

Online gender-based violence against women and girls



Guide of basic concepts, 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

Foreword	05
Introduction	07
Part 1. Basic concepts: Acknowledging online violence is the first step to combating it	11
A. What is online gender-based violence against women?	12
B. What are the consequences for women and girls who are victims of online violence?	19
C. Who are the aggressors?	23
Part 2. Overview of the types of gender-based violence against women and girls facilitated by new technologies	26
A. Online creation, dissemination, distribution, or sharing of photographs, videos, audio clips of a sexual or intimate nature without the victim's consent	30
B. Unauthorized access, use, control, manipulation, sharing, posting, or publication of private information and personal data	33
C. Impersonation and identity theft	34
D. Acts that harm the reputation or credibility of a person	35
E. Surveillance and monitoring of a person	36
F. Online stalking	37
G. Online harassment	38
H. Cyberbullying	41
I. Direct threats of harm or violence	41
J. ICT-facilitated physical violence	43
K. Abuse, exploitation, and/or trafficking in women and girls using ICTs	43
L. Attacks against women's groups, organizations, or communities	44
Part 3. Preventing and combating online violence against women: The perspective of institutions	46
A. Interventions to combat online violence against women and girls	47
B. What is being done in the countries of Latin America and the Caribbean?	50
Part 4. Manual on self-protection and response: digital security tools to cope with online gender-based violence	52
A. Basic digital security recommendations: preventive measures	53
B. Advice on digital security for women victims of domestic or partner violence	63
C. What can I do if I'm being the victim of acts of digital violence?	66
D. To explore further	71
Glossary of terms	73
Bibliography	77

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.

Foreword

A quick search on the Internet is enough to highlight growing abuse, aggressiveness, cyberattacks, and unlawful actions that are disproportionately impacting women and girls because of their gender.

Although this phenomenon has gained greater notoriety over the past few years, it is often forgotten that none of this is hardly new. Violence against women observed on digital forums is an extension of the gender inequality and discrimination that have existed and continue to prevail in all aspects of their lives. This form of violence has become one of the principal risks for women's freedom of expression, privacy, and digital security and is seriously harming both the victims themselves and the digital community, because of how it undermines human rights on the Internet and the possibility of enjoying a cyberspace that is free, safe, and equitable and for the benefit of all.

Likewise, when women are victims of online violence, they often reduce their digital interactions and practice self-censorship because of the risk of violence being continued, thereby constraining their capacity to use Internet freely and confidently, on an equal footing with others and in line with their needs and preferences. It must be kept in mind that the cumulative impacts of online gender-based violence against women and girls transform and have multidimensional impacts on the Internet. They also alter how persons interact on the web and the benefits of the digital revolution in the information society. To date there is a persistent confusion about this issue, not only among the women themselves who have been its victim or who could potentially become victims, but also among policymakers, authorities, infrastructure operators, and national and international forums, who are used to viewing online gender-based violence as an isolated matter.

Along with this, it can be seen that women and girls are, for the most part, devoid of even minimal knowledge about digital security and protection measures on the Internet, which in turn heightens the risks and harm they sustain as a result of online violence. Although more and more women are using the Internet, the persistence of gender-based stereotypes that keep them away from handling technology, compounded by the normalization of online gender-based violence, leads them to navigate cyberspace without the information and tools they would need to prevent attacks on their digital integrity, in a situation of high vulnerability with respect to their attackers who have found new ways of expanding the control and violence they previously exercised offline.

In this context and in view of the many opportunities that are available for consolidating women's participation in digital spaces, the Cybersecurity Program of the Inter-American Committee against Terrorism (CICTE) and the Inter-American Commission of Women (CIM) of the Organization of American States (OAS) have decided to forge a partnership leading to a turning point in the region's approach to women's digital security.

On the one hand, this partnership shall mainstream a gender perspective into the region's cybersecurity strategy in order to acknowledge and combat the specific risks and threats that women encounter on the Internet. On the other hand, it wishes to build up the Hemisphere's efforts to prevent and eliminate violence against women by establishing a new approach, one that acknowledges the transformations that technologies are promoting among gender-based relationships.

On the basis of the present document, we intend to reach a broad public, raising awareness about the need for information that we have detected on this issue. For that purpose, there are recommendations, advice, and resources for women and girls who use the Internet, survivors of online violence, staff who are experts in providing services to victims of violence, civil servants, and persons with ties to the cybersecurity sector, all of whom will surely benefit from reading the present guide and putting it into practice.

We firmly believe that tools such as those appearing in the present guide are indispensable for building a cyberspace that is safe for all, because they highlight the realities, threats, and risks that usually go unnoticed but which exert an impact, not only on the lives of the victims, but also on how we understand and experience the Internet.

We therefore hope that the present guide shall contribute to spreading knowledge about, and building up capacities in, an area that is undergoing rapid change. At the same time, the CICTE and CIM are continuing to work hand in hand to promote this project, among others, to strengthen the right of women and girls to building safe networks and cyberspaces.

Alison August Treppel

Executive Secretary, OAS Inter-American Committee against Terrorism

Alejandra Mora Mora

Executive Secretary, OAS Inter-American Commission of Women

Introduction



The Internet has become an extension of human life and experience. New and diverse worlds, social practices, emotions, and relationships have emerged from this seemingly intangible space, flowing and converging there, but also, at the same time, being perceived in, and having an impact on, physical space. One can live in the Internet, rebuild one's identities, and undertake digital journeys and draw digital maps which open up countless possibilities that we would never have imagined otherwise.

The digital revolution has profoundly impacted how we communicate amongst ourselves, how we obtain information, how we interact, and in general how we make sense of ourselves. It has brought with it a gradual fusion of online-offline realities, which we are now experiencing as a single continuum (Shapiro, 2013) and it has rendered obsolete the separation between the “offline” world and the “online” world which had been common until just recently.

This online-offline interweaving has been a constant process, which in addition was given an unexpected boost by the current COVID-19 pandemic. The measures of confinement adopted almost worldwide since early 2020 because of the pandemic have expanded this virtual reality and speeded up the migration of countless human activities to the Internet, and millions of persons have had to build new ways of socializing online to compensate for the absence of face-to-face socialization.

It is important to avoid generalizations about the Internet's accessibility and impact on persons and communities, especially since, by the end of 2019, only 53.6% of the world's population were connected¹. The digital divide between countries, and in countries themselves, is still wide, and it is compounded by the digital literacy divide, in other words, the ability of persons to interact with online contents using critical judgment (UNICEF, 2017). These differences are further aggravated if they are viewed with a cross-cutting perspective, taking into account elements such as gender, ethnic origin, disabilities, age, or rural/urban context of persons.

In this scenario, the disparities being encountered by women on the Internet are particularly wide and underscore the systemic problems that have persisted with the digital revolution (Segrave and Vitis, 2017). In 2019, the International Telecommunication Union (ITU) reported that only 48% of women in the world had access to the Internet, compared to 55% of men. Furthermore, women are those who are in the greatest need of the digital literacy that would help them take full advantage of all that the Internet offers (Web Foundation, 2018).

Over the years, it has become evident that the Internet does not exist independently from the material, economic, political, and ideological conditions from which it emerged, which have always put women in a situation of subordination and disadvantage. In life online, as in life offline, women are discriminated against for the mere fact of being women and it is from that fact that pandemic proportions of gender-based violence have spread², which is now being facilitated by new information and communication technologies (ICTs). Because of the absence of adequate data and legal tools to protect its victims, however, it has become a pressing problem.

¹ International Telecommunication Union (2019). *Measuring digital development. Facts and figures 2019*. ITU Publications. Available at: <https://www.itu.int/en/ITU-D/Statistics/Documents/facts/FactsFigures2019.pdf>

² World Health Organization. “Devastatingly pervasive: 1 in 3 women globally experience violence.” Available at: <https://www.who.int/es/news/item/09-03-2021-devastatingly-pervasive-1-in-3-women-globally-experience-violence>

A brief search on the web shows there are many continuous acts of gender-based violence and hate, which taken as a whole highlight an extremely wide-ranging problem (Jane, 2017). There are millions of localized stories in different places of the planet pointing to online sexual harassment and rape threats, nonconsensual distribution of intimate audiovisual material, domestic violence on social media, and sexual exploitation facilitated by new technologies, among many other digital attacks against women on a daily basis (UN-SRVAW, 2018, para. 14).

In effect, in various investigations on the subject, it has been observed that, **compared to men, women are disproportionately the victims of certain types of violence** (UN-SRVAW, 2018; EIGE, 2017). According to a study published in 2015 by the ITU-UNESCO Broadband Commission for Sustainable Development, 73% of women have experienced some type of online gender-based violence, whereas 61% of the attackers were men (UNBC, 2015). Other sources point out that 23% of women have reported experiencing online harassment at least once in their life, and it has been estimated that 1 in 10 women has sustained some form of online violence since the age of 15 (UN-SRVAW, 2018, para. 16; EIGE, 2017:3; AI, 2017).

On many occasions, the mere fact that women are online puts them at risk of being victims of gender-based violence, a possibility that increases when they participate in digital conversations or in politics or when they make statements about issues involving gender equality (RELE, 2018; UN-HRC, 2018; AI, 2019).

Furthermore, as many sources have confirmed³, this violence has worsened with the constraints on movement and confinement required because of the COVID-19 pandemic: as more and more women and girls resort to digital spaces, online gender-based violence against them is rising (UN Women; CIM, 2020; Derechos Digitales, 2020). Likewise, as a further ramification of the gender-based digital divide, it has been observed that **many of those women are coping with this violence without benefiting from any basic knowledge about digital security measures** and personal data protection or the financial resources to purchase their own cell phone or data packages to communicate autonomously with the outside world and call for help.

This phenomenon is being observed in a scenario fraught with many challenges. As recognized by the European Institute for Gender Equality (EIGE), information on online violence against women is still scarce. Very little is known about the real percentage of victims and the prevalence of the harm it inflicts (EIGE, 2017). In addition, to date there is no single definition of online gender-based violence or any precise terminology agreed upon either regionally or internationally⁴. There is a wide disparity between the responses from states and those from international agencies, and as a rule, there is no adequate statutory framework to protect the victims.

³ 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 (2020). *COVID-19 in Women's Lives: Reasons to Recognize the Differential Impacts*. Available at: <http://www.oas.org/es/cim/docs/ArgumentarioCOVID19-ES.pdf>

⁴ As indicated by the United Nations Special Rapporteur on violence against women, there is still no consensus about the terminology to use to identify this form of violence. The expression “violence against women facilitated by information and communication technology (ICT)” is probably the most inclusive term because it encompasses the very wide range of behaviors this form of violence assumes. Nevertheless, in the present publication, following common usage, the terms “ICT-facilitated violence,” “online violence against women,” “digital violence,” and “cyberviolence against women” shall be used interchangeably.”

Fortunately, there has been recent progress made in connection with this issue. In the framework of the United Nations, in June 2018, the Special Rapporteur on Violence against Women published, for the first time, a report on online violence, which presents this type of violence as a growing problem for the international community and as a violation of women's rights⁵. To this report were added statements from the Human Rights Council and General Assembly of the United Nations⁶.

Renewed efforts have also been observed in the inter-American system. In particular, the Rapporteurship for Freedom of Expression (RELE) of the Inter-American Commission on Human Rights (IACHR) has already stated the importance of tackling growing online gender-based violence⁷, and recently the Cybersecurity Program of the Inter-American Committee against Terrorism (CICTE) and the Inter-American Commission of Women (CIM) forged a partnership to lay the groundwork for a regional dialogue that would make it possible to reach a greater in-depth understanding of the diverse forms of online violence and how they can be combated.

The present publication has emerged specifically in the framework of this partnership between CIM and the OAS Cybersecurity Program, which is contributing to regional efforts to highlight, prevent, and eliminate online violence against women⁸.

The document is divided into four parts, each one of which tackles the different thematic areas of violence against women and how they are facilitated by new technologies:

1° Part:

The first part presents certain basic concepts to ensure greater understanding of the features and impact of this violence.

2° Part:

The second part offers a descriptive list of the types of behavior deemed to be manifestations of online gender-based violence.

