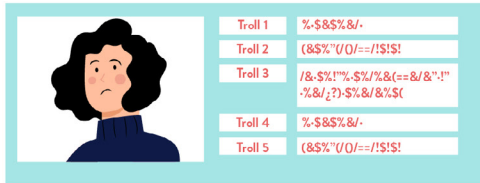


05

Actions involving the surveillance and monitoring of a person.

06





Cyberbullying.



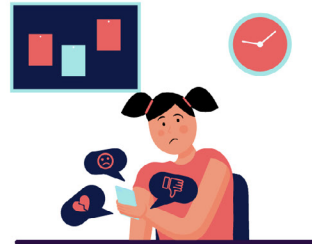
Technology-facilitated physical violence.



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

07

Cyber harassment.



08

09

Direct threats of harm or violence.



10

11

Technology-facilitated abuse, exploitation, and/or trafficking of women and girls.



12



## *Creation, dissemination, distribution, or exchange, online and without consent, of photographs, videos, or audio clips of a sexual or intimate nature*

Women are the main victims of this form of digital violence, which affects them disproportionately across the world. Several studies have found that women account for 90% of all people affected by the non-consensual digital distribution of intimate images (UNSRVW, 2018; *Cyber Civil Rights Initiative*).



This consists of the **non-consensual** creation, exchange, or dissemination online of intimate or sexually explicit images, videos, or other materials, obtained with or without consent, with the purpose of shaming, stigmatizing, or harming the victim (UNSRVW, 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 the victim to a current or former partner (perhaps by sexting); as part of cyberstalking or Cyber harassment campaigns by friends, acquaintances, or strangers; or the materials can be obtained by hacking or physical accessing devices<sup>7</sup>.

It also includes the following acts:

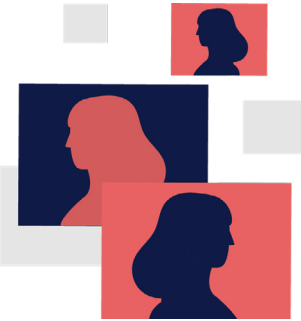
- 01 Recording and distributing images of sexual abuse.
- 02 Taking, without consent, photos or videos of intimate parts of women's bodies in public spaces and sharing them online (e.g., upskirting or downblousing photos and creepshots).
- 03 **Creating sexualized edited images or deepfake videos,** in which images or videos of women may be taken from online sites or social media accounts and superimposed onto other people's bodies to simulate sex scenes or pornographic content with the aim of damaging the victim's reputation.

<sup>7</sup> Hacking is the use of techniques and procedures by a hacker to gain unauthorized entry into another's computer system in order to manipulate it, to obtain information, or simply 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 victim's privacy or the confidentiality of the information stored therein, or to damage the data or hardware.



## What is a deepfake video?

Software that uses machine learning techniques to swap one person's face with another's has been available since 2017 (Knight, 2019). These programs are being used to create fake pornographic videos that are then posted online (Farokhmanesh, 2018). In particular, such videos have been used to attack women involved in political life; their use is expected to spread, however, as the technology has become more accessible to non-expert users (Deeprtrace, 2019). In addition, since deepfake videos use machine learning techniques, it may eventually be difficult to distinguish between a fake video and a real one without the help of forensic tools (Maras and Alexandrou, 2018).



The production of intimate photographs or videos without consent **may be accompanied by extortion or threats to distribute them**, it may take place without the victims' knowledge in closed social networking groups in which several men share naked images of women without their consent for the members' sexual gratification, or it may be part of money-making schemes in which the perpetrators compile and sell links to files or "packs" of sexual images of women obtained in various ways without their consent (the term "packs" is also common in some Spanish-speaking countries, including Mexico and Chile)<sup>8</sup>.

Another very common practice is **to leak personal data about the women appearing in those images or videos**, many of whom are then forced to leave school, work, home, or their community to avoid constant humiliation (Henry, Powell, and Flynn, 2017).



### Remember...

This form of online violence has been commonly referred to as "revenge porn." This is not, however, a correct term, and its use is problematic since it does not reflect the diversity of motivations found among perpetrators, which extend beyond revenge and range from a reassertion of their masculinity to economic extortion and sexual gratification. The term also minimizes the harm done to victims, obscures the non-consensual component of the conduct, and emphasizes the images rather than the perpetrators' abusive acts (Powell, Henry, and Flynn, 2018).



## What is sexting?

Sexting is a practice that involves the creation and exchange of sexually explicit material (UNODC, 2019; Interagency Working Group, 2016). It covers the consensual creation and transmission of images and the consensual creation of images that are then distributed without consent (Salter, Crofts, and Lee, 2013, p. 302). Studies have found that it is a common practice among young men and women, who use 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, Sancí, and Temple, 2013).

<sup>8</sup> 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>



## Close-up:

### Some important issues related to sexting and the non-consensual distribution of intimate images and videos:

01

Although consent can be given to exchange intimate photos with someone or to record sexual acts (even in the presence of others), **that consent does not imply permission to store, publish, reproduce, or disseminate the content.** Consenting to a photo or a recording does not mean that consent has been given for other stages in the process. Any who does so is violating the privacy of the person who participated in the sexting. This is a serious form of gender-based violence, a violation of human rights, an illegal act, and is already criminalized in many countries.

**The practice of sexting should not be stigmatized.** Women and men alike have the right to use technology to express their sexuality. However, it is very important to keep in mind that there are risks in doing so and it is therefore necessary **to consider digital security.**

02

03

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

The website [Acoso.online](https://acoso.online)<sup>9</sup> offers information about this form of digital violence, as well as tips for reporting a case to internet platforms and details about the different laws in Latin American countries on which a complaint can be grounded. The [Without my Consent](https://withoutmyconsent.org) organization's website also has a variety of resources to support survivors of this form of violence. In addition, some additional tips and advice can be found on page 33 of this handbook.

**Note that the provision of these resources does not constitute an endorsement by the OAS or its member states of the content or the organizations named therein. The resources are presented as examples of the organizations, guides, tools, etc., that are available in the region so that readers can explore further information related to this publication's subject matter.**

<sup>9</sup> 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/>



## *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 lives (AI, 2017).

This type of violence manifests itself in the form of **attacks on a person’s online accounts or devices** (mobile phones, computers, tablets, etc.) to obtain, manipulate, and/or publish unauthorized information by stealing passwords, installing spyware, stealing equipment, or deploying keyloggers<sup>10</sup> (APC, 2017). It can also involve unauthorized access to and full control over a person’s accounts or devices.

### **Doxing:**

The term is an abbreviation of the phrase “dropping docs” and entails **the unauthorized extraction and publication of personal information** — such as full name, address, telephone numbers, email addresses, names of spouses, family, and children, financial or employment details — as a form of intimidation or with the intention of locating the person in “the real world” in order to harass them (APC, 2017; Women’s Media Center, 2019). In other incidents, personal information has been posted on pornographic sites along with false advertisements that the victim is offering sexual services.



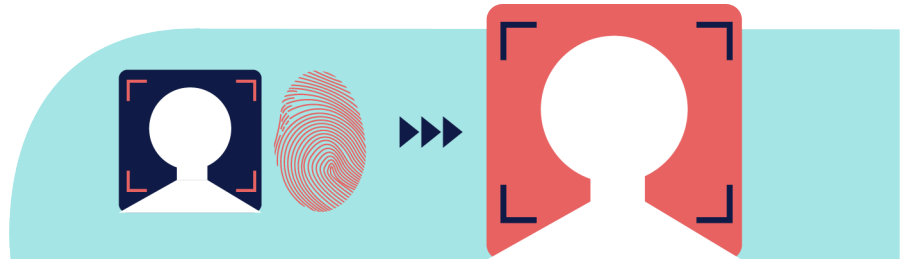
<sup>10</sup> A keylogger is a malicious program installed between the keyboard and the operating system to intercept and record, without the user’s knowledge, information about every keystroke on the device.



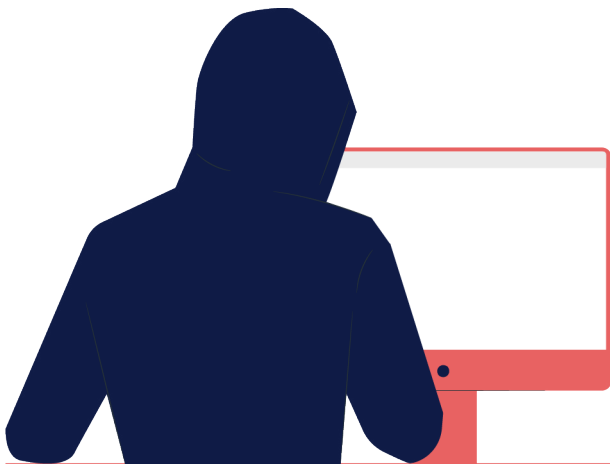


## Identity theft and impersonation

Research conducted by the Australian National University has revealed that women are 50% more likely than men to be victims of identity theft<sup>11</sup>.



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



### The case of the cyber attacker of a whole family

In one prominent case in Chile, a foreign assailant cyberstalked an entire family and their circle of friends (at least 50 people) for 13 years, stealing personal information and impersonating them—including stealing passwords, emails, social network profiles, and personal photos—to send obscene messages and make large-scale postings on pornographic websites. The attacker, suspected to be the former romantic partner of one of the family members, engaged in numerous acts of cyberviolence against anyone associated with or in contact with the original victim and her family (Paz Peña, 2017).

It is common in domestic violence cases for different mechanisms to be used to impersonate victims and steal their identities, to use their personal data in order to make illicit use of their credit cards or control their assets, to monitor their communications with other people, or to impersonate family members or friends on social networks in order to monitor them through these profiles.

<sup>11</sup> 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](https://accan.org.au/files/Grants/ANU%20ID%20theft/ANU%20ID%20theft%20infographic_Gender.pdf)



## *Actions 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*<sup>12</sup>, 15% of the victims interviewed indicated having been affected by the dissemination of false, manipulated or out of context information.

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

### **Camila Zuluaga Case**

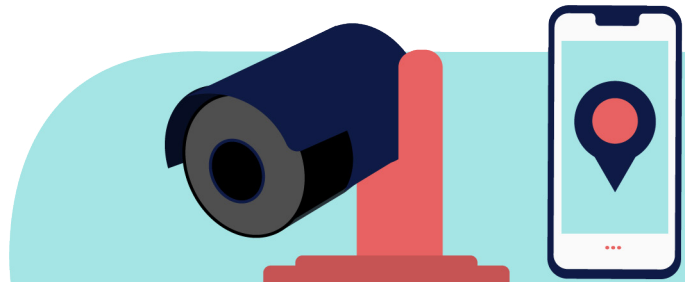
Civil society organizations throughout the region have documented an increase in online acts intended to damage the reputation and credibility of women journalists, politicians, and human rights defenders (Peña, 2017; Luchadoras, 2017; Cuellar and Chaher, 2020). In one case in Colombia, the journalist Camila Zuluaga suffered a coordinated mass attack in September 2019 after the Los Irreverentes website published, absent any proof, the claim that she had received 35 million pesos from a person implicated in a corruption scandal. The attacks were concentrated around the hashtags #CamilaEstásPillada and #CamilitaEstásPillada (“Camila, you’ve been caught”), which reached up to 10,000 mentions in one day. Investigations into the matter found evidence of automation in these coordinated attacks and the operation of a WhatsApp group in which instructions were given to carry out the attacks in order to discredit her journalistic work (Cuellar and Chaher, 2020).