3° Part:

The third part is an overview of the latest breakthroughs in this area in Latin America, along with some thoughts about the measures that authorities can take to prevent and combat this type of gender-based violence.

4° Part:

The fourth part is a manual for self-protection and response specifically addressed to women and girls, with practical advice, preventive measures, and tools so they can strengthen their digital security against online gender-based aggression and violence.

⁵ United Nations Special Rapporteur on violence against women, its causes and consequences (2018). *Report on online violence against women and girls from a human-rights perspective* (A/HRC/38/47, 18 June 2018). Available at: <https://undocs.org/pdf?symbol=es/A/HRC/38/47>

⁶ United Nations Human Rights Council (2018). *Accelerating efforts to eliminate violence against women and girls: preventing and responding to violence against women and girls in digital contexts* (A/HRC/38/L.6, 2 July 2018). Available at: https://ap.ohchr.org/documents/S/HRC/d_res_dec/A_HRC_38_L6.pdf; United Nations General Assembly (2018). *Intensification of efforts to prevent and eliminate all forms of violence against women and girls: sexual harassment* (A/C.3/73/L.21/Rev.1, 14 November 2018). Available at: <https://undocs.org/es/A/C.3/73/L.21/Rev.1>

⁷ Special Rapporteur for Freedom of Expression of the Inter-American Commission on Human Rights. *Freedom of Expression and the Internet* (CIDH/RELE/INF.11/13, 2013); *Annual Report of the Inter-American Commission on Human Rights 2015* (OEA/SER.LV/III Doc.48/15 v.2, 2015); *Standards for a free, open, and inclusive Internet* (OEA/Ser.LV/II, 2017); and *Women journalists and freedom of expression* (CIDH/RELE/INF.20/18, 2018).

⁸ Gender-based violence pervading the digital world disproportionately impacts not only women and girls, but also persons identified as lesbian, homosexual, bisexual, transsexual, transgender, intersex, and non-binary, and takes on specific characteristics depending on the identities the violence is targeting. In view of its objectives and scope, the present publication shall exclusively address gender-based violence against women and shall highlight, whenever necessary, those cases in which other subjectivities are seen to be equally affected by the violence. Without doubt, the study on the prevalence and impact of digital violence on the LGBTIQ+ community continues to an important issue that is pending, and it is expected that it will be addressed in another volume subsequent to the present publication.

The four parts of this guide are complementary, although they can be consulted separately. On the basis of its structure, language, and design, it attempts to provide information that women and girls need when they are users of the Internet or survivors of online violence, as well as to authorities and staff specializing in providing services to victims of violence, without neglecting the big challenges they are still encountering or the complexity of reaching a very broad and diverse public by means of a document of limited length such as the present one⁹.

In particular, the *manual for self-protection and response* in the fourth part is designed for users to explore and mainstream into their daily digital self-care practices, but also for authorities and staff specializing in providing first-responder services to violence, so that they can benefit from a support tool in their work of advising victims of online gender-based violence. The manual contains various links to external websites, learning resources, and online tutorials making it possible for users to broaden their knowledge when interested in a subject, online threat, or specific tool.

As evident in its content, the present guide is geared to securing the digital empowerment of women and girls. It is based on the premise that they can acquire the necessary skills to protect themselves both individually and collectively in their online interactions and to create their own spaces in the virtual world where they will be free of violence so that the Internet can become for them a bridge rather than a barrier to the realization of their plans for the future.

⁹ To prepare the present guide, public documents and information available on official websites and studies published on the subject by specialized agencies and nongovernmental organizations were reviewed. It is important to highlight that many of the sources substantiating the present publication used qualitative research methods, such as surveys and digital ethnography, which made it possible to incorporate descriptions provided by the victims and survivors of online gender-based violence.

Part *One*

Basic Concepts:

**ACKNOWLEDGING
ONLINE VIOLENCE
IS THE FIRST STEP TO
COMBATING IT**





What is online gender-based violence against women?

Key elements of online violence against women:

01

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

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

02

03

It entails diverse human rights violations against women and girls.

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

04

05

It brings psychological, physical, sexual, and/or economic harm and suffering to its victims and has impacts on families, societies, and collectivities.

Online violence against women is not an isolated phenomenon, rather **it is located in a broader social context of gender inequality and discrimination against women and girls**. Because of this, in order to understand digital violence, it is crucial for us to pause first in order to examine what gender-based violence is, because the aggression and attacks experienced by women in their online interactions are nothing other than an extension of the violence which for many years has been impacting them in all spheres of their lives.

What is gender-based violence against women and girls?

For the purposes of the Convention of Belém do Pará, violence against women shall be understood as “any act or conduct, based on gender, which causes death or physical, sexual or psychological harm or suffering to women, whether in the public or the private sphere” (Article 1).

Gender-based violence is “**violence that is directed against a woman because she is a woman or that affects women disproportionately**” (CEDAW Committee, General Recommendation No. 19, para. 6).



Gender-based violence against women has its origin in stereotypes and prejudices about the attributes and characteristics of men and women and about expectations of the social duties that both must fulfill (for example, women are the only ones in charge of household chores, they do not carry enough authority to hold managerial positions, and they are weak by nature). These sociocultural patterns place women in a **position of inferiority or subordination with respect to men** and promote discrimination against women. These elements are the core driving forces behind the violence directed against them (MESECVI, 2017, para. 37).

It is important to underscore that violence operates in synergy with gender inequality, not only as a consequence of the latter, but as a social mechanism that strives to keep women at a disadvantage. This means that violence is used in many cases to “punish” or “correct” women whose attitudes or activities supposedly go against what society expects of them (MESECVI, 2017, para. 36).

The United Nations has pointed out that violence against women is a problem encountered everywhere in all countries of the world and constitutes a systematic and widespread human rights violation, with a high degree of impunity.



Women and girls experience gender-based violence throughout their lives in all offline and online places which they go to and participate in, whether at home, at school, at work, on streets, in politics, in the media, in sports, in public institutions, or when browsing social media (CEDAW, General Recommendation No. 35). This violence has no borders, is aimed at all women merely because they are women, and **has a higher impact on certain groups of women because they suffer from intersectional discrimination**, as in the case of indigenous and migrant women, women with disabilities, lesbian, bisexual, and transgender women, among others (MESECVI, 2017).

One of the most important achievements for women has been acknowledgment that **violence perpetrated against them is not a private problem**, but rather constitutes a matter of public interest and a human rights violation as enshrined in international instruments and domestic laws which specify the obligation of states to prevent, address, investigate, redress, and punish it (Edwards, 2010). In the case of the inter-American system, the right of women to live a life without violence is recognized in the Inter-American Convention on the Prevention, Punishment and Eradication of Violence against Women (Convention of Belém do Pará), the first treaty on the subject which brought the fight to end gender-based violence against women to the fore as an issue of regional interest¹⁰.

What is online violence against women?



Although many civil society organizations, the academic sector, and international agencies have made major efforts to specifically define online gender-based violence against women, as pointed out at the beginning, to date no consensus has been reached on its definition, nor has its terminology been consolidated (Van Der Wilk, 2018).

In 2015, the Association for Progressive Communications (APC), which has worked on this matter for more than ten years, defined online violence against women as **acts of gender-based violence that are committed, abetted, or aggravated in part or fully, by the use of information and communication technologies (ICTs)**, such as cellphones, the Internet, social media platforms, and email (APC, 2017: 3). Furthermore, the Due Diligence Project underscored that these actions lead or may lead to physical, sexual, psychological, or economic harm or suffering (Abdul, 2017).

As for the International Center for Research on Women, it defines technology-facilitated gender-based violence as acts by one or more persons that **do harm to others because of their sexual or gender identity or by imposing harmful gender standards**. These acts, for which the Internet or mobile technology is used, consist of stalking, bullying, sexual harassment, smearing, hate speech, and exploitation (Hinson et al., 2018: 1).

Finally, 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**” (UN-SRVAW, 2018, para. 23).

¹⁰ Inter-American Convention on the Prevention, Punishment and Eradication of Violence against Women. Available at: <https://www.oas.org/juridico/spanish/tratados/a-61.html>

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

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



This violation can be verified by checking a broad range of Internet platforms, for example, social media (Facebook, Twitter, TikTok), email services, instant messaging applications (WhatsApp), online dating applications (Tinder, Grindr, Hinge, Match.com), online videogames, content sharing sites (Reddit), online discussion forums (in the comments section of newspapers) or user-created platforms (blogs, sites for sharing images and videos).

Online gender-based violence is a constantly evolving concept. As recognized by the United Nations Special Rapporteur on violence, **the rapid development of digital technologies has impacts on online violence** and gives rise to different and new manifestations of violence as digital spaces are transformed and disrupt life outside the Internet (UN-SRVAW, 2018, para. 24).

Online violence has varied since the origins of the Internet and will surely continue to morph as digital platforms and technological tools move forward and establish further interconnections with our lives.

Ongoing online-offline process of violence: new forms of the same violence

Online violence is evident in the continuum of multiple, recurring, and interrelated forms of gender-based violence against women (UN-SRVAW, 2018).

We must avoid falling into the trap of considering online violence as a phenomenon separate from violence in the “real” world, because it actually is an integral part of the ongoing and interconnected manifestations of violence that women were already experiencing offline.



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

In 1989, Liz Kelly drew attention, for the first time, to the fact that different types of gender-based violence and abuse could be conceived as an **ongoing process of violence (the continuum of violence) in the lives and experiences of women throughout the world** (and not merely as sporadic or abnormal events), encompassing a wide spectrum of acts ranging from those expressly categorized as criminal offenses to behaviors of control and domination that are so common they have been accepted as normal (Kelly, 1989).

All types of gender-based violence against women have something in common: they are forms of coercion, abuse, or aggression that are used to control, restrict, or constrain the life, status, movements, and opportunities of women and to facilitate and guarantee the privileges of men (Kelly, 1989).

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

Thus we observe that, in the digital age, forms of violence persist or are amplified by the use of new technologies and that new forms of online sexism and misogyny are emerging, which in turn can step out of cyberspace to become physical aggression against women. Violence against women can, for example, start with sexual harassment in a public space, such as “honor-based” violence in a community or as physical attacks perpetrated by an intimate partner, which in turn can be transformed and relocated via technology by the nonconsensual dissemination of intimate images, acts of online harassment, sexist hate speech on social media, surveillance using a cellphone, etc. Conversely, violence may start with social media interactions by a minor with supposedly new friends and culminate with encounters during which acts of sexual violence or kidnapping are perpetrated. All of these new acts have an impact on women’s interactions not only online but also in all spaces of their offline life.

In many cases, gender-based violence has intensified, because digital spaces provide very convenient anonymity, and abuse can be perpetrated from anywhere, via a wide range of new technologies and platforms which perpetrators of violence have at their disposal, and which make it possible for digital contents to spread rapidly and remain online permanently.

Some aspects of the new ICT that have contributed to transforming gender-based violence against women are their rapid expansion, online permanence of contents which leave an indelible digital record, their replicability and global searchability, and the possibility of easily locating persons and information about them, which facilitates the contact of aggressors with the women they target, as well as secondary victimization (UN-SRVAV, 2018).



Spotlight:

The close connection between domestic violence and new technologies

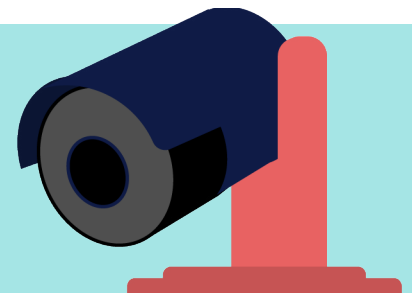


For several years now, ICTs have been performing a very important role in the upsurge of new strategies of abuse and control used by perpetrators of domestic and partner violence (Dragiewicz, 2019). Diverse studies have revealed that **77% of the victims of online harassment have also sustained some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

As new technologies have been mainstreamed in virtually all daily activities of persons, aggressors have taken advantage of, extended, and intensified abusive, possessive, and domineering behaviors that had not been possible before (Woodlock, 2017). As a result, women are now experiencing this violence without any bounds in terms of space and time and with the added feeling that the aggressor is present everywhere (Harris, 2018), which has serious impacts on their mental health¹¹.

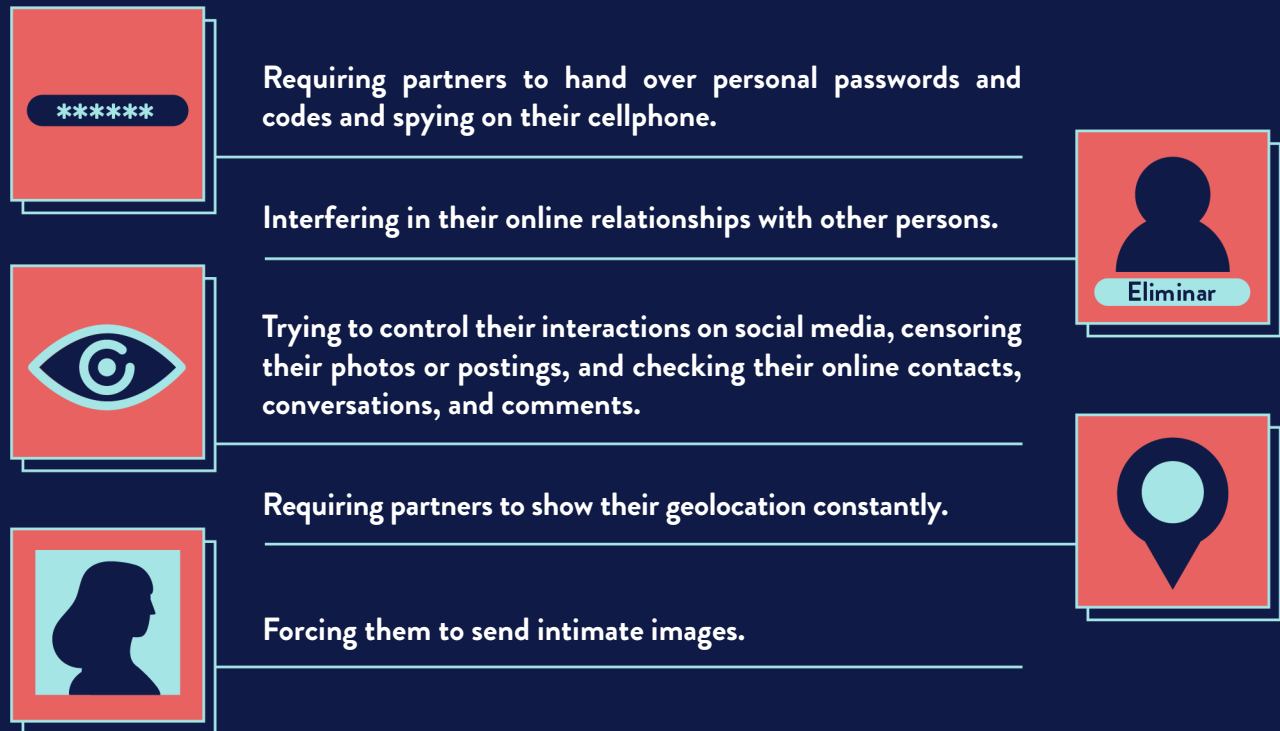
Although research on this matter is still in its infancy, various initial studies indicate that certain technologies are used more widely than others to perpetrate abuse and exercise online control in contexts of domestic or partner violence. And that holds true for text messaging, social media such as Facebook, or software to monitor the location of victims via their cellphones (Dragiewicz, 2019).

Nevertheless, the manifestations of digital abuse and surveillance of women and intrusion into their lives are constantly changing and encompass a wide range of actions, from incidents of identity theft by the partner or former partner to make purchases via Internet to an aggressor's use of smart devices installed in homes, such as thermostats, cameras, microphones, alarms, or locks to create psychological stress in victims.



¹¹ 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>

It has also been observed that, in young couples, **new behaviors are becoming normalized in the current online-offline context, disguised by notions and myths about romantic love, but at the bottom of this partners are seeking to impose cybercontrol** and restrict the digital lives of women. Some of these practices are listed below:



In the specific case of victims of domestic and partner violence, online violence can deter the women from abandoning the relationship, because they often feel trapped in a situation they cannot escape from. It has also been documented that, in many cases, digital violence increase at the time of separation (not only against the victims but also their children, relatives, friends, or intimate partners). It would even seem that, with certain aggressors, breaking up abruptly and cutting off all online communication or interaction can increase the risk for survivors and their family (Dragiewicz, 2019).

To this can be added the **exponential rise throughout the world of physical violence and sexual abuse against women and girls during the COVID-19 pandemic** (UN Women, CIM, 2019). Because of lockdown requirements, they have been required to remain locked up with their aggressors, and for them technology has become an indispensable tool to communicate with the outside world and have access to caregiving services.

In this context, supporting victims and survivors of domestic and partner violence so they can recognize online control, protecting their digital safety and integrity, and **using technology as a means of support to break away from the circle of violence** are essential and must now become an integral part of the ecological models to prevent, provide services for, and punish violence against women, which entails working with families, communities, and institutions.



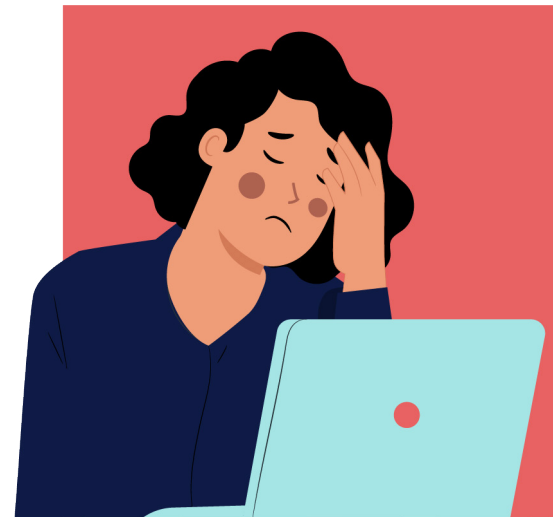


What are the consequences for women and girls who are victims of online violence?

Online violence against women does real harm

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

The manifestations and repercussions of this violence may be highly diverse depending on the form it takes. For example, depression, anxiety, stress, fear, and panic attacks in cases of online stalking, suicide attempts by women victimized by the nonconsensual dissemination of sexual images, physical harm done to victims of doxxing¹², or economic damages because of the loss of employment as a result of online smearing of their reputation (Pew Research Center, 2017; Kwon et al., 2019; AI, 2017).



Unfortunately, there continues to be inadequate understanding of the gravity of the consequences and harm caused to women by online violence, harm that is often deemed to be “not real” because they were found on the Internet. This reflects a mistaken understanding of the online-offline continuum in which we are now conducting our lives, as well as the characteristics of the continuum of multiple and interrelated forms of violence that women and girls are experiencing in their social interactions.

It has also been observed that **the characteristics of certain technologies exponentially increase the magnitude of the harm inflicted by certain acts of violence**, extending beyond that of the original act (their fast-spreading searchability, global scope, anonymity, and permanence) (APC, 2017), because women are judged more severely than men for their online attitudes. This is the case of incidents of nonconsensual dissemination of sexual images, where it has been observed that women and girls who have been stigmatized for exercising their right to sexuality and have seen their images posted, have to experience permanent humiliation and shame in their social environment, which in many cases has led them to commit suicide.

¹² Doxxing or doxing is a cyberattack consisting of obtaining someone’s personal information and making it public online.

Women impacted by violence oftentimes hold themselves personally responsible for the actions that might have motivated the violence and they withdraw from online spaces, censor themselves, or become socially isolated (Citron, 2014). Furthermore, it is very common for them to be revictimized by relatives, authorities, and the media, which frequently charge them with the responsibility of protecting themselves instead of highlighting the unlawful conduct of the aggressors, and that is how they normalize and minimize the violence (UN-SRVAW, 2018, para. 25).



Coupled with these individual impacts, **online violence leads to collective and intergenerational harm** and incurs both direct and indirect costs for societies and economies, because victims and survivors not only require medical care and judicial and social services, but they may also see their productivity and interactions in the community curtailed (UNBC, 2015). Likewise, **this violence has a silencing effect**, because it is a direct threat to women’s freedom of expression (AI, 2017) and undermines their online access and participation as active digital citizens, which in turn leads to a democratic deficit by preventing women’s voices from being heard freely in online debates (UN-SRVAW, 2018, para. 29).

Research on the matter indicates that 28% of women who had suffered ICT-based violence intentionally reduced their presence online (UN-SRVAW, 2018, para. 26) and censored themselves for fear their privacy or safety would be breached (AI, 2017). To make things worse, survivors were often advised to “stay away from” or “drop out of” technologies after an incident of violence.

Are there women who are being attacked online more than others?

When reviewing online violence, it is important to avoid broad generalizations based on a supposedly common experience among women. In each case the specific characteristics of the different online experiences of women must be taken into account, as well as their diverse identities defining them.

Although online violence is a common phenomenon among women and girls who are navigating the digital world, it is also true that it **affects women differently depending on other forms of discrimination** they encounter in their daily lives because of their race, ethnic origin, sexual orientation, gender identity, social class, or nationality.

According to Amnesty International, women encountering discrimination offline because of specific features of their identity frequently find that online violence and abuse against them are targeting those same features (AI, 2018). These women are especially vulnerable to victimization because of a combination of forms of abuse that reflect racist and sexist beliefs, stereotypes, social prejudices, and ideas on an alleged gender order.

In her 2018 report, the United Nations Special Rapporteur on violence against women pointed out that certain groups of women are especially targeted by online violence, such as women members of parliament, journalists, young women, women who participate in online debates, and women from ethnic minorities or who belong to the LGBTIQ+ community (UN-SRVAW, 2018; Van Der Wilk, 2018; UNBC, 2015; EIGE, 2017; Henry and Powell, 2016). As a rule, digital violence against them takes the form of attacks on their visibility, sexuality, freedom of expression, and political participation. It is evident that one of the goals of online violence is to keep women silent and in conditions of subordination in society.



Did you know that?



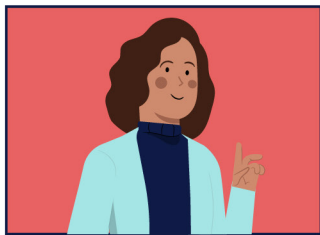
There are several reports indicating that women 18 to 24 years of age are particularly at risk of being targeted by online violence, with a 27% higher likelihood of being victims of online abuse, compared to men (APC, 2001; UNBC, 2015). The Pew Research Center also reported that these women are particularly vulnerable to online harassment (Pew Research Center, 2014 and 2017).

It has been observed that the mere fact of being a woman and a public figure or of participating in politics entails being the target of extremely misogynistic comments, sexual violence, and online threats of physical violence and femicide (Rawlison, 2018). Women who participate in public debates on the Internet or who write about gender issues are disproportionately the victims of online harassment aimed at keeping them silent and intimidating them, and they are customarily the target of massive campaigns of sexualized verbal abuse and violence, along with hate speech and threats of sexual abuse and rape (UN-SRVAW, 2018, para. 25). According to Amnesty International, 88% of women suffer abuse and online harassment after they have posted feminist contents (AI, 2018).



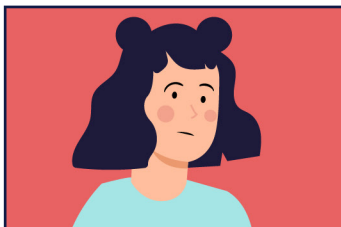
Spotlight: Women who tend to be the targets of certain types of online violence¹³

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



Human rights defenders, journalists, women participating in political activities, active participants in online debates, or women who have a public profile. These women are frequently the target of online harassment and stalking on the Internet, including online threats and verbal abuse of a misogynistic and sexual nature.

Lesbian, bisexual, transgender, or intersex women, women with disabilities, women from an ethnic or racial minority, indigenous women or women from marginalized groups. These women are usually the target of online hate speech or abuse, with homophobic, racist, or sexist slurs.



Young women are also the frequent target of online sexual violence, which reproduce forms of stalking, harassment, and sexual abuse.

¹³ Association for Progressive Communications (APC). *From impunity to justice. Exploring corporate and legal remedies for technology-related violence against women 2012-2015*. Available at: <https://genderit.org/onlinevaw/>



Who are the aggressors?