<sup>12</sup> 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](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/tecnorestencias/wp-content/uploads/2019/01/violencia\\_genero\\_linea\\_peru\\_2018.pdf](https://hiperderecho.org/tecnorestencias/wp-content/uploads/2019/01/violencia_genero_linea_peru_2018.pdf)



## *Surveillance and monitoring of a person*

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



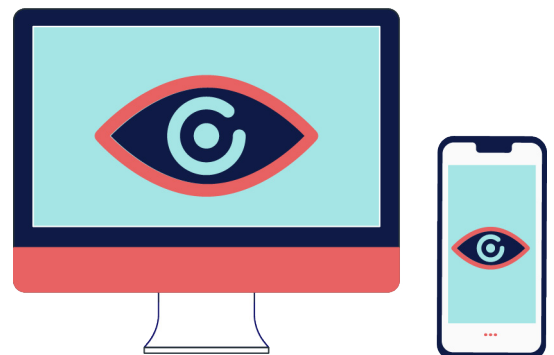
Constant monitoring and surveillance of a **person's online and offline activities** or location constitutes a form of violence (APC, 2017).

- This can be done with spyware installed on the victim's cell phone to monitor her clandestinely or steal her information.
- Geolocation devices placed in cars or handbags, toys, surveillance cameras, virtual assistants, or connected smart devices can also be used.



### *What is spyware?*

Spyware is a type of malicious software installed on a person's devices to record everything they do, including text messages, emails, photos, or even every keystroke. With certain types of spyware, attackers can remotely turn on a cellphone's camera or microphone, track the victim's location, monitor application usage, or intercept calls.





## Cyberstalking or cybermolestation



Studies of the subject have shown that the crimes of cyberstalking and cybermolestation have a pronounced gender dimension and that women and girls are more likely to be victims of these forms of violence (Reyns, Henson, and Fisher, 2011).

To date, there is no single definition of cyberstalking, as it encompasses a wide range of abusive digital behaviors. It can be broadly defined as **intentional and repeated actions** conducted via computers, mobile phones, and other electronic devices which, in isolation, may or may not constitute harmless acts, but which, when taken together, make up 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). These actions can also be directed against victims' family members, friends, or romantic partners.

Unlike cyberstalking, cybermolestation involves a pattern and the commission of **more than one act over a period of time using ICTs**, with the repeated aim of harassing, stalking, annoying, attacking, humiliating, threatening, frightening, offending, or verbally abusing a person (UNODC, 2015). It may consist of emails, calls, text messages, online chats, or the constant sending of obscene, vulgar, defamatory, or threatening comments over the internet. Some of the behaviors it can entail are:



Spying on, obsessing about, or collecting online information about someone and engaging in communication with that person without their consent; constantly sending friend requests on social networks; joining all the online groups to which the victim belongs; following up on the victim's social media posts through shared acquaintances, colleagues, friends, or family; or constantly viewing her profile in a way that she is aware of it (UNODC, 2019).



Repeatedly calling or sending emails, texts, 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 (photos of the offenders' male genitalia), or constantly monitoring and tracking a person's location or daily activities and communications (Henry and Powell, 2016).



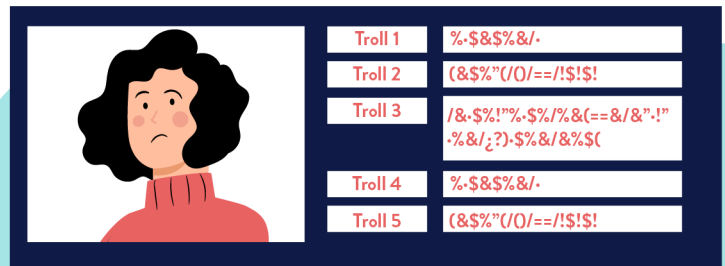
Constantly posting false, malicious, or offensive information about a person on their pages, blogs, or social networks.

Perpetrators of cyberstalking can be intimate or sexual partners, former partners, acquaintances, friends, family members, or strangers. It should also be noted that **this tactic is particularly prevalent in contexts of domestic or intimate partner violence.**



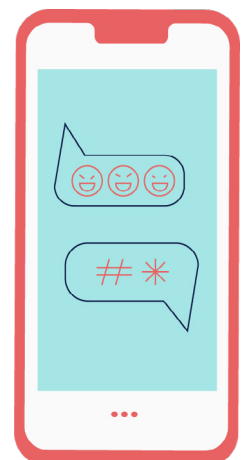
## Cyber harassment

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



Cyber harassment involves the **intentional use of ICTs to humiliate, harass, attack, threaten, alarm, offend, or insult a person** (Maras, 2016). Unlike cyberstalking, in which there is a pattern of threatening behavior, a single incident is sufficient to constitute Cyber harassment, although the practice may also involve more than one (UNODC, 2019).

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





## What is hate speech?

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

Cyberharassment can also include revealing personal information about the victim (doxxing) with invitations to rape her, which has led to situations of revictimization in which the harassers and attackers visit the victim's home.



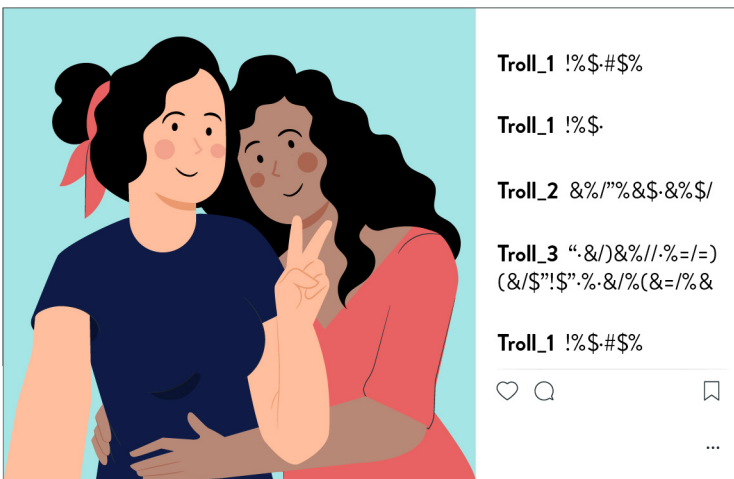
**Cyber harassment, which disproportionately affects women across the world, has sexual connotations** (Li, 2006; Henry and Powell, 2017, p. 212). It can involve threats of rape, femicide, sexualized physical violence, or incitement to physical and sexual violence directed against the victim or her family members, and sexist or offensive verbal attacks relating to women's gender status or physical appearance. It includes sending unwanted sexually explicit materials, content that dehumanizes women and presents them as sex objects, or misogynistic, sexually explicit, and abusive comments (Jane, 2016).



## Did you know that?

Studies show 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": sending obscene photos to a woman without her consent (e.g., pictures of the stalker's genitals) in order to annoy, intimidate, or embarrass her.

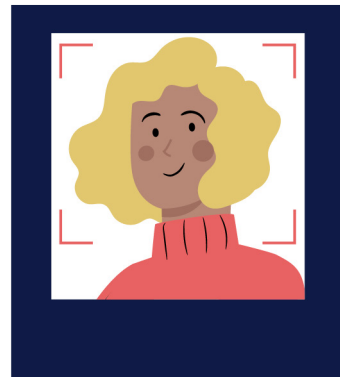


Some perpetrators of Cyber harassment are trolls: posters of extremely offensive and vitriolic comments intended to provoke an emotional reaction and response from other internet users. Such behavior is called trolling (Maras, 2016).

**Gender trolling is the posting of messages, images, or videos, and the creation of hashtags, for the purpose of harassing women and girls or inciting violence against them (UNSRVW, 2018; Mantilla, 2013).**

**Cyber harassment can also be a group undertaking**, when two or more people organize and coordinate to repeatedly harass a person online, often in a sustained manner over time and with a 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 encountered (Jane, 2017).

Attacks by groups coordinated through networks of trolls and hackers, such as the “Legión Holk” (originating in Colombia and Peru) or the “Secta 100tifika”, are proliferating in Latin America; they carry out mass attacks and harassment with the aim of fueling confrontation and controversy, generating trends, and promoting discrimination, racism, and misogyny. These groups often target women who are active on social media, who have a public profile, or who are feminists. The dissemination of sexualized photomontages, the impersonation of their identity on social networks for defamatory purposes, and the distribution of degrading content are common (Peña, 2017; Barrera, 2017).



Some of these attacks have grown to disproportionate dimensions: “cybermobs” are formed by organized online groups that mass post offensive or destructive content with the intention of embarrassing someone or having them remove their social media profile (Citron, 2014).

### Ana Gabriela Guevara Case

An emblematic case of coordinated attacks in Mexico was that of former athlete and senator Ana Gabriela Guevara: in December 2016, after having made public on social networks the physical aggressions she suffered in public, she was attacked by organized groups of trolls and hackers with fake accounts that caused hashtags with references to gender violence to go viral. The hashtags used included #MujerGolpeadaEsMujerFeliz (“a beaten woman is a happy woman”) or #GolpearMujerEsFelicidad (“beating women is happiness”), which became trending topics in several Spanish-speaking countries (Peña Ochoa, 2017; Barrera, 2017).



## Ciberbullying



According to a worldwide investigation carried out by IPSOS<sup>13</sup> 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 or cyberintimidation is the use of technology by minors to humiliate, annoy, alarm, insult, or attack another minor, to spread false information or rumors about them, or to threaten, isolate, exclude, or marginalize their victims (Maras, 2016; Hinduja and Patchin, 2014; UNODC, 2015).

This can be done through text messages, emails, virtual surveys, blogs, social media posts, online video games, or virtual reality sites, and it can cause very serious damage to the emotional and physical health of its targets, who may even self-harm or commit suicide.

In most countries, **both the perpetrators and victims of cyberbullying must be minor-aged children** (Duggan et al., 2015). In others, such as Australia and New Zealand, cyberbullying can involve adults.



### Did you know...?

Opinions differ on whether gender is a determining factor in cyberbullying (Navarro and Jasinski, 2013; Smith, 2012; Fanti, Demetriou, and Hawa, 2012; Livingstone et al., 2011; Calvete et al., 2010). That notwithstanding, what is clear is that the harm and repercussions suffered by girls and boys are different depending on the gender stereotypes with which they live: it is common for girls who are victims of cyberbullying to be attacked with offensive and violent comments about their bodies or their sexuality.

<sup>13</sup> 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](https://www.ipsos.com/sites/default/files/ct/news/documents/2018-06/cyberbullying_june2018.pdf)





## 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*<sup>14</sup>, 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.