It has been observed that aggressors and those responsible for online gender violence against women are identified, as a rule, as male (Van Der Wilk, 2018, 34-37). These aggressors may be a person the victim does not know (such as an online sex stalker who systematically targets several women for his attacks or an individual who engages in child grooming, or the online sexual grooming of children)¹⁴ or a member of the victim's circle of relatives, coworkers, or friends. Certain studies indicate, for example, that between **40% and 50% of the victims knew their online aggressors** (a former intimate partner, a relative, a friend, or a coworker) and that, **in one third of cases, the aggressors were having or had had an intimate relationship with the person being attacked** (Pew Research Center, 2017; APC, 2015).

There are two identifiable types of persons responsible for online violence against women (Abdul, 2017):

The original perpetrator:

The person who committed the initial act of online violence or abuse or who created, manipulated, or posted, for the first time, harmful information, personal data, or intimate images without the victim's consent.

The secondary perpetrator or perpetrators:

The person or group of persons who are involved in continuing or disseminating an online act of violence by resending, uploading, reposting, or sharing harmful information, personal data, or intimate images obtained without the victim's consent.

What do aggressors seek when they engage in online violence against women and girls?

The purpose of violence is to create a hostile online environment for women in order to shame, intimidate, disparage, belittle, or silence them via surveillance, theft or manipulation of information, or control over their channels of communication (AI, 2018).



Spotlight:

Online violence as a violation of the human rights of women

As underscored by the United Nations Special Rapporteur on violence against women in her 2018 report, the human rights of women as enshrined in international treaties must also be protected online, in particular “through the prohibition of gender-based violence in its ICT-facilitated and online forms” (UN-SRVAV, 2018, para. 17).

¹⁴ Child grooming, or online sexual grooming of children, consists of deliberate acts by an adult to approach a minor in order to initiate a relationship and secure emotional control to facilitate sexual abuse, undertake virtual relationships, obtain child pornography, or engage in the trafficking of minors.

As for the United Nations Human Rights Council, it recognized that violence in online contexts prevents “women and girls from fully enjoying their human rights and basic freedoms” as enshrined 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 which online violence is violating are indicated below (UN-SRVAW, 2018; Vela and Smith, 2016; APC, 2017):

- Right to equality and nondiscrimination.
- Right to live free from violence.
- Right to personal integrity.
- 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 data protection.
- Right to protection of honor and reputation.
- Sexual and reproductive rights of women.



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



Spotlight:

The Internet of things (IoT) and domestic violence

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

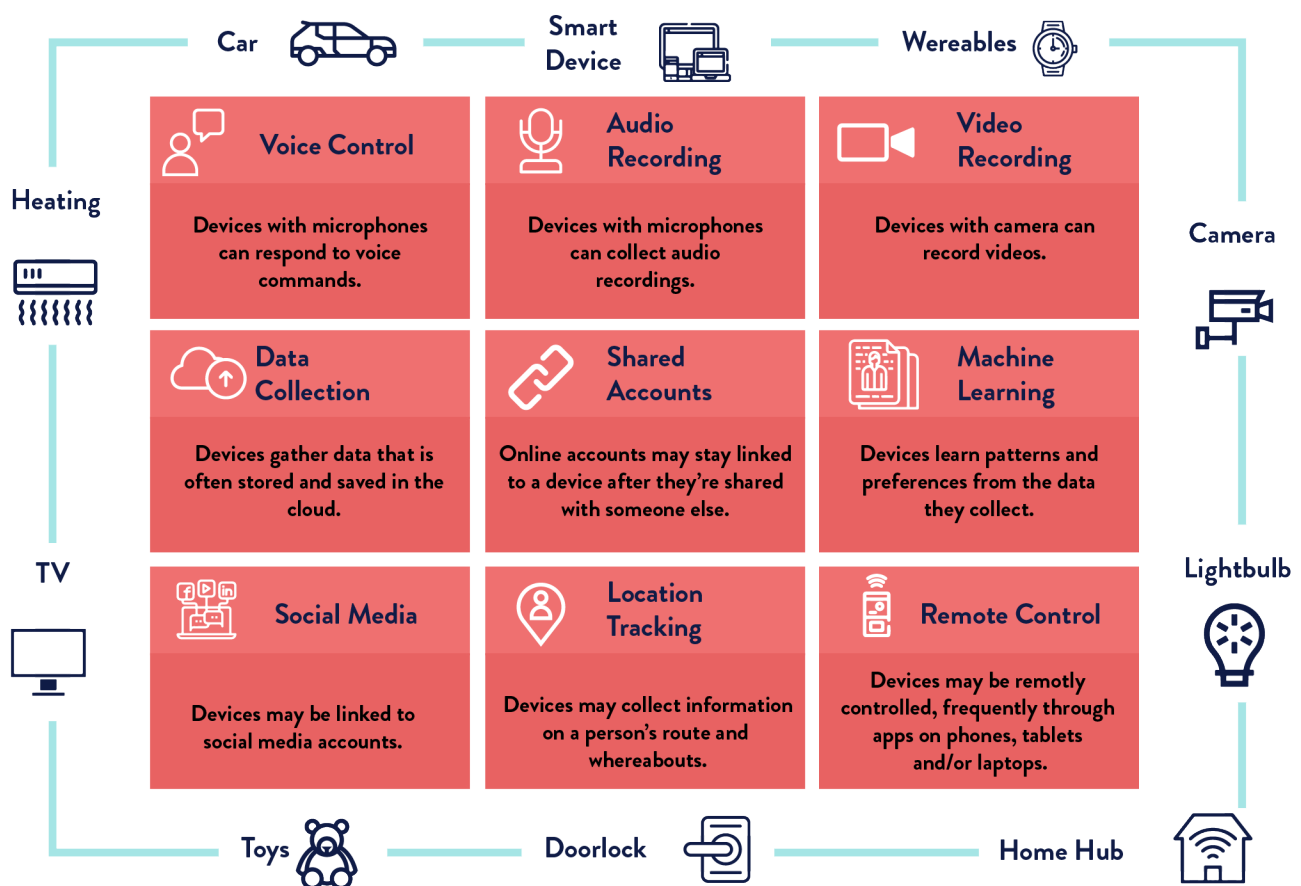
It is said that these devices are “smart” because they can gather and process data, communicate between each other, and carry out actions with any direct human intervention. For example, via the IoT, a home’s security system can be controlled from an application installed in a cellphone using voice commands addressed to virtual assistants, and cameras or lighting systems can be disabled or enabled remotely.

The IoT has many benefits because it facilitates practical matters of daily life, but it can also entail potential risks for privacy and security because the devices assume that all persons using them trust one other. For example, in the case of domestic violence, an aggressor can use the IoT to monitor a victim or prevent that person from opening the locks of their house, or a hacker can remotely control a security camera to take or record intimate images or videos directly in a victim’s home without consent.

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

- Online stalking.
- Coercive and controlling behaviors, including threats of harm or abuse to frighten a victim, for example, by denying them the right to control heating, lighting, or locks at home.
- Digital gaslighting, which is a form of psychological abuse involving the manipulation of a victim's reality, whereby the victim's sanity, memory, or perceptions are put into question.

How IoT can affect victims of domestic and sexual violence



Implication:

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

Consideration:

It is important that support services are aware of IoT's functionalities, as they may inform assessments and safely planning for victims.

Mitigation:

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

Information:

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

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

Part *two*

OVERVIEW OF THE TYPES OF

GENDER-BASED VIOLENCE

AGAINST WOMEN AND GIRLS
FACILITATED BY NEW
TECHNOLOGIES





It is important not to lose sight of the fact that online gender-based violence against women is a term encompassing a broad range of harmful or offensive practices and behaviors and online-offline contexts which are evolving in lockstep with technological breakthroughs.

What we understand to be online violence against women involves, in fact, highly diverse practices and behaviors that could be identified as online criminal offenses or unlawful acts that carry administrative, civil, or criminal responsibilities depending on each country's laws (IGF, 2015; UN-SRVAV, 2018; APC, 2017).

To date there is still a huge disparity in the terminology used to refer to the diverse types of online violence against women and their manifestations, with constant variations among the terms used by states, international agencies, nongovernmental organizations, and the academic sector (Van Der Wilk, 2018). Unfortunately, this has spread confusion about how to classify said behaviors and, in many cases, has led to imprecise references in domestic law.

In an effort to clarify this scenario, **a non-exhaustive list of behaviors and cyberattacks deemed to be online gender-based violence against women is presented below, with their respective descriptions**, for the purpose of facilitating the identification of personal experiences and, as a result, learning about the measures that can be taken to strengthen the digital security of victims (see the fourth part of the present guide).

This catalogue was established on the basis of a review of bibliographical references and should not be viewed as something fixed or static, because digital violence is evolving constantly alongside technology, and new manifestations of violence are emerging as new technological tools appear (UNBC, 2015).

Likewise, as will be noted in the present section, it is important to bear in mind that there may be cases in which two or more forms of digital violence are being used simultaneously, are interdependent (for example, online threats followed by the nonconsensual dissemination of intimate images) or are coupled with other forms of violence outside the Internet (as often happens in cases of domestic violence).

In any case, it must be kept in mind that these cyberattacks and online acts are deemed to be gender-based violence because they are inflicted upon women merely because they are women (in other words, because of their gender identity) and because they affect women disproportionately.



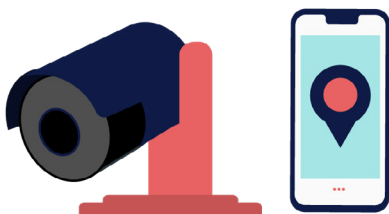
Types of gender-based violence against women and girls facilitated by new technologies:



Unauthorized access to, use, manipulation, sharing, or distribution of personal data.



Acts that damage a person's reputation or credibility.



Online stalking.

01

Online creation, dissemination, distribution, or sharing of photographs, videos, or audio clips of a sexual or intimate nature without the victim's consent.

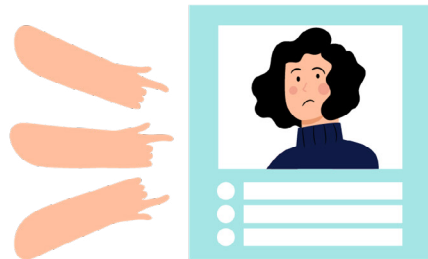
02



03

Identity theft or impersonation.

04

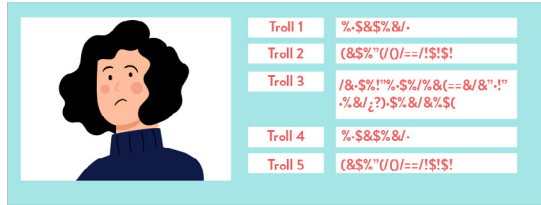


05

Acts that involve surveillance and monitoring of a person.

06





Cyberbullying.



Technology-facilitated physical violence.



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

07

Online harassment.

08



09

Direct threats of harm.



10

Abuse and exploitation of women and girls using technologies.

11

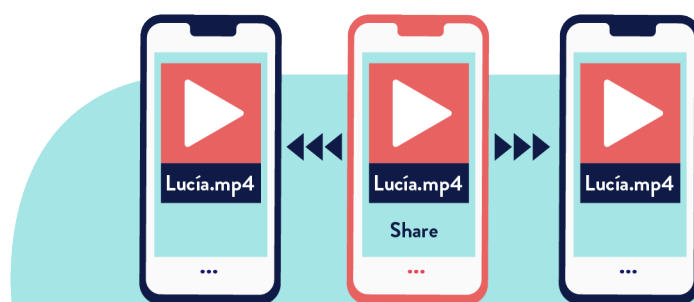


12



Online creation, dissemination, distribution, or sharing of photographs, videos, audio clips of a sexual or intimate nature without the victim's consent

Women are the principal victims of this form of digital violence, which affects them disproportionately throughout the world. Diverse studies have confirmed that 90% of the persons affected by the online distribution of intimate images without their consent are women (UN-SRVAW, 2018; *Cyber Civil Rights Initiative*).