If you tell anyone, I'll upload your photos.

This type of violence consists of using technologies to send or post communications or content (verbal or written messages, photos, or videos) that express the **intent to commit physical harm or sexual violence** (APC, 2017; Barrera, 2017).

It includes digital extortion, which occurs when one person puts pressure on another to force them to act in a certain way through threats, intimidation, or aggression, to bend their will, or to control them emotionally. It can 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?



Sextorsion consists of threatening a person with publishing intimate images or videos in order to obtain more sexually explicit material, have sex, or extort money (UNSRVW, 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).

Violence of this kind, which has grown exponentially in recent years, 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 sextorsion for their own sexual gratification. A 2018 report by the FBI's Internet Crime Complaint Center noted that there had been a 242% increase in emails threatening extortion, most of which involved sextorsion (FBI-ICC, 2018).

<sup>14</sup> 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](https://amnistia.org.ar/corazonesverdes/files/2019/11/corazones_verdes_violencia_online.pdf)

### #GamerGate Case

In 2014, #GamerGate<sup>15</sup> — one of the first mass online attack campaigns — targeted several women in the video game industry, including developers Zoe Quinn and Brianna Wu and media figure 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, and organized on online platforms such as 4Chan, Twitter, and Reddit to coordinate large-scale attacks that included acts of cyberharassment, doxxing, and rape and death threats. The three women reported doxxing attacks with threats that escalated to such an extent that they had to flee their homes. In particular, the attacks on Anita Sarkeesian reached highly aggressive proportions that included bomb threats when she was nominated to receive an award in San Francisco and terrorist threats when it was announced that she was to participate at a conference at Utah State University.



## Technology-facilitated physical violence



In the UNESCO and ICFJ research entitled *Online Violence: The New Line of Battle for Women Journalists - # JournalistsToo*<sup>16</sup> 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 take various forms, such as sexual attacks that are organized or planned through ICTs, or sexual violence based on the online publication of the victim's personal data after she has been located (doxxing).

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

<sup>15</sup> Eliana Dockterman (2014). "What is #GamerGate and why are women being threatened about video games?" *Time*. Available at: <https://time.com/3510381/gamergate-faq/>

<sup>16</sup> 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](https://unesdoc.unesco.org/ark:/48223/pf0000375136_spa)



## *Technology-facilitated abuse, exploitation, and/or trafficking of women and girls*

Surveys indicate that new technologies are facilitating global human trafficking (80% of the victims of which are women, and 95% are sexually exploited) 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 exercise power over a person through the sexual exploitation of their image or body against their will (Barrera, 2017). The following are some of the behaviors included in this form of violence:

- the use of technology to target and recruit women and girls for sexual abuse or trafficking, to coerce them into accepting trafficking and situations of sexual abuse, to exert power and control over them, or to prevent them from freeing themselves from abuse, including by threatening to disclose private information (UNSRVW, 2018, para. 32).
- Grooming: i.e., deliberate acts by an adult to approach a minor (possibly cultivating a romantic connection) with the aim of establishing a relationship and emotional control that allows the adult to commit sexual abuse, engage in virtual relationships, obtain child pornography, or traffic the minor (Women's Media Center, 2019).
- The publication of sexual images without a person's consent for the purposes of commercialization and prostitution.



## *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).

Intentional acts carried out to censor and harm women's organizations, including attacks on their channels of expression (Barrera, 2018); for example: accessing them without consent; hacking websites, social networks, or email accounts to affect their work; getting the organization's profile or social networks taken down by using community standards to denounce content that the platform considers sensitive; denial of service (DDoS) attacks<sup>17</sup>; domain usage restrictions or domain theft; and internet blackouts during meetings or protests (APC, 2017).

This form of violence includes surveillance and monitoring of the activities of community or group members, direct threats against them, Cyber harassment through sexually explicit content, the 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 and women's human rights defenders, intended to block access to their content or to take it offline either temporarily or permanently. Notable cases include those of the Mexican feminist collective Las Hijas de la Violencia and the Colombian feminist organization Mujeres Insumisas, and the constant coordinated attacks against black feminist and transfeminist activists and groups in Brazil (Lyons et al., 2016; Peña, 2017).

<sup>17</sup> An online attack that entails mobilizing people to send a large number of requests to a website's server in order to overload it and render it inaccessible.

# Part three

*Self-Protection and Response Handbook:*

## **DIGITAL SECURITY TOOLS AND RESPONSIVE STRATEGIES FOR ONLINE GENDER VIOLENCE**





## *Basic digital security recommendations: preventive measures*



**Taking steps to strengthen digital security is the first line of defense against online threats, attacks, and violence.** Obviously, not all women have the same priorities or are threatened in the same way, and appropriate measures may vary from case to case. It is important to remember that cybersecurity is a personal process that can be self-paced and that can be attained with a little patience and proper planning.

The following sections offer some basic tips for safe surfing and controlling digital interactions, along with additional resources for learning more about the topic. This wealth of information may be overwhelming at first sight. However, **this handbook seeks to demystify the process of strengthening women's cybersecurity.** Remember that you can take these recommendations one step at a time and, along the way, you are certain to discover that bolstering your digital security is much simpler than it seems.

Please note that the provision of the following resources does not represent an endorsement of their content or the organizations named by the OAS or its member states. The resources are offered as examples of the organizations, guides, tools, etc. that are available in the region so that readers can learn more about the topics covered in this publication.

### 01 Use strong passwords to protect against hacking or identity theft

Strong, secure passwords are crucial to protecting online information, as they are the gateway to our accounts and, through them, to details about our personal lives.





We commonly choose personally significant or easily remembered passwords (e.g., 12345) but this puts us at risk, as someone we know or a hacker could easily guess them. For effective protection, **unique passwords should be used: do not use the same or very similar passwords** on different pages and accounts (e.g., by simply adding a 1 or recycling them) and, if possible, use a different username for each account (e.g., one password and username for email, another for your bank account, another for social networks, etc.).



**Change your passwords constantly** (preferably every 90 days), particularly for more sensitive accounts. Above all, change them if you receive a legitimate, verified email (first make sure it is not a phishing attempt) informing you that your account has been compromised.



**Create complex passwords.** To provide effective protection, passwords need to be long, unique, random, and difficult to predict; they should include a combination of at least 12 upper and lower case letters, numbers, and symbols. The Surveillance Self-Defense website hosts a: [guide on creating strong passwords](#)<sup>17</sup>.



Activate **two-factor authentication**<sup>18</sup> on your email and social network accounts. This option asks the user to identify herself with a combination of two authentication methods: i.e., it asks for the password and a unique code sent by SMS or generated by an app, which must be entered to log in to the account from a new or unregistered computer, phone, or browser. More information on [two-factor authentication](#) is available on the Electronic Frontier Foundation<sup>19</sup> website as well as directly from [Facebook](#)<sup>20</sup>, [Instagram](#)<sup>21</sup>, [Twitter](#)<sup>22</sup>, [Gmail](#)<sup>23</sup> and [Apple](#)<sup>24</sup>.



To make things easier, you can use an **automatic password generator or online password manager**, which create random, secure passwords for each of your accounts. If you choose this option, all you have to remember is the master password to unlock the other passwords. Examples of password managers include [1Password](#), [LastPass](#), [Password Generator](#) and [KeePassXC](#)<sup>25</sup>. For further information, a [video](#) can be consulted at the website of *Surveillance Self-Defense*<sup>26</sup>.

<sup>17</sup> Surveillance Self-Defense. *Creating Strong Passwords*. Available at: <https://ssd.eff.org/es/node/23/>

<sup>18</sup> Available at: <https://twofactorauth.org/>; <https://ssd.eff.org/es/module/c%C3%B3mo-habilitar-la-autenticaci%C3%B3n-de-dos-factores>

<sup>19</sup> Electronic Frontier Foundation. *The 12 Days of 2FA: How to Enable Two-Factor Authentication for Your Online Accounts*. Available at: <https://www.eff.org/deeplinks/2016/12/12-days-2fa-how-enable-two-factor-authentication-your-online-accounts>

<sup>20</sup> Facebook. *What's two-step authentication and how does it work on Facebook?* Available at: <https://www.facebook.com/help/148233965247823>

<sup>21</sup> Instagram. *Keeping Instagram Safe*. Available at: <https://help.instagram.com/1372599552763476>




<sup>22</sup> Twitter. *How to use two-factor authentication*. Available at: <https://help.twitter.com/es/managing-your-account/two-factor-authentication>

<sup>23</sup> Google. *Two-factor authentication*. Available at <https://www.google.com/intl/es-419/landing/2step/>

<sup>24</sup> Apple. *Two-factor authentication for Apple ID*. Available at: <https://support.apple.com/es-es/HT204915>

<sup>25</sup> Available at: <https://1password.com/>; <https://www.lastpass.com/es/>; <https://passwordsgenerator.net/>; and <https://keepassxc.org/>

<sup>26</sup> Surveillance Self-Defense. *Animated Overview: Using Password Managers to Stay Safe Online*. Available at: <https://ssd.eff.org/es/node/85/>

-  **Use the security questions** on sites that offer this option, but do not answer them with real information (for example, the name of a pet or the street name of your home address). The answers should be difficult to guess and not contain data that can be found on the internet or social networks (grandmother's surname, for example). The answers can also be saved in a password manager.
-  **Never share passwords over an unsecured connection**, such as text messages or SMS.
-  **Do not save passwords in your browser settings, in the cloud<sup>27</sup>**, or in an insecure document on your computer or phone, as they are easy to find if your device is hacked. They can be stored in an encrypted document on a secure physical device or written down and stored in a place where they can be easily erased. More information about file encryption [Windows](#) on Microsoft's website or the website of [Apple](#) for the iOS operating system<sup>28</sup>.

To learn more about password strength, see also the publication [Media Literacy and Digital Security](#) from the OAS and Twitter<sup>29</sup>.

## 02 Using different email addresses

One useful security measure is **to have different email addresses for each of your accounts** for different purposes on the internet: for example, one for personal communications, one for work, one for your public profile, one for social networks, one for online gaming, and one for receiving promotional materials. This prevents someone who gains access to one account from automatically gaining access to the others.



<sup>27</sup> The cloud is a data storage system, such as Google Drive, Dropbox, or iCloud, which is not in personal devices.

<sup>28</sup> Microsoft. *How to encrypt a file*. Available at: <https://support.microsoft.com/es-es/windows/c%C3%B3mo-cifrar-un-archivo-1131805c-47b8-2e3e-a705-807e13c10da7>; and Apple. *iCloud security overview*. Available at: <https://support.apple.com/es-es/HT202303>

<sup>29</sup> Organization of American States (OAS) and Twitter (2019). *Media Literacy and Digital Security: Best Twitter Practices*. Available at: <https://www.oas.org/es/sms/cicte/docs/alfabetizacion-y-seguridad-digital.pdf>

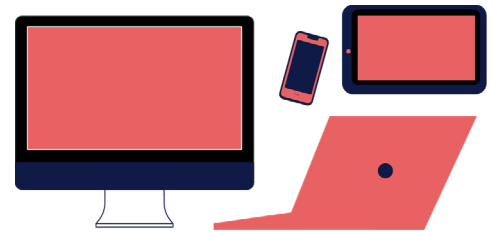




**Remember: Basic precautions when navigating**  
**Caution is the best defense online.**



- Always delete emails, posts, or messages that look suspicious.
- Connect through reliable Wi-Fi networks only. If you do connect via a public network, limit the information that is sent or consulted.
- Use a virtual private network (VPN)<sup>30</sup>: a network technology that protects against cyberattacks when connecting to the internet through a public Wi-Fi network by making it difficult for third parties to steal confidential information. [Free or paid VPN](#), and, as explained in this [video](#) it is a relatively simple process.
- Always browse in secure mode: check that the website name starts with [https://](#) (and not [http://](#)), which means that the information is encrypted in transit.
- When using other people's devices, always browse in private or incognito mode to keep your passwords from being recorded.
- Download apps from official sites only, to make sure they are safe.

**03 Protect electronic devices (desktop computer, laptop, mobile phone, or tablet)**



**What is malware?**

Malware is malicious software that executes unsolicited actions on devices to infiltrate and damage a computer or information system.

- 
**Don't forget to update your devices' software.** Updating your software regularly not only helps make your device faster; it also provides greater security, as updates can protect against threats and resolve vulnerabilities in previous versions.
- 
**Use an antivirus program.** Although antivirus apps cannot detect all malicious programs, they do provide your devices with an additional layer of protection. There is a wide variety of antivirus software on the market, and you can choose the one that best suits your needs. The Reason Security site offers some [recommendations](#) for choosing a computer antivirus<sup>31</sup>.

<sup>30</sup> Avast Blog. *Por qué y cómo configurar una VPN en un iPhone o un Android.* Available at: <https://blog.avast.com/es/por-que-y-como-configurar-una-vpn-en-un-iphone-o-un-android>; We Live Security. *¿Qué es una VPN y cómo funciona para la privacidad de la información?* Available at: <https://www.welivesecurity.com/la-es/2012/09/10/vpn-funcionamiento-privacidad-informacion/>

<sup>31</sup> Reason security. *Which antivirus is best for laptops?* Available at: <https://blog.reasonsecurity.com/2020/01/12/which-antivirus-is-best-for-laptops/>

**Verify apps.** To bolster the security of your devices, you should check which applications are installed on your mobile phone (they can be seen in the settings menu). If you find an unused or unknown app, search the internet to find out what it is for. If it is not recognized or does not belong to the phone's operating system, it should be uninstalled for safety's sake. The following links show how to delete applications on [Android](#) and [Apple](#)<sup>32</sup>.

**Protection against malware.** Some attackers may try to access a device to extract information or spy on it through phishing attacks: that is, by installing programs concealed in email attachments or as messages that appear innocent but that actually contain malicious software. Such programs can turn on your device's microphone or camera, relay conversations, see what you type, copy files or messages, monitor your movements, or steal passwords. The best strategy to prevent this is to **always be suspicious about strange emails**, check who is sending the file, and **never open files attached to suspicious emails**. Do not click on untrusted links or download any such files.

**Protect mobile phones.** Cellphones are open windows into our lives. They hold and interconnect much of our personal information and our social interactions. In addition, they are normally synchronized with other devices. For that reason, some basic steps should be taken to protect these tools that are closely tied in with our online and offline lives:

- Place a **password lock** on the phone so that it cannot be used without entering a code (preferably a combination of words and numbers) in the event of theft or loss.



### What is phishing?

Phishing is a technique used to fraudulently obtain confidential information (passwords, bank details, etc.) through a misleading electronic communication (email, text message, etc.). In general, such messages impersonate a person or company so that the recipient provides private data. These messages can also infect your devices with spyware to monitor or steal information.

- **Avoid storing sensitive information on your phone** and, when necessary, use the feature that allows data to be encrypted or scrambled. The following links provide instructions for encrypting data on n [Apple devices](#) and [Android devices](#)<sup>33</sup>. You can also block access to applications to protect your information and interactions with apps such as [Smart App Lock](#)<sup>34</sup>.

<sup>32</sup> Google support. Help Center. Delete or disable apps on Android. Available at: <https://support.google.com/googleplay/answer/2521768?hl=es>; Apple support. Delete apps on your iPhone, iPad, and iPod touch. Available at: <https://support.apple.com/es-es/HT207618>

<sup>33</sup> Microsoft. Encrypting your Android device. Available at: <https://docs.microsoft.com/es-es/mem/intune/user-help/encrypt-your-device-android>; Apple Support. About encrypted backups on your iPhone, iPad, or iPod touch. Available at: <https://support.apple.com/es-mx/HT205220>

<sup>34</sup> Smart AppLock (App Protect). Available at: <https://play.google.com/store/apps/details?id=com.thinkyeah.smartlockfree&hl=en>

- If you need to delete sensitive information, it is important to remember that deleting it from your cell phone is not enough: in many cases that information may have been automatically uploaded to the cloud, so it is also necessary to delete it there. Android does not automatically upload information to the cloud, but Apple devices do, so you have to disable this option manually. A guide to [disabling automatic synchronization with iCloud](#) can be found in this Apple help center<sup>35</sup>.
- **Check which applications are installed on your cellphone.** If an app is unfamiliar or seems suspicious, search the internet for information about it and, if it is not necessary, uninstall it. Additionally, unused applications should be uninstalled, because they can be a source of vulnerability. Having only what you need installed increases your digital protection.
- Every step you take on the internet is recorded, and over time the browser used on your phone or computer becomes a big book of your life. To boost your privacy and protect your digital identity, **you should delete your browser history.**



### Did you know that?

The average person taps or swipes their phone more than 2,600 times a day.

- Your location reveals a great deal about your activities and habits, and applications installed on your phone can constantly record your movements without you even realizing it and provide attackers with information. **Check and disable the location permissions** so that apps do not locate you unnecessarily.



### What are photo or image metadata?

They are information fields embedded in all digital photographs that are stored on a device. Among other things, they show details about geolocation and the day and time they were taken.

Before posting or sending your photos, be aware that this information will be embedded in them. If necessary, remove metadata to avoid compromising sensitive information.



**Camera security. Cover your mobile phone's or computer's webcam** when not in use (with a Post-it note or special cover), which will prevent anyone recording or taking pictures if they obtain remote access to your device.

<sup>35</sup> Apple Support. Change your iCloud settings. Available at: <https://support.apple.com/es-es/HT207689>



### Remember: protection against doxxing

Your information is spread all across the web. Details such as your full name, address, telephone number, email address, the names of family and friends, and social security numbers can be found on various websites, and can be collected by stalkers seeking to doxx you.


You can check with data brokers what information about you is on the internet and ask them to delete it. Some of these data brokers are: [White Pages](#), [Instant Check Mate](#), [Acxiom](#) or [Spokeo](#)<sup>36</sup>. Other services such as [DeleteMe](#) or [Privacy Duck](#) can monitor sites to ensure that your information remains deleted.

You can also do a reverse Google search for your information by entering your address, email, or phone number, or a [reverse image search](#) with [Google Images](#) or on sites such as [TinEye](#) and [Bing](#)<sup>37</sup>.









## 04 Security on social networks

**Social networks have become an essential way to navigate and express ourselves in the new online-offline reality** and they allow us to keep in touch with family, friends, work, interests, hobbies, etc. However, we must not forget that they can be a channel for cyberattacks and acts of cyberviolence. They can offer strangers a gateway into our lives, and so it is vital to make sure you only share personal information with those you choose to.

 The first step is to ask yourself, **what information do I want to keep private?** The information and photos we post online leave an indelible trace. That is why you must ask yourself what you want to make publicly available and assess the risks and benefits of making that information public. Be aware that a stalker could take advantage of data such as your location, city or date of birth, or photos posted on public profiles.

<sup>36</sup> *White Pages*. Available at: <https://www.whitepages.com/suppression-requests>; *Instant Checkmate*. Available at: <https://www.instantcheckmate.com/opt-out/>; *Acxiom*. Available at: <https://isapps.acxiom.com/optout/optout.aspx#section8>; *Spokeo*. Available at: <https://www.spokeo.com/optout/>; *Delete Me*. Available at: <https://joindeleteme.com/>; *Privacy Duck*. Available at: <https://www.privacyduck.com/>

<sup>37</sup> *Digital Inspiration. Reverse Image Search*. Available at: <https://www.labnol.org/reverse/>; *Google*. Google Search Help. Available at: <https://support.google.com/websearch/answer/1325808?co=GENIE.Platform%3DAndroid&hl=es> *TinEye*. Available at: <https://tineye.com/> *Microsoft Bing*. Available at: <https://www.bing.com/?setlang=es>

-  To avoid being easily identified, consider **using a pseudonym** and profile pictures that do not show physical features.
-  **Understand and configure the privacy and security options** of your social networks. It is important to take the time to see what information of yours is exposed on the networks (for example, who can see your profile or posts, what content they can add, or where they can tag you), which can be reviewed and controlled through the privacy settings. Useful guides for exploring privacy settings can be found at the OAS's [Media Literacy and Digital Security](#) (p. 17)<sup>38</sup>, on the Take Back The Tech website<sup>39</sup>, or directly on Facebook, Twitter, [Instagram](#) and [Tik Tok](#)<sup>40</sup>.
-  **Disable geolocation** in apps that don't need your location to function, along with the location tag on social networks like Facebook and Instagram. This is an important precautionary measure because whenever you post something on social networks, the geolocation data is recorded, and that information can be used to find your home address or the places you frequent.
-  If family members or friends are sharing photos of you or social network updates with your information and you think it would be best to keep that information private for security reasons, you can ask them to turn off the geolocation or location tag on their posts.
-  Check **what devices are connected to social networks**. If you find an unknown device, you should disconnect it, as it could mean that your phone has been cloned and that someone else has access to your apps (and data) from another phone or computer.
-  The help and support services of the different social networks ([Facebook](#), [Twitter](#), [Instagram](#) and [Tik Tok](#)) can be consulted directly to resolve specific questions about how they function or problems that may arise during interactions<sup>41</sup>.




<sup>38</sup> Organization of American States (OAS) and Twitter (2021). *Media Literacy and Digital Security: The importance of keeping safe and informed*. Available at: <https://www.oas.org/es/sms/cicte/docs/alfabetizacion-y-seguridad-digital.pdf>

<sup>39</sup> Take Back the Tech. *Social Media Privacy*. Available at: <https://www.takebackthetech.net/es/privacidad-en-las-redes-sociales>

<sup>40</sup> Facebook. *How can I change the privacy setting of Facebook?* Available at: <https://www.facebook.com/help/193677450678703>; Twitter. *Privacy*. Available at: <https://help.twitter.com/es/safety-and-security#ads-and-data-privacy>; Instagram. *Privacy settings and information*. Available at: <https://www.facebook.com/help/instagram/196883487377501>; TikTok. *Account privacy settings*. Available at: <https://support.tiktok.com/es/account-and-privacy/account-privacy-settings>.