It consists of creating, sharing, or disseminating online, **without consent**, intimate or sexually explicit materials, images, or videos obtained with or without the consent of a person, for the purpose of shaming, stigmatizing, or harming that person (UN-SRVAW, 2018, para. 41).

This form of violence can occur in a broad range of interpersonal contexts and relationships: in an intimate relationship based on trust in which these images are transmitted voluntarily by a person to his or her partner or former partner (probably by sexting), as part of online stalking or harassment patterns by friends, acquaintances, or unknown persons or when the material is obtained by hacking¹⁵ or physical access to devices.

It also includes the following acts:

- 01 Recording and distribution images of sexual abuse.
- 02 Taking, without consent, photographs or videos of intimate body parts of women in public spaces and sharing them online (for example, photographs taken up the skirt or down the blouse, acts identified as upskirting, downblousing, or creepshots).
- 03 **Creating sexualized images that are edited using photo montage techniques, or deepfake videos**, in which case the images or videos of the women can be taken from online sites or social media accounts and placed over the body of other persons to simulate sex scenes or pornographic content for the purpose of undermining the victim's reputation.

¹⁵ Hacking involves a hacker using techniques and procedures to break into third-party computer systems without authorization for the purpose of manipulating them or obtaining information or having fun. Cracking is a practice similar to hacking but it entails infiltrating third-party systems for criminal purposes to violate the intimacy of the affected persons or the confidentiality of the information or to damage the information or hardware.



What is a deepfake video?

Since 2017 there are software programs using automatic learning techniques to swap the face of one person for that of another (Knight, 2019). These programs are being used to create fake pornographic videos and to post them online (Farokhmanesh, 2018). With these videos, women who participate in politics in particular have been attacked, although it is expected that use of this technology will spread because it has become increasingly accessible to users who are not experts (Deeptrace, 2019). In addition, because deepfake videos use automatic learning techniques, eventually it may become difficult to differentiate a fake video from a real one without the help of forensic tools (Maras and Alexandrou, 2018).



The production of intimate photographs or videos without the victim's consent **may be coupled with extortion or threats to disseminate them** or may take place without the victim's knowledge in closed social media groups in which various men disseminate images of naked women without their consent for the sexual gratification of other members or as part of money-making schemes in which the aggressors compile and sell links with files or "packages" of sexual images of women obtained by diverse means without their consent (files which, in countries like Mexico and Chile, have been called packs)¹⁶.

It is also **very common to infiltrate the personal data of the women appearing in those images or videos**, which in turn forces many of them to drop out of school, quit their job, leave home or their communities to avoid constant humiliation (Henry, Powell and Flynn, 2017).



Reminder...

This form of online revenge is commonly called "porn revenge." Nevertheless, it is not a correct term, and its use is problematic because it does not reflect the diversity of motives driving the perpetrators, as it extends beyond revenge itself and encompasses a range of behaviors, from reassertion of their masculinity to economic extortion or sexual gratification. This term also minimizes the harm it inflicts upon victims, conceals the nonconsensual component of the behavior, and puts emphasis on the image rather than on the abusive behavior of the perpetrators (Powell, Henry, and Flynn, 2018).



What is sexting?

The term sexting refers to a practice that involves creating and sharing sexually explicit materials (UNDOC, 2019; Interagency Working Group, 2016). It may include creating and sending images with the consent of the persons involved or creating images that are disseminated without their consent (Salter, Crofts, and Lee, 2013, p. 302).

In various studies, it has been proven that it is a widespread practice among young people of both genders, who are using these technologies as a tool for sexual expression. It has been observed, however, that sexting appears in contexts where young women and girls are subjected to greater social pressure than boys to share sexual and degrading images of their body, whereas young men and boys are under pressure to request images, receive them, and share them with their male friends in order to reassert their heterosexual identity (Walker, Sancí, and Temple, 2013).

¹⁶ 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>



Spotlight:

Important aspects of sexting and the dissemination of intimate images and videos without due consent are described below:

01

Although there may be consent to exchange intimate photographs with someone or to record sexual acts (even in the presence of other persons), **this consent does not entail permission to store, post, publish, reproduce, or disseminate those contents.** Consenting to a recording does not mean that consent has been granted for another stage of the above-mentioned process. Whoever does the latter is breaching the intimacy of the person who participated in the practice of *sexting*. This is a serious form of gender-based violence, a human rights violation, an unlawful act, and has already been formally classified as a criminal offense in many countries.

The practice of *sexting* must not be stigmatized. All of us, women and men, have the right to use technology to express our sexuality. Nevertheless, when doing so, it is very important to bear in mind that there are risks involved and that, as a result, it is necessary **to consider digital security.**

02

03

States have the obligation of adopting appropriate measures to prevent, investigate, punish, and repair harm caused by this form of violence. Internet platforms are also required to prevent the dissemination of intimate images and videos without due consent, to remove these contents, and to reduce or mitigate related risks.

Information on this form of digital violence, as well as advice to report a case to Internet platforms, in addition to details about the different laws in the countries of Latin America supporting a whistle-blowing report of this nature, can be found on the following website: [Acoso.online](https://acoso.online). The website of the organization [Without my Consent](https://withoutmyconsent.org) also has a wide range of resources to support survivors of this form of violence¹⁷. Additional recommendations and advice can also be found on page 33 of the present guide.

It is stressed that providing these resources does not mean that the OAS or its member states are endorsing the contents or organizations identified herein. These resources are offered as an example of those organizations, guides, tools, etc., that are available in the region for readers to expand their access to information related to the subject of the present publication.

¹⁷ 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, posting, or publication of private information and personal data



According to Amnesty International, one fourth of all women have been victims of doxing at least once in their life (AI, 2017).

This form of violence appears in the form of **hacking of online accounts or devices** of a person (cellphones, computers, tablets, etc.) to obtain, manipulate, and/or post information without authorization via the theft of passwords, the installation of spyware, the theft of equipment or keyloggers¹⁸ (APC, 2017). It can also involve the unauthorized access to, and total control over, a person's accounts or devices.

Doxing or doxxing:

The term comes from the phrase *dropping docs*, which consists of **the unauthorized extraction and posting of personal information**—such as the complete name, address, phone numbers, emails, names of spouse, relatives, and children, financial or employment details—as a way of intimidating the targeted persons or for the purpose of locating them in “the real world” in order to harass them (APC, 2017; Women’s Media Center, 2019). It has also been observed that personal information can be posted on porn websites along with the announcement that the victim is offering sex services.

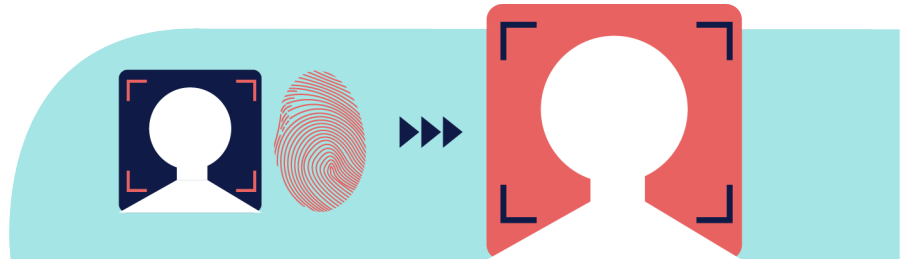


¹⁸ A keylogger is a malware installed between the keyboard and the operating system to intercept and log information from each key struck on the device without the user being aware of it.

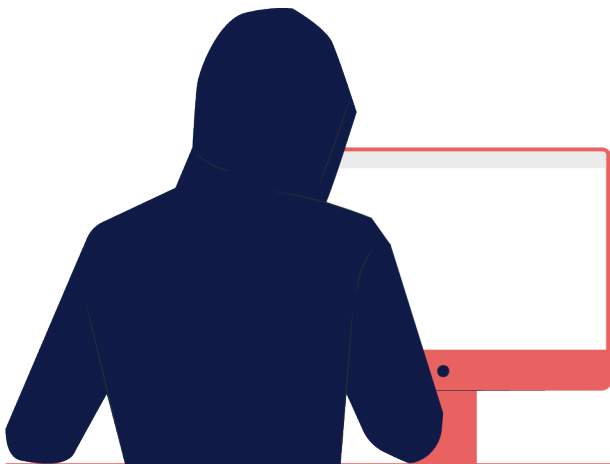


Impersonation and identity theft

Research by the National University of Australia revealed that women are 50% more likely than men to be victims of identity theft¹⁹.



It is a malicious activity consisting of **pretending to be someone else online by using their personal data for the purpose of threatening or intimidating them** (Women's Media Center, 2019). This can be done by creating fake profiles or accounts on social media or usurping email accounts or phone numbers that can be used to contact the friends, relatives, coworkers, or acquaintances of the victims for the purpose of contacting them and gaining access to information about them (APC, 2017; Barrera, 2017).



The case of the cyber attacker of a whole family

In a well-known case in Chile, a foreign online aggressor harassed an entire family and their circle of friends (at least 50 persons) for 13 years, stealing personal information and impersonating them, including the theft of passwords, emails, and social media profiles, as well as personal photos to send obscene messages and postings on porn sites on a large scale. The assailant, suspected to be the former dating partner of one of the members of the family, carried out many acts of cyber violence against every person related to the original victim and her family or who had any contact with her (Paz Peña, 2017).

In cases of domestic violence, it is frequent to see impersonation and identify theft via different mechanisms, such as the use of personal data for the unlawful use of their credit cards or control over their assets, to control communications they engage in with other persons or to pretend to be relatives or friends on social media to monitor them via those profiles.

¹⁹ 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



Acts that harm the reputation or credibility of a person



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*²⁰, 15% of the victims interviewed indicated having been affected by the dissemination of false, manipulated or out of context information.

They consist of **creating and sharing fake personal information with the intent to undermine the reputation of a person**, such as creating false profiles on social media or online accounts; engaging in a photo montage or edited images involving sexual content based on photos obtained on social media; posting notices on dating or porn websites with intimate images; disseminating offensive or fake comments or postings or memes in discussion forums, social media, or websites (including acts of vandalism in Wikipedia); and engaging in acts of slander and manipulation (APC, 2017; Barrera, 2017).



What is slutshaming?

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

Camila Zuluaga Case

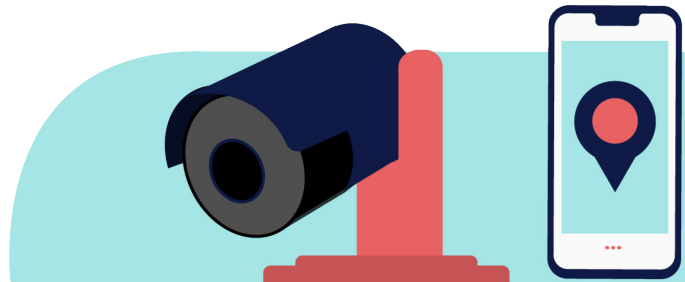
Many different civil society organizations have documented a rise, throughout the region, in online acts aimed at undermining the reputation and credibility of women journalists, politicians, and human rights defenders (Peña, 2017; Luchadoras, 2017; Cuellar and Chaheer, 2020). In one case in Colombia, the journalist Camila Zuluaga was attacked in September 2019 by a coordinated massive campaign after the portal *Los Irreverentes* posted, without providing any evidence whatsoever, that she had received 35 million pesos from a person involved in a corruption scandal. The attacks focused on the tags #CamilaEstásPillada [#CamilaCaughtRedHanded] and #CamilitaEstásPillada [CamilitaCaughtRedHanded], which achieved up to 10,000 mentions in a single day. Investigations found evidence of automation in these coordinated attacks and the operation of a WhatsApp forum which gave instructions to conduct the attacks in order to discredit her work as a reporter (Cuellar and Chaheer, 2020).

²⁰ UNESCO and the International Center for Journalists (ICFJ) (2021). Online Violence: The New Line of Battle for Women Journalists - #JournalistsToo. Available in: https://unesdoc.unesco.org/ark:/48223/pf0000375136_spa; Carlos Guerrero and Miguel Morachimo (2018). Know to resist. Online Gender Violence in Peru. Available in: https://hiperderecho.org/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 cases of domestic or intimate violence, the partner or former partner has used some kind of spyware or geolocation equipment installed in the computers or cellphones of the women targeted (Women's Aid, 2014).