<sup>41</sup> Facebook. *Help Service*. Available at: <https://www.facebook.com/help>; Twitter. *Help Center*. Available at: <https://help.twitter.com/es>; Instagram. *Help Center*. Available at: <https://help.instagram.com/>; TikTok. *Help Center*. Available at: <https://support.tiktok.com/en/>

## 05 Online gaming security

-  Do not use information or profile pictures that reveal personal details.
-  For added security, use unique gamertags<sup>42</sup> and different names on each platform. With this, if one game account has been compromised, the others cannot be located so easily.
-  Understand and **change the privacy settings** of online gaming systems to control what information is made public (e.g., who can see your profile or real name, who can see your friends list or send messages, who can see when you are online or your videos).



 **Tip**

More tips for safe online gaming can be found in the guide on the [Feminist Frequency](#)<sup>43</sup>.

## 06 Safe sexting

Technology has opened up new channels for the expression of intimacy and sexuality. However, given the dynamics of violence and gender discrimination that have permeated digital spaces, you must be aware of the risks involved and take control of that technology to protect yourself, understanding that the process is never completely safe. The [Acoso.online](#) platform asks some very useful questions to guide people through three key stages of this process, identified by the letters R, S, and P<sup>44</sup>:




- 1. Recording:** Who is going to record it, and where? On which device? Does that device automatically save a copy to the cloud? Will my face or any physical characteristics that could identify me be shown?
- 2. Storage:** Who is going to store the material and where (in the cloud, on the phone, on the computer)? Who will have access to the recording? For how long? What digital security measures will be taken to ensure that no one else has access to the material?
- 3. Publication:** Are you planning to share or publish the material? Are you sure the material will be erased if you want to delete it later? What options does the internet platform offer to protect the security and privacy of users?


<sup>42</sup> A gamertag is an identifier of persons who play games and share contents in the community of the digital gaming service platform Microsoft Xbox Live. It is created on the basis of an alias, an avatar, or an image and information about the player's preferences.


<sup>43</sup> *Feminist Frequency. Speak Up & Stay Safe(r): A Guide to Protecting Yourself from Online Harassment.* Available at: <https://onlinesafety.feministfrequency.com/en/>


<sup>44</sup> *Acoso.online. Resiste y toma control sobre la tecnología [Resist and take control over technology].* Available at: <https://acoso.online/mx/4-resiste-y-toma-control-sobre-la-tecnologia/>


## Basic recommendations:


 **Do you trust them?** It is vital that you feel safe with the person who will receive the image or video, because they will also be responsible for protecting the privacy of the participants.


 **Consent is key.** Agree on how the photos will be shared and the types of details they can contain.

 Look for safe angles and **try not to show physical features or places that could reveal your identity.**

 **Edit the content** if necessary (e.g., use emojis to cover features that could reveal your identity).

 **Do not forget the image metadata,** which can provide information to identify the person who took the photo. In addition, make sure that recordings are always made on your own device, understand and control your settings, and disable automatic location tags.

 **Choose the right channels.** Do not share intimate images over public Wi-Fi connections. In addition, when using messaging apps such as WhatsApp, there is a risk of your pictures and videos being retransmitted or shared. This is because although they encrypt messages end-to-end, the content is stored on the devices. Snapchat allows you to make temporary posts that are deleted after a while, but the recipient can always take a screenshot of the received image and save it to their device.

 **Periodically delete photos stored** in your device's memory (and in the cloud) so that no one can steal them.



### Tip

For added protection, you can use applications<sup>45</sup> such as [Signal](https://signal.org/es/), which offers the option of deleting messages in conversations; [Confide](https://getconfide.com/), which has encrypted messages that self-destruct (on devices and in servers) once they have been viewed and also blocks screenshot attempts, or [Wickr](https://wickr.com/) which is able to detect if the person who received the image took a screenshot and will notify you.



### Tip

The Ciberpatrulla<sup>46</sup> site contains a [tutorial](#) on reviewing and deleting image metadata on Windows, Mac, iOS, and Android.

Also available are [programs to delete metadata](#), such as Nectar, MediaInfo, Metanull, and Get-Metadata.

<sup>45</sup> *Signal*. Available at: <https://signal.org/es/>; *Confide*. Available at: <https://getconfide.com/>; *Wickr*. Available at: <https://wickr.com/>

<sup>46</sup> Ciberpatrulla. ¿Qué son los Metadatos de fotos e imágenes? Cómo puedes utilizar los datos EXIF en tus investigaciones (y de paso aprender a borrarlos para no dejar huella). [What are metadata of photos and images? How can you use EXIF data in your browsing (and at the same time learn to delete them so as not to leave any traces)?] Available at: <https://ciberpatrulla.com/metadatos-de-fotos/> Tekcrispy. 4 programas para extraer los metadatos de archivos multimedia. [Four programs to extract metadata from multimedia files]. Available at: <https://www.tekcrispy.com/2018/04/22/extraer-metadatos-audiovisuales/>



## Digital safety tips for women victims of domestic or intimate partner violence

It is increasingly common in abusive relationships for the aggressor to try to exert control and perpetrate violence through new technologies; this is particularly true of cellphones, which are the principal means through which we maintain connectivity in our daily online and offline activities. When this happens, the victim may think that her partner or former partner is a hacker or consummately tech-savvy, because he always manages to know where she is, what she is doing, the messages she sends, the things she searches for on the internet, or with whom she communicates. However, several studies have found that **most assailants have a very basic knowledge of technology that they simply know how to leverage to their advantage.**



Of course, not all victims' experiences, threats, and risks are the same. It is important to keep in mind, however, that all women can learn very simple techniques to take care of themselves, strengthen their digital safety, protect their communications, and even use technology to reach out to trusted contacts, ask for help, or document violence.

Here are some tips that could be of use if domestic violence by a current or former partner has spread to your mobile phone. Some of them are based on the recommendations published by the organizations Derechos Digitales and MaríaLab in their *Guide of digital precautions for women victims and survivors of violence during the COVID-19 pandemic*<sup>47</sup>.

Before adopting any of these measures, however, it is very important that you assess your own risks and **do only what is safe or comfortable.** There are no universal formulas for dealing with such situations, and digital security is a personal process that each person develops at his or her own pace and according to his or her own circumstances.







First, to properly consider your options and safety, you should ask yourself: Did my assailant provide the mobile phone or did he have access to it for a period of time? Does he have permanent access to the phone that you can do nothing about?

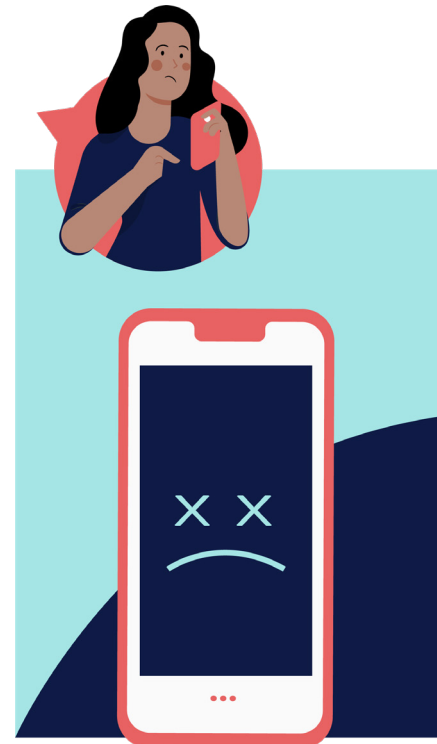
If the answer is yes, it is possible that the attacker has access to the cellphone through spyware; in such cases, it is advisable to disconnect the device from the internet, check its settings, and — if possible — stop using it and find another phone to communicate.



<sup>47</sup>Goldman y Natansohn (2020). *Cuidados durante la pandemia: “¿Cómo denunciar la violencia doméstica?”*[Services during the pandemic. How to report domestic violence?]. Derechos Digitales and MaríaLab. Available at: <https://www.derechosdigitales.org/wp-content/uploads/covid-violencia-domestica.pdf>



-  You can **check your phone for spyware** (through which your photos, chats, location, or calls can be monitored) using applications such as [Root Verifier](#) for Android<sup>48</sup>.
-  In addition, **attackers often use applications that may seem harmless** but that actually reveal the victim's location, such as the lost or stolen device locator apps that many phones have installed (e.g., Find my Phone). If you find this application and do not recognize the login account, it is possibly being used to track your phone; it should therefore be disabled. These links show you how to disable apps on [Android](#) and how to disable [Find my iPhone](#)<sup>49</sup>.
-  You can also [check check if any of the phone's apps has superuser permissions](#) for a superuser<sup>50</sup>, as it may be spyware<sup>51</sup>.
-  Remember that much of your information is stored in the cloud, so **changing the password for the Google or iCloud account on the phone** is a crucial step. Another recommendation is to log on through a device that you know is secure and change the passwords on all your accounts. The Google and Apple websites provide information on how to change your account password on an [Android](#) device and the [ID of Apple](#)<sup>52</sup>.
-  If you still suspect spyware after following the above steps, you can reset your device to the original factory settings, which will disable all its installed programs. Remember that this will also delete your [photos](#), data, and contacts, so it is important to make a backup copy of them first. The following links provide guides to [backing up information](#)<sup>53</sup> and restoring factory settings on [Android](#) and an [iPhone](#)<sup>54</sup>.
-  If you would prefer a much more thorough check, you can disconnect the device from the internet, stop using it immediately, and take it to a digital security expert, who will be able to discover more details about the possible spyware.



Equipping your phone with a secure lock password is of the utmost importance. If that is not feasible because of pressure from your attacker (for example, if it could make him violent), an application can be installed that simulates a bug on the phone in the event that someone tries to use its apps without a password.

<sup>48</sup> Google Play. *Root Verifier*. Available at: [https://play.google.com/store/apps/details?id=com.abcdj.rootverifier&hl=en\\_US](https://play.google.com/store/apps/details?id=com.abcdj.rootverifier&hl=en_US)

<sup>49</sup> Google Play Help. *Delete or disable apps on Android*. Available at: <https://support.google.com/googleplay/answer/2521768?hl=es>; and iPhone News. *How to turn off Find My iPhone*. Available at: <https://www.actualidadiphone.com/desactivar-buscar-mi-iphone/>

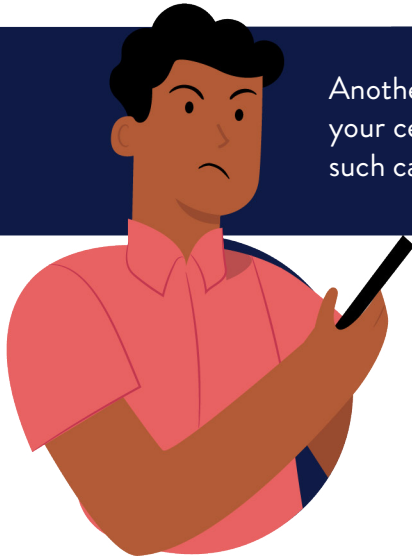
<sup>50</sup> Superuser permits, or the root access in the Android system, make it possible for the user to have high privileges to exceed the constraints imposed by the manufacturer and to make deep changes in the device's operating system, including the possibility of replacing applications of the system or executing specialized software.