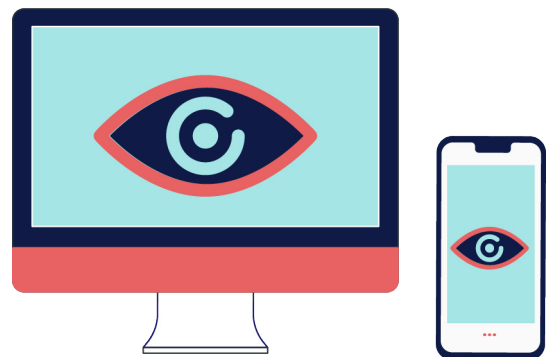
Constant monitoring and surveillance of the **activities of a person online and offline** or their location constitute a form of violence (APC, 2017).

- Using spyware installed in the cellphone of the victim to monitor her secretly or steal her information.
- Also using geolocation devices in cars or handbags, toys, surveillance cameras, virtual assistants, or connected smart devices.



What is spyware?

It is a type of malware installed in a person's device to record everything that person does, including text messages, emails, photos, or even all of the keys struck on a keyboard. With certain types of malware, aggressors can remotely turn on the camera or microphone of a cellphone to track the victim's location, monitor use of applications, or intercept calls.





Online stalking



Various studies on the subject have shown that online stalking is an online criminal offense with a heavy gender connotation and that women and girls are the most likely ones to be victims of this form of violence (Reyns, Henson, and Fisher, 2011).

At present, there is no single definition for online stalking, because it encompasses a wide range of online abuse. As a rule, it can be defined as an **intentional and recurring activity** using computers, cellphones, and other electronic devices, which separately may or may not consist of inoffensive acts in themselves but which, together, constitute a **pattern of threatening behaviors that undermine a person's sense of safety** and trigger fear, anxiety, or alarm (EIGE, 2017: 4; PRC, 2018; Maras, 2016). This activity can be turned against the victim's relatives, friends, or intimate partner.

In contrast to online harassment, online stalking entails a pattern and the perpetration of **more than one incident over time using ICTs**, for the purpose of repeatedly intimidating, stalking, pestering, attacking, humiliating, threatening, frightening, or offending a person or verbally abusing that person (UNODC, 2015). It may consist of emails, phone calls, text messages, online chat, or the constant sending of obscene, vulgar, slanderous, or threatening comments via the Internet. Some of the behaviors include the following:



Spying on, obsessing, or gathering information online about someone and attempting to communicate with that person without her consent; constantly sending requests for friendship on social media; joining all the online groups she belongs to; following up on the notes posted by the victim on social media via acquaintances they have in common or coworkers, friends, or relatives; or constantly looking at her profile so that she will notice it (UNODC, 2019).



Calling or sending emails, text or voice messages repeatedly, including threatening messages or messages attempting to control the victim.



Making unwanted and repeated propositions of a sexual nature, sending unsolicited sex photos (photos of the male genitalia of the aggressors), or constantly monitoring or watching a person's location and daily activities and communications (Henry and Powell, 2016).



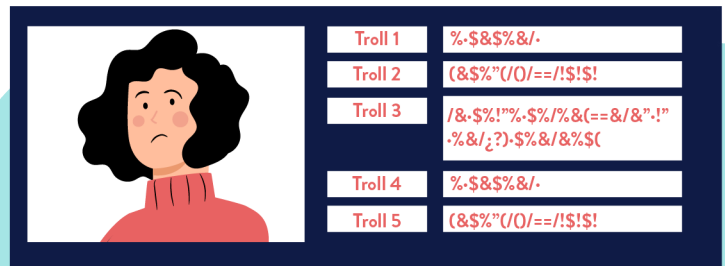
Constantly posting fake, malicious, or offensive information about a person on that person's web pages, blogs, or social media.

Perpetrators of online stalking may be intimate or sexual partners, former partners, acquaintances, friends, relatives, or strangers. It is also important to highlight that **this tactic is especially frequent in contexts of domestic or partner violence.**



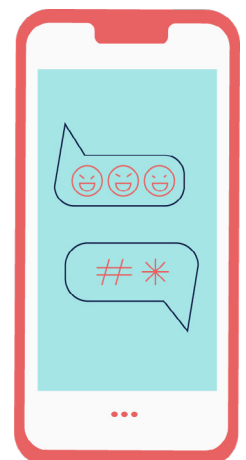
Online harassment

In a study published in 2018 by Amnesty International, it was indicated that 23% of women surveyed had experienced some type of abuse or harassment on social media at least once (AI, 2018).



Online harassment involves the **intentional use of ICTs to humiliate, molest, attack, threaten, alarm, offend, or insult a person** (Maras, 2016). In contrast to online stalking, where there is a pattern of threatening behaviors, in the case of online harassment a single incident is enough to identify the behavior, although it can also involve more than one incident (UNODC, 2019).

Online harassment **may appear under many different manifestations and be coupled with other forms of online violence.** For example, it can include sending unwanted or intimidating messages by email or on social media, inappropriate or offensive insinuations on social media or in chat rooms; verbal violence or online threats of physical violence or death threats; hate speech; theft or posting of personal information, images, and videos; and the dissemination of fake information or rumors to undermine a person's reputation (EIGE, 2017; APC, 2017, UNODC, 2019).

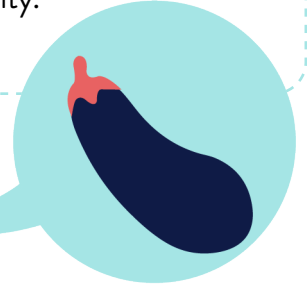




What is hate speech?

It is the use of language to disparage, insult, threaten, or attack a person because of their identity and other characteristics, such as their sexual orientation or disability.

Online harassment can also include the disclosure of the victim's personal information (doxing) with invitations to rape her, promoting situations of revictimization in which harassers and aggressors go to the home of the woman being targeted.

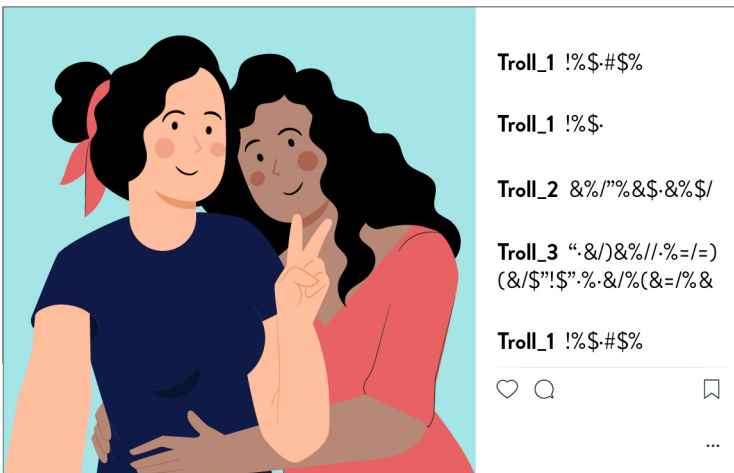


Did you know that?

Various studies reveal that women are more than twice as likely to be the target of online sexual harassment than men (Reid, 2016).

Online harassment, which disproportionately affects women throughout the world, has sexual connotations (Li, 2006; Henry y Powell, 2017, p. 212). It may entail threats of rape, femicide, sexualized physical violence, or the instigation to engage in physical and sexual violence against the victim or her relatives, and sexist or offensive verbal attacks on the gender status or physical appearance of women. It includes sending unwanted sexually explicit materials, contents that dehumanize women and present them as sexual objects or misogynist, explicitly sexual, and abusive comments (Jane, 2016).

A common form of online harassment is cyberflashing, or the sending of obscene photos of a woman without her consent (for example, photos of the harasser's genitalia) for the purpose of pestering, intimidating, or unsettling her.

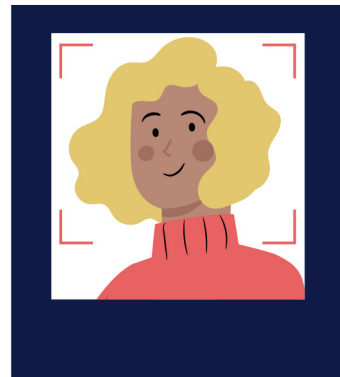


The perpetrators of online harassment may be trolls, who publish extremely offensive and virulent comments to trigger an emotional reaction and response from other Internet browsers. This behavior is called trolling (Maras, 2016).

Gender trolling involves the posting of messages, images, or videos, as well as the creation of hashtags, for the purpose of pestering women and girls or instigating violence against them (UN-SRVAV, 2018; Mantilla, 2013).

Online harassment may also involve a group, when there are two or more persons organizing and coordinating the recurring online harassment of a person, oftentimes harassment that is sustained over a long period of time and based on a strategy. These groups can be comprised of members of online communities, forums, or sites (such as Reddit or 4chan), where certain types of especially violent masculinities have been found (Jane, 2017).

In Latin America group attacks coordinated by networks of trolls and hackers, such as “Legión Holk” (originally established in Colombia and Peru) and “Secta 100tifika,” are proliferating. They engage in mass attacks and harassment in order to trigger confrontation and controversy, creating trends and promoting discrimination, racism, and misogyny. These groups are accustomed to attacking women who are active on social media, who have a public profile, or who are feminists. It is common for them to disseminate sexualized photo montages, to impersonate their victims on social media for the purpose of discrediting them, and circulating degrading contents (Peña, 2017; Barrera, 2017).



Some of these attacks have become disproportionate, turning into cybermobs, which are made up of groups organized online to massively engage in posting offensive or destructive contents with the intention of shaming someone or forcing the victim to remove her profile from social media (Citron, 2014).

Ana Gabriela Guevara Case

In Mexico a flagship case of coordinated attacks involved the former sportswoman and senator Ana Gabriela Guevara, who in December 2016, after having publicly disclosed on social media the physical aggression she was exposed to in the street, was attacked by organized groups of trolls and hackers who created viral hashtags using fake accounts and referring to gender-based violence. The hashtags included #MujerGolpeadaEsMujerFeliz [#BeatenWomanIsHappyWoman] and #GolpearMujerEsFelicidad [#HittingWomanIsHappiness], which became trending topics in many Spanish-speaking countries (Peña Ochoa, 2017; Barrera, 2017).



Ciberbullying



According to a worldwide investigation carried out by IPSOS²¹ in 2018, 1 in 5 parents indicated that their daughter / daughter had been a victim of cyberbullying. It was also identified that Peru, Argentina and Mexico were the countries with the highest levels of cyberbullying in social networks.

Cyberbullying involves the use of technologies by minors to humiliate, pester, alarm, insult, or attack another under-age girl or boy or to disseminate fake information or rumors about the victims, as well as to threaten, isolate, exclude, or marginalize them (Maras, 2016; Hinduja and Patchin, 2014; UNODC, 2015).

It can be carried out via text messages, emails, virtual surveys, blogs, social media postings, online videogames, or virtual reality websites and they can lead to very serious harm to the emotional and physical health of the persons under attack, who may eventually self-harm or commit suicide.

In most countries, it is deemed that, **in cases of cyberbullying, boys and girls are responsible for and victims of this form of violence** (Duggan et al., 2015). In others, such as Australia and New Zealand, cyberbullying may involve adults.



Did you know that?

There is a broad range of views about whether or not the gender of a person 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). Without detriment to the above, what is indeed clear is that the harm and consequences sustained by girls and boys are different depending on the gender-based stereotypes they encounter: girls who are victims of cyberbullying, however, are usually attacked with offensive and violent comments about their bodies and sexuality.

²¹ 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



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*²², 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 sending or posting communications or contents (voice or written messages, images, videos) using technologies to express the **intent to do physical harm** or engage in sexual violence (APC, 2017; Barrera, 2017).

It includes online extortion, which occurs when a person exerts pressure on another to force her to act in a certain way under threat, intimidation, or aggression, for the purpose of bending her will or controlling her emotionally. It can take the form of sexual blackmail, involving threats of online posting or sending private, sexual, or intimate information to persons unknown to the victim.



What is sextorsion?