<sup>51</sup> Betech. *How to remove permits from an app on Android and iOS*. Available at: [https://as.com/meristation/2020/02/12/betech/1581547469\\_996131.html](https://as.com/meristation/2020/02/12/betech/1581547469_996131.html)

<sup>54</sup> Google Support. *Change or reset your password*. Available at: <https://support.google.com/mail/answer/41078?co=GENIE.Platform%3DAndroid&hl=es>; Apple Support. *Change your Apple ID password*. Available at: <https://support.apple.com/es-es/HT201355>

<sup>53</sup> ESET-LA. *Guía de Backup*. [Backup Guide]. Available at: <https://www.welivesecurity.com/wp-content/uploads/2017/03/guia-backup.pdf>

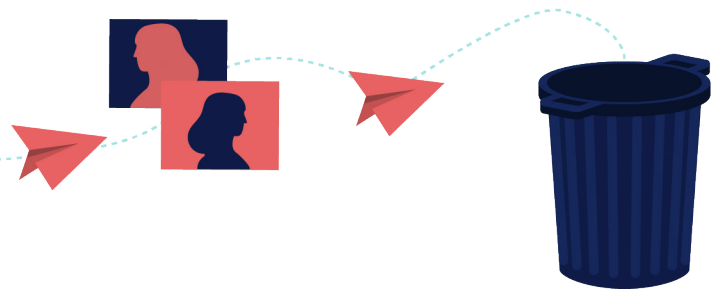
<sup>54</sup> Google Help Center. *Reset your Android device to factory settings*. Available at: <https://support.google.com/android/answer/6088915?hl=es>; Apple Support. *Restore your iPhone, iPad, or iPod to factory settings*. Available at: <https://support.apple.com/es-es/HT201252>



Another possibility is that your aggressor frequently checks your cellphone and there is nothing you can do to avoid it. In such cases, consider the following steps:



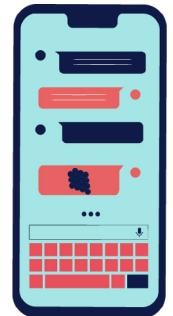
If you are thinking of seeking help, **remember not to leave any traces on your phone** that could be identified by the aggressor: delete photos, videos, messages, and internet search history entries that could indicate you are thinking about getting help.



Remember that all the information you search for on the internet and the websites you visit are recorded on your phone or computer. If you have searched for sensitive information that you want to keep hidden (for example, emergency numbers or violence support services), you can delete your browser search history and use incognito or private mode to leave no trace. The Google site explains how to [clear your Chrome browsing history](#)<sup>55</sup>.

You can agree on a “**secret code**” with people you trust to ask for help using specific emojis: for example, grapes emoji = 🍇 he’s attacking me. Memorize those codes and delete the message after sending it.

Try to **delete your chat message history** and use the communication codes agreed on with your support network.



Do not store any names on your phone that might give your attacker the idea that you are seeking help. For example, instead of identifying a contact as “Shelter,” label it “Ms. Martinez.”

Jot down the phone numbers of trusted contacts on a piece of paper and keep it in a safe place. This will be useful if the attacker prevents you from using your phone.

<sup>55</sup> Google Support. Delete your Chrome browsing history. Available at: <https://support.google.com/chrome/answer/95589?co=GENIE.Platform%3DDesktop&hl=es>



## What can I do if I am a victim of digital violence?

Every woman and girl has unique needs and experiences and faces online violence differently, so it is important not to generalize when offering strategies to prevent violence. Taking that diversity into account, here are some practical tips that could be useful when facing a situation of digital violence.

### Pause and remember: the victim of the violence is NOT at fault



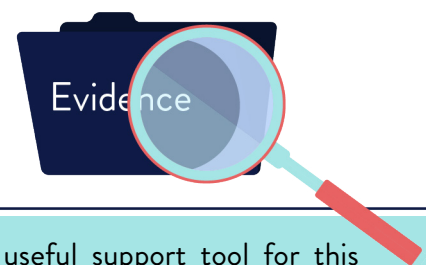
If you are attacked, harassed, threatened, or have your intimate images or videos posted on the internet, remember that it is never the victim's fault, even if you did not take the necessary digital precautions.

Online violence experienced by a woman or girl **is not her fault**, regardless of whether or not she took precautions beforehand or shared intimate images in a relationship of trust. **Responsibility always lies with the aggressor and not with the victim.**

In such situations, a personal self-care exercise or a bout of digital cleansing can be a great help to the survivor of violence. Consider taking a break, going for a walk or resting your eyes, chatting with a friend, or detoxing from social media. Online violence can be overwhelming, and taking a moment to take care of yourself can help you better navigate both the internet and the situation.

### Document

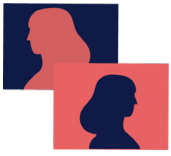
If you are a survivor of any kind of online violence, you should **document, record, and store in a safe and orderly manner any evidence of violence** that may be relevant (emails, messages received on social networks, SMS messages, audio messages, phone calls). Not only will this help you feel in control of the situation, it will also be useful should you decide to go to the authorities or to report the incident to the online platforms. This can be done manually, by saving the hyperlinks to the websites where the material appears, or by taking screenshots of the violence received using inbuilt Windows or Mac functions or with applications such as Snapfiles or Evernote<sup>56</sup>.



One useful support tool for this process is the [evidence chart](#) developed by Aceso.online.

<sup>56</sup> Microsoft Support. *How to take and annotate screenshots on Windows 10*. Available at: <https://support.microsoft.com/es-es/windows/c%C3%B3mo-tomar-y-anotar-capturas-de-pantalla-en-windows-10-ca08e124-cc30-2579-3e55-6db63e36fbb9>; Apple Support. *Take a screenshot on your Mac*. Available at: <https://support.apple.com/es-es/HT201361>; Snapfiles. *SnapDraw Free*. Available at: <https://www.snapfiles.com/get/alphascreenshot.html>; Evernote. Available at: <https://evernote.com/intl/es/features/webclipper>.

The evidence must be kept in an ordered, chronological fashion in folders. Precautions should also be taken to store evidence securely, either in password-protected digital format or even in hard copy.



**If you are a victim of non-consensual distribution of intimate or sexual content, the evidence must be saved and backed up before deleting it:** take screenshots of the websites where the material appears, the text messages or emails received (with time and date and group members), and, if applicable, download the video and save it.

**If you are a victim of domestic violence perpetrated by a current or former partner,** being able to document the violence when reporting it to the authorities can be very important. This can be done by using your mobile phone and various applications to save recordings and videos, take photos, take screenshots of violence on social networks, or record hostile text messages. Before doing so, however, you must determine whether this could put you at greater risk (for example, if your current or former partner has access to the device). If you feel a risk exists, it may be better to skip the documentation phase or consider sending the evidence to a trusted friend or family member for safekeeping (and, after sending, delete it from your phone and the cloud). It is also important to note the time, date, and place of the incident. More information on documentation can be found in the [Guide from Derechos Digitales and MariaLab](#).

## Block or report violence on social networks

Blocking bullies and cyberbullies on social media can be helpful in protecting yourself from harmful, unwanted, and inappropriate behavior, especially if the level of cyberviolence is causing a lot of anxiety or negative feelings. However, the **decision to block someone or not to block them is strictly personal** and will depend on the specific context.

- **Block and mute on Twitter.** As noted by Amnesty International, Twitter is the social network where women suffer the highest volumes of Cyber harassment and cyberstalking. Knowing how to use this social network safely is therefore an important matter: for example, knowing how [to block and mute potential stalkers](#) or [share block lists](#)<sup>57</sup>. The OAS publication [Media Literacy and Digital Security](#), also contains recommendations on tools for navigating Twitter safely and reporting tweets, messages, accounts, and rule violations.
- Instructions for blocking attackers can also be found on the sites of [Facebook](#), [Instagram](#) and [Tik Tok](#).

Social networks also have **specific tools for reporting harmful, abusive, or disruptive** information and behavior or violent threats, and they are obliged to examine such reports and take the necessary steps: from issuing a warning to the user responsible to the permanent suspension of their account. While much remains to be done to improve how internet platforms respond to cases of violence, reporting incidents allows patterns of aggression to be documented and helps raise the profile of the digital violence that affects millions of women online.

<sup>57</sup> Twitter Help Center. *About being blocked*. Available at: <https://help.twitter.com/es/using-twitter/someone-blocked-me-on-twitter>; *Twitter blog. Sharing blocked lists makes Twitter a safer place*. Available at: [https://blog.twitter.com/es\\_es/a/es/2015/compartir-listas-bloqueadas-convierte-a-twitter-en-un-espacio-m-s-seguro.html#:~:text=Para%20exportar%20o%20importar%20las,cuentas%20que%20se%20quieren%20exportar](https://blog.twitter.com/es_es/a/es/2015/compartir-listas-bloqueadas-convierte-a-twitter-en-un-espacio-m-s-seguro.html#:~:text=Para%20exportar%20o%20importar%20las,cuentas%20que%20se%20quieren%20exportar).

If you choose to report violence, you will normally need to **describe the incident or type of threat or send a screenshot** with the violent content or a link. Platforms including Twitter or Facebook also let you report content directly by clicking on the top right of the post when it appears. Reporting guidelines are available at [Tik Tok](#), [Instagram](#), [Twitter](#), [Facebook](#) and [YouTube](#)<sup>58</sup>.

## Get support

If you are a victim of online violence or suspect that you may be, you should seek help from family members, friends, or people you trust. If you find yourself in a high-stress situation, you can even ask a friend to monitor your social media updates or abusive posts so you don't have to do it personally.

The internet also hosts a large **support network and collective digital security practices** that women have created to support each other in cases of technology-facilitated violence. Several organizations have emergency numbers to call if you are a victim of non-consensual distribution of intimate images, and they can help you file reports with internet platforms, track images or videos circulating online, and request their removal (a list of some of these organizations can be found on table 2).

It is also important to reach out to mental health services. Digital violence can be overwhelming and have serious psychological consequences, from feelings of distress and depression to suicidal tendencies; the importance of emotional and psychological support during this process should therefore not be underestimated.