Sextorsion consists of threatening a person to release intimate pictures or videos of the victim to secure additional explicit material on sexual acts, to engage in sex with them, or to extort money from them (UN-SRVAW, 2018, para. 32). This form of violence disproportionately affects women and, with few exceptions, it is generally perpetrated by persons identifying themselves as men (Kelley, 2019).

This form of violence has grown exponentially over the past few years and can be conducted in many different ways, ranging from hackers who send emails demanding money in exchange for not releasing intimate pictures or images supposedly taken remotely by enabling the camera of a device to intimate partners or former partners engaging in sextorsion for their own sexual gratification. A 2018 report from the FBI Center for Complaints on Cybercrimes pointed out that there had been a 242% rise in emails containing threats of extortion, most of which were acts of sextorsion (FBI-ICC, 2018).

²² Amnesty International published the research *Green Hearts: Online Violence Against Women during the debate on abortion legislation in Argentina*. Available at: https://amnistia.org.ar/corazonesverdes/files/2019/11/corazones_verdes_violencia_online.pdf

#GamerGate Case

One of the first massive online campaigns attacking women of the videogame industry was launched in 2014. It was called #GamerGate²³ and targeted the developers Zoe Quinn and Brianna Wu and the communicator Anita Sarkeesian, among several others, after they made statements against sexism and gender inequality in videogames. The participants of #GamerGate voiced their opposition to the influence of feminism in the videogame culture and organized themselves using online platforms such as 4chan, Twitter, and Reddit to coordinate large-scale attacks that included acts of online harassment, doxxing, and rape and death threats. The three women reported the doxxing attacks, including threats, which reached such a magnitude that they were forced to flee from their homes. The attacks against Anita Sarkeesian in particular were so egregiously aggressive that they included bomb threats when she was nominated to receive a prize in San Francisco and terrorist threats when she announced she would attend a conference at the University of Utah.



ICT-facilitated physical violence



In the UNESCO and ICFJ research entitled *Online Violence: The New Line of Battle for Women Journalists - # JournalistsToo*²⁴ it was documented that 20% of surveyed women had been attacked offline in connection with the violence they experienced online.

This form of violence includes a range of manifestations, such as ICT-organized or planned sexual attacks or sexual violence based on the online posting of the victim's personal data after she has been located (doxxing).

It can also appear when an aggressor engages in an online friendship with a person to become acquainted with her and then abuse her sexually (as may occur with dating applications) or when an aggressor requires a person to engage in sexual relations under threat of releasing intimate or sexual information (sextortion) (Henry and Powell, 2018).

²³ Eliana Dockterman (2014). "What is #GamerGate and why are women being threatened about video games?" *Time*. Available at: <https://time.com/3510381/gamergate-faq/>

²⁴ 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



Abuse, exploitation, and/or trafficking in women and girls using ICTs

Certain surveys indicate that new technologies are facilitating human trafficking worldwide (in which women account for 80% of the victims and 95% of the cases of sexual exploitation) with a new digital modus operandi, using the Internet to recruit, sell, advertise, and exploit women and girls (Van Der Wilk, 2018).



This form of online violence entails the intermediation of technologies to wield power over a person on the basis of the sexual exploitation of her image or body against her will (Barrera, 2017). Behaviors included in this form of violence are as follows:

- Use of technologies to screen and recruit women and girls for the purpose of sexual abuse or trafficking, compelling them to accept situations of trafficking or sexual abuse, exercising power and control over them and preventing them from leaving the abuse, including threats of disclosing private information (UN-SRVAW, 2018, para. 32).
- Child grooming, or online sexual grooming of children, in other words deliberate actions taken by an adult to approach a minor (eventually building a sentimental connection) for the purpose of engaging in a relationship and exerting emotional control over the victim, making it possible for sexual abuse to be perpetrated, for virtual relationships to be initiated, child pornography to be obtained, and trafficking in the minor to be carried out (Women's Media Center, 2019).
- Posting of sexual images without the consent of the person for marketing and prostitution activities.



Attacks against women's groups, organizations, or communities



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

They consist of intentional acts to censor and harm women's organizations, including attacks on their media channels (Barrera, 2018), such as gaining access to them without their consent and hacking webpages on the Internet, social media, or email accounts to undermine the performance of their duties, making sure they shut down their organization's profile or remove it from social media by using community standards to report contents the platform deems to be sensitive, distributed denial-of-services attacks (DDoS)²⁵, restrictions on the use of the domain or theft of domain, and Internet blackouts during a meeting or protest march (APC, 2017).

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



Cases of attacks on feminist groups

In Latin America, there have many attacks against websites, profiles, or accounts of feminist groups or women human rights defenders to block or shut down their online contents either temporarily or permanently. Cases have been reported, such as the one of the Mexican feminist collective Las Hijas de la Violencia (Daughters of Violence) and the Colombian feminist organization Mujeres Insumisas (Dissident Women), as well as the constant coordinated attacks against activists and groups of black feminist and transfeminist women in Brazil (Lyons et al., 2016; Peña, 2017).

²⁵ An online attack consists of enlisting persons to send a huge number of requests to a website's server in order to flood it and thus make it inaccessible.

Part three

PREVENTING AND COMBATING ONLINE VIOLENCE AGAINST WOMEN:

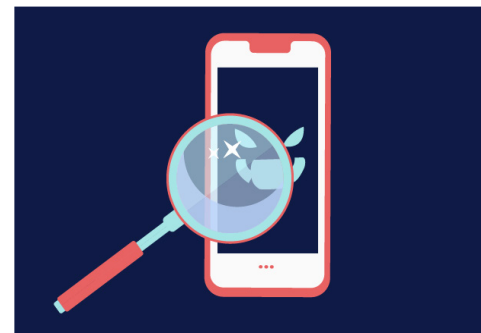
The perspective of institutions





Interventions to combat online violence against women and girls

Measures to prevent, address, investigate, and punish ICT-facilitated acts of violence against women have been the focus of growing attention in countries and globally. As the extent of the phenomenon and its serious impacts on women and girls have become increasingly apparent, many sectors have turned to finding measures that would make it possible to tackle the threats to women's safety and integrity that have come with rapid changes in technology.



Certain initial studies and testimonies by victims and survivors have made it possible to find common elements that are no doubt a valuable guide for institutional capacity building. For example, the widespread absence of information about the characteristics of ICT-facilitated gender-based violence and the digital security practices that women could implement to protect themselves has been documented. In many countries, support services for victims are missing and authorities from all levels continue to be in dire need of training so they can provide adequate orientation in the matter. Likewise domestic statutory frameworks hampering women who sustain this form of violence from having access to justice are still in force (Barrera, 2017; APC, 2017; Peña Ochoa, 2017; Van Der Wilk, 2018).



It has also been proven that, oftentimes, institutions in charge of enforcing the law trivialize online violence against women and blame the victims (more than the aggressors), which has led to a culture of silence in which survivors prefer not to report acts of violence to authorities because of the risk of being ignored or revictimized (Abdul, 2017, p. 7; UN-SRVAW, 2018, para. 68).

In her 2018 report on online violence, the United Nations Special Rapporteur on violence against women took up several proposals made by the Internet Governance Forum regarding state measures to address this phenomenon. She underscored the obligations of states to ensure that both state and non-state agents refrain from engaging in online acts of violence against women, as well as to use due diligence in order to prevent, investigate, and punish these acts (UN-SRVAW, 2018, para. 62). Among the measures pointed out by the Special Rapporteur, the following are included:

- ✓ Apply a gender perspective to all forms of online violence.
- ✓ Take measures to raise awareness about the fact that online violence is a form of violence against women, a form of discrimination, and a human rights violation.
- ✓ Gather and publish sex-disaggregated data on access to the Internet, the prevalence of online violence against women, and the harm it causes.
- ✓ Provide rapid, adequate, and accessible assistance services to women affected by this form of violence, including the establishment of hotlines for providing help and specialized service units, as well as widely disseminating information on these services so that women are aware of their existence.
- ✓ Provide victims with appropriate legal aid.
- ✓ Establish legal mechanisms that make it possible to investigate and punish acts of online violence against women with due diligence, in addition to offering the possibility of requesting protective orders for the victims.
- ✓ Adopt effective measures to prevent the posting of contents that are harmful on the grounds of gender and to prevent their dissemination.
- ✓ Promote technical knowledge of authorities in charge of administering and imparting justice.
- ✓ Adopt clear and specialized intervention models, protocols, and codes of conduct so that civil servants can provide a timely response to this form of violence.
- ✓ Combat the culture of impunity regarding the perpetrators, with the enforcement of penalties that are adequate, necessary, and proportional to the criminal offense.
- ✓ Grant reparations to the victims of online violence in proportion to the seriousness of the harm sustained, financial compensation to defray the costs incurred by material and moral damages, and measures of redress, rehabilitation, and satisfaction, as well as guarantees of non-repetition.
- ✓ Establish a comprehensive legal framework to combat and prevent ICT-facilitated violence against women so that its perpetrators can be brought to justice.
- ✓ Take measures to eliminate all forms of gender inequality in terms of access to technologies and to promote digital literacy.



By the same token, interviews of survivors of ICT-facilitated domestic violence and staff specializing in providing services to address violence against women have provided guidelines for other measures that could be adopted in this area, among which the following (Dragiewicz, 2019):

- ✓ Educate and raise awareness of authorities and first responders on the characteristics and impacts of this violence.
- ✓ Provide adequate training to the police about securing evidence of online violence against women and give survivors guidance for adopting digital security measures.
- ✓ Recognize the digital divide affecting many of the victims of domestic violence and address the problem.
- ✓ Mainstream training in ICT-facilitated violence against women into university curriculums for degrees in law, psychology, and social services.
- ✓ Facilitate the work of experts in technology and security so they can provide advisory services and assistance in care centers and shelters for survivors of violence (for example, with the analysis of potential threats to digital integrity for women who go to these centers).

Undoubtedly, in view of the newness of the phenomenon, there is still much to learn about the reality being encountered daily by victims of online gender-based violence, and surely new and updated schemes shall emerge as women call for justice and further knowledge becomes available on the links between gender-based violence and new technologies.

Furthermore, the contributions and participation of national authorities shall be required, in addition to those of Internet providers, representatives of victims, civil society, the academic sector, and all stakeholders who are involved both in the governance of the Internet and in the drafting of national and regional cybersecurity policies and local strategies to eradicate violence against women.



In this common context of learning and collaborative work, bearing in mind the momentum behind this issue and the need to tackle it adequately, there are **certain elements that are important to consider in the thinking already focusing on online gender-based violence against women**, as well as on how to promote them in the future.

First of all, online violence against women, as part of a continuum of multiple, interrelated, and recurring forms of gender-based violence, **is a complex problem with many causes and dimensions**, along with social roots that go beyond the mere intermediation of technology and for which there is no one-size-fits-all solution, but which rather **requires a multidisciplinary approach and the participation of diverse sectors**.

Second, on the basis of national experiences in applying models of intervention to combat offline gender-based violence, it is important **to adopt a comprehensive and holistic vision that takes into consideration the individual, families, communities, and society, as well as the global impacts** that gender-based violence has on the effective access of women to new technologies and, as a result, to develop a fairer and more egalitarian Internet that can be for the benefit of all societies.

Third, as already reasserted internationally, it is essential to keep in mind that **the human rights of women must be protected both online and offline** and, in particular, to recognize the role that women's right to have access to the Internet on an equal footing and without discrimination plays in the digital revolution.

Finally, it will be crucial to work with a mindset promoting **the digital empowerment of women and their online security**, tackling this task from the standpoint of vision that fosters their digital autonomy, acknowledges their diversity, and challenges the models that treat women as helpless victims of online aggression and cybercrimes, denying them their basic right to security and the freedom to navigate the digital world.

Without doubt, empowering women and girls of all ages so they can dismantle the barriers that keep them away from technology and so they can develop strategic thinking about their digital security requires a comprehensive strategy channeling collective efforts in the near future. This has been precisely the premise used to structure the present guide and on the basis of which it is hoped further interventions shall be promoted in this area.



What is being done in the countries of Latin America and the Caribbean?