### Some organizations that can provide advice:

[Acoso.online](#)

[SocialTIC](#)

[Fundación Activismo Feminista Digital](#) (Argentina)

[MariaLab](#) (Brazil)

[SOS Digital](#) (Bolivia)

[Fundación Karisma](#) (Colombia)

[Datos Protegidos](#) (Chile)

[Ciberfeministas](#) (Guatemala)

[Frente Nacional para la Sororidad y Defensoras](#)

[Digitales](#) (Mexico)

[TEDIC](#) (Paraguay)

[Hiperderecho](#) (Peru)

**The provision of these resources does not represent an endorsement by the OAS or its Member States of their content or of the named organizations. The resources are presented as an example of those organizations, guides, tools, etc., that are available in the region so that readers can expand the information related to the subject matter addressed in this publication.**

<sup>58</sup> Facebook Help Center. What is blocking on Facebook and how do I block someone? Available at: <https://www.facebook.com/help/168009843260943>; Instagram Help Center. Blocking People. Available at: <https://help.instagram.com/426700567389543>; TikTok. Help Center. <https://support.tiktok.com/en>; Internet Matters. TikTok Privacy Settings. Available at: <https://www.internetmatters.org/es/parental-controls/social-media/tiktok-privacy-and-safety-settings/#:~:text=A%20bloquear%20o%20informar%20a,opciones%2C%20seleccione%20bloquear%20o%20informar>.

## Should I reply to the offender?

There is no right answer or universal formula that applies to interactions with online stalkers and perpetrators of violence, and whether or not to maintain contact will depend entirely on each person's priorities and what makes them feel most comfortable and safe.

In cases of domestic violence facilitated by new technologies, for example, the victim may feel that failing to respond could lead to an escalation of physical violence by the intimate partner or former partner; in such cases, victims might maintain online interactions or, conversely, feel safe enough to block all digital communication with them. As noted above, all experiences are different and, to the extent possible, it is best to weigh the options available in the specific personal context.

In other types of online violence, such as Cyber harassment incidents, priorities can be determined. If, for example, psychological and emotional protection is a priority, it may be best not to interact with the perpetrator(s) to avoid escalating the attacks. On the other hand, if it is important to expose the harassment or confront the aggressors and you can accept the risk of

further attacks or cyberbullying, one viable option is to write directly to the aggressors, retweet their comments, or forward them to friends, activists, organizations, or journalists to make them public and viral. Some tips on how to respond safely to harassment can be found at the [PEN America guide](#) and [Ciberseguras](#)<sup>59</sup>.

Another technique is to “talk back” to the attacks, using active, non-violent communication to give visibility to the aggressors' sexism and gender-based violence (e.g., incorporating irony or humor into your replies).

In short, there is no single answer to this question: it will largely depend on what each victim feels is best for her physical and emotional integrity.

## Report the attack to the authorities

Women and girls have the right to live a violence-free life online and offline, and the right to justice when this is violated. Lodging a report with the authorities can allow acts of digital violence to be duly registered and documented, and speed up the internet platforms' removal of harmful content, especially in cases of Cyber harassment, doxing, or non-consensual distribution of intimate images.

### Emergency numbers for requesting help:

**Argentina** (144) / 1127716463 (WhatsApp)  
**Belice** (0800-A-WAY-OUT / 672-9628 (WhatsApp)  
**Brazil** (180)  
**Bolivia** (800 14 0348)  
**Chile** (1455)  
**Colombia** (155)  
**Costa Rica** (911)  
**Ecuador** (09 992 8032)

**El Salvador** (2510-4300)  
**Guatemala** (1572)  
**Mexico** (911)  
**Nicaragua** (118)  
**Panama** (5006172)  
**Paraguay** (137),  
**Peru** (100)  
**Uruguay** (0800 4141 or \*4141 from a cellphone)



<sup>59</sup> Pen America. *You're not Powerless in the Face of Online Harassment*. <https://onlineharassmentfieldmanual.pen.org/fight-back-write-back/>; Ciberseguras. *Machitrol y autodefesa feminista*. [Macho troll and feminist self-defense]. Available at: <https://ciberseguras.org/machitrol-y-autodefensa-feminista/>

In addition, in cases of alleged intimate or domestic violence, given the recurrent use of technology to extend the scope of abuse and control, it may be important to notify the authorities of all digital violence incidents occurring during or after the relationship so that they can consider them in their analysis of the case and, if necessary, issue protective orders.

Likewise, under the Inter-American Convention on the Prevention, Punishment, and Eradication of Violence against Women (Convention of Belém do Pará), states have the obligation to prevent, investigate, punish, and duly redress online gender-based violence committed against women and girls.

While much remains to be done to improve the authorities' attention to and monitoring of online violence, the region has made progress with recent efforts to train public officials and, significantly, the creation in many countries of special cybersecurity laws and units.

It is also important to keep in mind that, even when faced with conduct that may be “new” to us, existing legal frameworks (including those where no standards have been set or where these offenses have not been criminalized) allow for various acts of online violence against women to be defined, investigated, prosecuted, and punished under cybercrime laws, laws on violence against women, criminal law, and privacy and data protection laws. This may require slightly more advanced knowledge of legal concepts and techniques, but it does not mean that the survivors of digital violence cannot pursue it if they receive proper guidance. The organizations listed on “To learn more” have carried out work on this subject, and they could be consulted if you decide to approach the authorities.



## Create community

---

**Talking about, sharing, and socializing the experience** can be very useful. By raising the profile of this form of violence, we can ensure the issue is discussed and contribute to the availability of support tools for victims and survivors.

Dealing with online violence can also be an opportunity to learn more about technology and digital safety measures. While they may appear very different, cybersecurity, gender equality, and violence prevention are intimately interrelated in the digital age, and by learning how to protect our identities and sharing those lessons with other women and girls, we are helping to make the internet a more inclusive space for all of us.



## To learn more

The inclusion of the following resources does not constitute an endorsement by the OAS or its member states of their content or the organizations named therein. They are presented as examples of the organizations, guides, tools, etc., that are available in the region, so that readers can further explore the topics covered in this publication.

### Organizations, websites, helplines, 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 nuestro@ cuerpo@ 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 educativos \(2018\).](#) [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, TEDxRiodelaPlata, 2016.

[Netizens.](#) Cynthia Lowen, 2019.

# *Glossary of Terms*

**Application (“app”).** A computer program created to carry out or facilitate a set of specific tasks (professional, leisure, educational, etc.) that runs on smartphones, tablets, or other mobile devices. There are free and paid-for apps, generally made available on specific distribution platforms or through the companies that own the operating systems of electronic devices.

**Blog.** A website that allows the creation and publication of short articles on specific or general topics.

**Chat.** A method for real-time digital communication between several users whose computers are connected to a network.

**Cloud.** The worldwide network of servers designed to store and manage data, run applications, or deliver content or services.

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

**Cyber-flashing.** Sending obscene photographs to a woman without her consent for the purpose of annoying, intimidating, or embarrassing her.

**Cybermobbing.** The actions of organized online groups that mass post offensive or destructive content in order to embarrass someone or have their social media profile removed.

**Data encryption.** A process for converting digital data into an enciphered format, which makes the information unreadable except to those who have the key to decrypt it.

**Deepfake.** An artificial intelligence technique that allows the production of fake videos of people that appear to be real by applying learning algorithms to existing videos or images.

**Denial of service.** A cyberattack aimed at overwhelming a server with service requests in order to prevent legitimate users from being able to access it. A more sophisticated method is the distributed denial of service (DDoS) attack, whereby requests are sent in a coordinated manner by several computers.

**Downblousing.** Taking non-consensual photographs down the top of a woman’s blouse.

**Doxing (also “doxxing”).** An abbreviation of the phrase “dropping docs” that involves the unauthorized extraction and online publication of personal information.

**Emoji.** A small digital image or icon used in electronic communications to represent an emotion, an object, an idea, etc.

**Firewall.** A physical or digital system designed to allow or prohibit access to or from a network in order to ensure that all communications between the network and the internet are carried out in accordance with the security policies of an organization or corporation.

**Gamertag.** A personal identifier used by those who play and share content in the Microsoft Xbox Live digital platform community. It consists of an alias, an avatar, or a picture and information about the player’s preferences.

**Gaslighting.** A form of psychological abuse that entails manipulating the victim’s reality so that they question their sanity, memories, or perception.

**Gender discrimination.** Any distinction, exclusion, or restriction made on the basis of sex that 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: Article 1 of the Convention on the Elimination of All Forms of Discrimination against Women.]

**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.*]

**Gender gap.** Any disparity between the status or position of women and men in society (differences in access to resources, rights, and opportunities).

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

**Gender roles.** Social and behavioral norms that, within a specific culture, are widely accepted as socially appropriate for people of a specific sex. They generally determine the responsibilities and tasks traditionally assigned to men, women, boys, and girls. [Source: UNICEF, UNFPA, UNDP, UN-Women. *Gender Equality, UN Coherence and you.*]

**Gender stereotypes.** A generalized opinion or prejudice about the attributes or characteristics that men and women possess or should possess, or about the social roles that both men and women play or should play. [Source: OHCHR, *Gender stereotypes and their use.*]

**Gender trolling.** Posting messages, images, or videos, and creating hashtags, for the purpose of harassing women and girls or inciting violence against them.

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

**Gender-based online violence or gender-based cyberviolence against women.** Any act of gender-based violence against women committed with the assistance, in whole or in part, of information and communication technologies — including mobile phones and smartphones, the internet, social media platforms, or email — or aggravated by the use thereof, directed against a woman because she is a woman or that disproportionately affects her. [Source: United Nations Special Rapporteur on violence against women.]

**Geolocation.** The ability to obtain the actual geographical location of an object, such as a radar, a mobile phone, or a computer connected to the internet.

**Grooming.** Deliberate acts by an adult to approach a minor for the purpose of establishing a relationship and emotional control that allows the adult to commit sexual abuse, engage in virtual relationships, obtain child pornography, or traffic the minor.

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

**Hacking.** The use of techniques and procedures 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 victim’s privacy or the confidentiality of the information stored therein, or to damage the data or hardware.

**Hashtag.** A string of characters starting with the # symbol, 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.

**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.

**HTTPS.** From “Hypertext Transfer Protocol Secure”: a network protocol for the secure transfer of encrypted data.

**Internet blackout.** An internet outage caused by an attack on a website, internet service provider (ISP), or internet domain name system (DNS). It can also be an outage due to an incorrect configuration of the web server infrastructure.

**Internet of Things (IoT).** The network of everyday internet-connected devices and objects that can share data with each other.

**Keylogger.** Malicious software that is placed between the keyboard and the operating system to intercept and record information about each key pressed on the device without the user's knowledge.

**Malware.** An apocoptation of "malicious software." A type of software that intended to infiltrate and/or damage an information system without the user's consent.

**Metadata.** Data about data, i.e., information that is used to describe the data contained in a file, document, photograph, web page, etc.

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

**Packs.** A collection of intimate or sexual images of women obtained and/or distributed without their consent.

**Phishing.** A scam perpetrated through a deceptive and apparently official electronic communication (email, text message, or by telephone) in which the scammer or phisher impersonates a trusted person or company so that the recipient provides confidential information (passwords, bank details, etc.). It is called "smishing" when the scam is done via SMS and "vishing" when it is done by recreating an automated voice.

**Revenge porn.** An incorrect term used to refer to the non-consensual distribution of intimate images or videos.

**Sex (biological).** The biological characteristics that define human beings as women and men.

**Sexting.** A practice that involves the creation and exchange of sexually explicit material between two people. It covers the consensual creation and transmission of images and the consensual creation of images that are then distributed without consent.

**Sextortion.** Threatening a person with the publication of intimate images or videos in order to obtain more sexually explicit material, engage in sexual intercourse, or obtain money.

**Social network.** An information service that offers users an internet-based communications platform where they can create a profile with their personal data, facilitating the creation of communities based on shared interests and allowing communications, so that users can interact through messages, share information, images, or videos by allowing those publications to be immediately accessible by all the people in a group.

**Software.** The collection of computer programs, instructions, and rules that allow electronic devices to perform certain tasks.

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

**Trending topic.** The most repeated word or phrases on social networks at a given time.

**Troll.** An unidentified person who posts messages online with the intent to annoy, provoke an emotional response from users, or disrupt online conversations.

**Uniform resource locator (URL).** The specific address assigned to each of the resources available on the network (pages, sites, documents) so that they can be located or identified.

**Upskirting.** The non-consensual taking of photographs from beneath a woman 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: Article 1 of the Inter-American Convention on the Prevention, Punishment, and Eradication of Violence against Women.]

**Virtual private network (VPN).** A computer network technology that establishes a secure extension of a local area network (LAN) over a public or uncontrolled network, allowing the computer on the network to send and receive data over public networks as if it were a private network (making this connection secure by encrypting the information).

**Virus.** A self-propagating computer program that is intended to alter the normal operation of an electronic device. Viruses differ from other types of malware in that they replicate automatically: in other words, they are able to copy themselves from one file or computer to another without the user's consent.

**Wi-Fi.** A network of interconnected wireless devices and also usually connected to the internet through a wireless access point.

# Bibliography

- Abdul Aziz, Z (2017). [Due Diligence and Accountability for Online Violence against Women](#). APC Issue Papers, Consultado el 9 de septiembre de 2020.
- European Union Fundamental Rights Agency (FRA) (2014). [Violence against women: an EU-wide survey](#). Accessed September 9, 2020.
- Amnesty International (2018). [Toxic Twitter-A Toxic Place for Women](#). Accessed September 9, 2020.
- (2017). [Amnistía revela alarmante impacto de los abusos contra las mujeres en Internet](#). [Amnesty reveals alarming impact of online abuse against women]. Accessed September 9, 2020.
- Amnesty International (2019). Corazones Verdes. *Violencia online contra las mujeres durante el debate por la legalización del aborto en Argentina* [Green Hearts. Online violence against women during the debate to legalize abortion in Argentina]. Available at: [https://amnistia.org.ar/corazonesverdes/files/2019/11/corazones\\_verdes\\_violencia\\_online.pdf](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. Accessed September 9, 2020.
- Barrera, L. (coord) (2017). *La Violencia en Línea contra las Mujeres en México*. [Online Violence against Women in Mexico]. Report of the Special Rapporteur on violence against women. Luchadoras, Mexico.
- Citron, D. (2014). *Hate Crimes in Cyberspace*. Massachusetts: Harvard University Press.
- United Nations. Committee for the Elimination of Discrimination against Women (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](#) [General recommendation No. 35 on gender-based violence against women, updating general recommendation No. 19]. Accessed September 9, 2020.
- (1992). A/47/38. [Recomendación General No. 19. La Violencia contra la Mujer](#). [General recommendation No. 19: Violence against women]. Accessed September 9, 2020.
- Inter-American Commission of Women (CIM) (2020). [COVID-19 en la vida de las mujeres. Razones para reconocer los impactos diferenciados](#) [COVID-19 in Women's Lives: Reasons to Recognize the Differential Impacts]. Accessed September 9, 2020.
- Cuellar, L and Sandra Chaher (2020). [Ser periodista en Twitter. Violencia de género digital en América Latina](#). [Being a Journalist on Twitter: Digital gender-based violence in Latin America]. Fundación Sentido, Comunicación para la Igualdad Ediciones, UNESCO.
- Deeptrace (2019). [The State of Deepfakes: Landscape, Threats and Impact](#). Accessed September 9, 2020.
- Derechos Digitales América Latina (2020). *COVID-10 and the increase of domestic violence against women in Latin America: A digital rights perspective*. Document presented by Derechos Digitales to the United Nations Special Rapporteur on violence against women, its causes and consequences.
- 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". *Violence against Women under International Human Rights Law*, 36-87. Cambridge: Cambridge University Press.
- Fanti K., A. G. Demetriou, and V. Hawa. (2012). "A longitudinal study of cyberbullying: Examining risk and protective factors". *European Journal of Developmental Psychology*, Vol. 9(2), 168-181.
- Federal Bureau of Investigation. Internet Crime Complaint Center (FBI-ICC) (2018). [Internet Crime Report](#). Accessed September 9, 2020.
- United Nations Children's Fund (UNICEF) (2017). [Access to the Internet and Digital Literacy](#). Accessed September 9, 2020.

- Freed, D., J. Palmer, D. Minchala, et al. (2017). "Digital technologies and intimate partner violence: a qualitative analysis with multiple stakeholders". In *Proceedings ACM Human-Computer Interaction*, Vol. 1, 46:1- 46:22.
- Goldsmán, F. and G. Natansohn (2020). *Cuidados durante la pandemia: ¿Cómo denunciar la violencia Doméstica?* [Caregiving during the pandemic: How to report domestic violence?]. Derechos Digitales and María Lab.
- Henry, N. and A. Powell (2018). "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research". In *Trauma, Violence, & Abuse*, Vol. 19 (2), 195-208.
- Henry, N. and A. Powell (2017). "Sexual Violence and Harassment in the Digital Era". In Antje Deckert y Rick Sarre (eds.). *The Palgrave Handbook of Australian and New Zealand Criminology, Crime and Justice*. Palgrave Macmillan.
- Henry, N. and A. Powell (2016). "Sexual Violence in the Digital Age: The Scope and Limits of Criminal Law". In *Social & Legal Studies*, Vol. 25 (4), 397-418.
- Henry, N., A. Powell and F., Asher (2018). "[AI can now create fake porn, making revenge porn even more complicated](#)". In *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". In K. Fitz-Gibbon, S. Walklate, J. McCullough, and J. Maher (eds.), *Intimate partner violence, risk and security: Securing women's lives in a global world* (pp. 52-70). Londres: Routledge.
- Hinduja, S., and 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](#)". In *ECPAT International and ECPAT Luxembourg*, Luxemburgo. Accessed September 9, 2020.
- Internet Governance Forum (IGF) (2015). [2015: Best Practice Forum \(BPF\) on Online Abuse and Gender-Based Violence against Women](#). Accessed September 9, 2020.
- European Institute for Gender Equality (EIGE) (2017). [La ciberviolencia contra mujeres y niñas](#). [Cyberviolence against women and girls]. Accessed September 9, 2020.
- Jane, E. (2017). *Misogyny Online. A Short (and Brutish) History*. Londres: Sage Publications.
- Jane E. (2016). "Online Misogyny and Feminist Digilantism". In *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](#)". In *MIT Technology Review*. Accessed September 9, 2020.
- Kwon, M., Y. S. Seo, S. S. Dickerson, E. Park, and J. A. Livingston (2019). "Cyber Victimization and Depressive Symptoms: A Mediation Model Involving Sleep Quality". In *Sleep*, 42(Supplement\_1), A322-A322.
- Qing Li (2006). "Cyberbullying in schools: a research of gender differences". In *School Psychology International*, Vol. 27(2), 157-170.
- Mantilla. K. (2013). "Gendertrolling: misogyny adapts to new media". In *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". In *International Journal of Evidence and Proof*, Vol. 23(3), 255-262.
- Follow-up Mechanism to the Belém do Pará Convention (MESECVI). Inter-American Commission of Women (2017). [Third Hemispheric Report on the Implementation of the Belém do Pará Convention](#). Accessed September 9, 2020.

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

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

Neris, N., J. Ruiz and M. Valente (2018). [Enfrentando Disseminação Não Consentida de Imagens Íntimas: Uma análise comparada](#). InternetLab. Accessed September 9, 2020.

United Nations Office on Drugs and Crime (UNODC) (2015). [Study on the Effects of New Information Technologies on the Abuse and Exploitation of Children](#). Accessed September 9, 2020.

--- (2019). University Module Series. Cybercrime. [Module 12. Interpersonal Crime](#).

United Nations. General Assembly (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. ccessed September 9, 2020.

---. Human Rights Council (UN-HRC) (2018). [Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence of women and girls in digital contexts](#). A/HRC/38/L.6. Accessed September 9, 2020.

---. Broadband Commission for Digital Development (UNBC) (2015). Working Group on Broadband and Gender. [Cyber Violence against Women and Girls. A World-Wide Wake-up Call](#). Accessed September 9, 2020.

Organization of American States (OAS) (2019). [Media Literacy and Digital Security: Twitter Best Practices](#). Accessed September 9, 2020.

Peña Ochoa, P. (ed) (2017). *Report on the situation of Latin American on gender-based violence exerted by electronic media*. Presentation for the Special Rapporteur on violence against women.

Pew Research Center (2014). [Online Harassment 2014](#). Accessed September 9, 2020.

--- (2017). [Online Harassment 2017](#). Accessed September 9, 2020.

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

United Nations Special Rapporteur on violence against women, its causes and consequences (UN-SRVAW) (2018). A/HRC/38/47. *Report on online violence against women and girls from a human rights perspective*. Accessed September 9, 2020. [https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session38/Documents/A\\_HRC\\_38\\_47\\_EN.docx](https://www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session38/Documents/A_HRC_38_47_EN.docx)

Inter-American Commission on Human Rights (IAHCR) Special Rapporteur for Freedom of Expression (RELE) (2018). *Women Journalists and Freedom of Expression: Discrimination and gender-based violence faced by women journalists in the exercise of their profession* (OEA/Ser.L/V/II), para. 48. Available at: <http://www.oas.org/es/cidh/expresion/docs/informes/MujeresPeriodistas.pdf>

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

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

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

Smith, Peter K. (2012). "Cyberbullying and cyber aggression". En S.R. Jimerson, A.B. Nickerson, M.J. Mayer, and 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*. Study commissioned by the Thematic Department of Citizen Rights and Constitutional Affairs of the European Parliament, Brussels: European Parliament.



Vela, E. and E. Smith. [“La violencia de género en México y las tecnologías de la información”](#). [“Gender-based violence in Mexico and information technologies”]. In *Internet en México: Derechos Humanos en el entorno digital* [Internet in Mexico: Human rights in the digital environment]. Ed. Juan Carlos Lara. Mexico: Derechos Digitales, 2016. Accessed September 9, 2020.

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

Web Foundation (2018a). [Advancing Women’s Rights Online: Gaps and Opportunities in Research and Advocacy](#). Accessed September 9, 2020.

Web Foundation (2018b). [Measuring the digital divide: Why we should be using a women-centered analysis](#). Accessed September 9, 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](#). Accessed September 9, 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

*Practical self-protection handbook: digital security tools and response strategies*

ISBN 978-0-8270-7306-7



OAS | CICTE



OAS | CIM | MESECVI