Over the past few years, several countries of Latin America and the Caribbean have gradually recognized the issue of online violence against women and have updated their statutory framework to tackle it, including the enactment of specific laws on online stalking, online harassment, online grooming, and cyberbullying.



In particular, throughout the hemisphere of the Americas, to a large extent because of the media's spotlight on the issue and the calls made by public opinion, important legislative breakthroughs have been made with respect to the nonconsensual dissemination of intimate or sexually explicit images (Neris et al., 2018).

In Paraguay, Law 19.580 passed in 2017 recognized telematic violence, understood to mean the ICT-facilitated dissemination or posting of audiovisual materials undermining the dignity or intimacy of women. In December 2018, Brazil enacted Law 13.772/2018 to penalize the unauthorized recording and storage and exhibition of nude or sexual contents. According to the law, cases of domestic violence are those in which there had been a preexisting relationship between the victim and the perpetrator. It also has Law 13.718/18, which classifies the dissemination of images of rape as a criminal offense.

By means of Legislative Decree No. 1410 of September 2018, Peru incorporated into its Criminal Code the crimes of ICT-facilitated harassment, sexual harassment, sex blackmail, and dissemination of images, audiovisual or audio materials with sexual contents. As for Chile, in 2019 it adopted Law 21.153 criminalizing the unauthorized dissemination of intimate materials or images recorded in public spaces without consent. In October 2020, Nicaragua adopted the Law on Cybercrimes, which punishes threats and harassment via new technologies, such as the dissemination of explicit sexual material.

In Mexico, 28 local lawmaking bodies have already adopted a total of 35 legislative reforms criminalizing the nonconsensual dissemination of intimate images. At the federal level, in April 2021, a series of legislative reforms of the Federal Criminal Code and the General Law on Women’s Access to a Life without Violence have been adopted, recognizing online violence and classifying the violation of the sexual intimacy of persons via the nonconsensual dissemination of intimate sexual materials as a criminal offense. This series of reforms has been called the “Olimpia Law” because of the work done to recognize this form of online violence by Olimpia Melo Cruz, who in 2014 was the victim of the unauthorized dissemination of a sex video²⁶.

In Argentina, the Commission to Amend the New Criminal Code proposed including the nonconsensual broadcasting and recording of sexual contents as a computer crime, a conduct which until then had only been penalized when involving minors. The Criminal Code of Buenos Aires has already incorporated the nonconsensual dissemination of intimate images or recordings and online stalking as a criminal offense.

Other bills of law are being discussed in Bolivia, Ecuador, and Chile in connection with this form of violence.

Over the past few years, progress has been seen in various countries with the establishment of police units specializing in cybercrimes that can investigate acts of online violence against women. The **Federal Police of Mexico** has a Forensic Division investigating national cybercrimes and tackling cases of online violence. The Office of the Attorney General of Mexico City recently established the Gender-Based Cybercrime Services Unit²⁷, in addition to an online government portal to raise awareness about online harassment. There are also specialized units in the **National Police of Colombia**, which has a Police Center for Cybernetics, and in **Brazil**, there is an **Office for the Suppression of Cybercrimes in the Federal Police** (in addition to specialized police departments in some of the states). **Argentina** has a **Technological Crimes Division in the Federal Police**; **Bolivia** has an **Agency for the Development of the Information Society**, which is the principal body for managing security matters; and **Paraguay** has a **Specialized Computer Crimes Unit**. Finally, the **Ministry of Women and Vulnerable Populations of Peru** has a digital platform on which online harassment incidents can be reported²⁸.



²⁶ OLegal system. *Ficha Técnica Ley Olimpia* [Fact Sheet on the Olimpia Law]. Available at: <http://ordenjuridico.gob.mx/violenciagenero/LEY%20OLIMPIA.pdf>

²⁷ Alejandra Balandrán Olmedo (2020). “Atenderá FGJCDMX ciberdelitos de violencia de género” [FGJCDMX shall tackle crimes of online gender-based violence]. *Diario ContraRéplica*. Available at: <https://www.contrareplica.mx/nota-Atendera-FGJCDMX-ciberdelitos-de-violencia-de-genero202028854>

²⁸ Ministry of Women and Vulnerable Populations. *Ponte alerta ante el acoso virtual* [Be alert to online harassment]. Available at: <http://www.noalacosovirtual.pe/alerta.html>

Part *four*

Manual on Self-Protection and Response:

DIGITAL SECURITY TOOLS

TO COPE WITH ONLINE GENDER-BASED VIOLENCE





Basic digital security recommendations: preventive measures



Taking measures to reinforce digital security is the first line of defense against online threats, attacks, and acts of violence. Of course, not all women have the same priorities or are being threatened the same way, and measures may vary depending on the case. It is important to recall that cybersecurity is a personal process that can be undertaken at one's own pace and that it can be achieved with a bit of patience and appropriate planning.

Key recommendations are provided below to safely navigate and control digital interactions, as well as additional resources to learn more about the subject. All of this information can be overwhelming when read for the first time. Nevertheless, **the present manual strives to demystify the process of cybersecurity capacity building for women.** It is important to recall that these recommendations can be put into practice gradually and, along the way, digital security capacity building will prove to be much easier than it might at first seem.

It is important to underscore that the provision of the following resources does not in any way entail an endorsement, by the OAS or its member states, of their content or the organizations identified. The resources are presented as examples of organizations, guidelines, tools, etc., which are available in the region so that readers examining them can broaden their information about the issue being addressed by the present publication.

01 Using safe passwords as protection against hacking or theft of identity

Using strong and safe passwords is crucial to protecting online information, as they are the gateway to our accounts and, as a result, to the details of our personal life.





Choosing passwords that, for us, are personal and easy to remember is a widespread practice (for example, 12345), but this puts us at risk, because an acquaintance or hacker would have no trouble guessing them. For effective protection, **unique passwords must be used; in other words, the same or very similar passwords must not be used** for one's many different webpages and accounts (by simply adding, for example, a "1" or recycling the same password). If possible, one should use a different username for each account (for example, one unique password and username for the email account, different ones for the bank account, yet others for social media, etc.).



Changing passwords constantly (preferably every 90 days), especially those for the most confidential accounts. Above all, passwords must be changed if a legitimate and verifiable email is received (making sure beforehand it does not involve any attempt at *phishing*) informing that the account of a service has been compromised.



Creating complex passwords. For effective protection, passwords must be long, unique, random, and difficult to guess, and they must include a combination of at least 12 uppercase and lowercase letters, numbers, and symbols. In the following site, Digital Self-Protection against Surveillance (*Autoprotección Digital contra la Vigilancia*), a guide can be consulted for creating safe passwords: [guía para crear contraseñas seguras](#)²⁹.



Activate **two-factor authentication**³⁰ of the email account and social media accounts. This option requests the user to identify herself using a combination of two methods of authentication; in other words, it requests a password and one-time verification code sent via SMS text message or generated by a dedicated application, which must be inserted in order to enter the account from a new or unregistered computer, phone, or browser. For further information on [two-factor authentication \(2FA\)](#) please consult the website of the Electronic Frontier Foundation (EFF)³¹, as well as directly on [Facebook](#)³², [Instagram](#)³³, [Twitter](#)³⁴, [Gmail](#)³⁵ and [Apple](#)³⁶.



For greater ease, using an **automatic generator or manager of online passwords**, which creates random and safe passwords for each account, is recommended. If that option is chosen, the only thing that has to be recalled is the master password to unblock the others. Examples of managers are as follows: [1Password](#), [LastPass](#), [Password Generator](#) and [KeepPassXC](#)³⁷. For further information, a [video](#) can be consulted at the website of *Surveillance Self-Defense*³⁸.

²⁹ Surveillance Self-Defense. *Creating Strong Passwords*. Available at: <https://ssd.eff.org/es/node/23/>

³⁰ Available at: <https://twofactorauth.org/>; <https://ssd.eff.org/es/module/c%C3%B3mo-habilitar-la-autenticaci%C3%B3n-de-dos-factores>

³¹ 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>

³² Facebook. *What's two-step authentication and how does it work on Facebook?* Available at: <https://www.facebook.com/help/148233965247823>

³³ Instagram. *Keeping Instagram Safe*. Available at: <https://help.instagram.com/1372599552763476>


³⁴ Twitter. *How to use two-factor authentication*. Available at: <https://help.twitter.com/es/managing-your-account/two-factor-authentication>

³⁵ Google. *Two-factor authentication*. Available at <https://www.google.com/intl/es-419/landing/2step/>

³⁶ Apple. *Two-factor authentication for Apple ID*. Available at: <https://support.apple.com/es-es/HT204915>

³⁷ Available at: <https://1password.com/>; <https://www.lastpass.com/es/>; <https://passwordsgenerator.net/>; and <https://keepassxc.org/>

³⁸ Surveillance Self-Defense. *Animated Overview: Using Password Managers to Stay Safe Online*. Available at: <https://ssd.eff.org/es/node/85/>

 **Using security questions** on the websites offering this option, but without providing answers with real information (for example, the name of a pet or the street of one's home address). The answers must be difficult to guess and must not contain any data that could be found on the Internet or social media (grandmother's last name, for example). It is also possible to save the answers in a password manager.

 **Never sharing passwords via a connection that is not secure**, such as text messages or SMS.

 **Never saving passwords in the setting of the browser, in the cloud³⁹**, or in an unsafe document on the computer or phone, because they are easy to find if the device is hacked. They can be saved in an encrypted document in a secure physical device or jotted down and kept in a place where any trace of them can be easily eliminated. Further information can be obtained on file encryption for [Windows](#) on Microsoft's website or the website of [Apple](#) for the iOS operating system⁴⁰.

To learn more about strengthening passwords, the OAS publication [Media Literacy and Digital Security](#) and Twitter can also be consulted⁴¹.

Using different email addresses

A useful security measure involves **having different emails for each one of our accounts** on the Internet and for diverse purposes; for example, one for personal communication, another for work, another for the public profile, another for social media, another for online games, and yet another for receiving promotions. That is how to prevent someone who has managed to enter into one of the accounts from automatically gaining access to the others.



³⁹ The cloud is a data storage system, such as Google Drive, Dropbox, or iCloud, which is not in personal devices.

⁴⁰ 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>

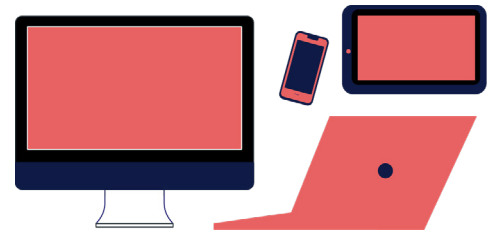
⁴¹ Organization of American States (OAS) and Twitter (2019). *Media Literacy and Digital Security: Best Twitter Practices*. Available at: <https://www.oas.org/es/sms/cicte/docs/alfabetizacion-y-seguridad-digital.pdf>



Reminder: Basic precautions when navigating
Precaution is the best online weapon.



- Always delete emails, postings, or message that seem suspicious.
- Only connect via reliable WiFi networks. If connecting to a public network, restrict the information you are sending or consulting.
- Use a virtual private network (VPN)⁴², which is a network technology that protects you from cyberattacks when the Internet connection is via a public WiFi network, because it makes it difficult for third parties to steal confidential information. It is possible [to download a free or paid VPN](#), as it is a relatively simple process as explained in this [video](#).
- Always browse in a secure mode making sure that the website begins with https:// (and not http://); that means that the information being carried is encrypted.
- When unknown devices are being used, always navigate privately or incognito to prevent your passwords from being registered.
- Download applications only from official websites to make sure they are safe.

03 Protecting electronic devices (desktop computer, laptop, cellphone, or tablet)




What is malware ?


It is a malicious software that carries out unwanted actions in devices in order to infiltrate and damage a computer or information system.


- 
Do not forget to update the software on your devices. Updating software regularly not only helps to make the device faster, but also provides greater security, as it can provide further protection against threats and solve the vulnerabilities of previous versions.
- 
Use an antivirus program. Although antiviruses cannot detect all malware, they do provide extra layers of protection to your devices. There is a wide range of antiviruses on the market, and you can choose the one that is most in line with your needs. In the website *Reason Security* it is possible to consult certain recommendations to choose an antivirus for your computer⁴³.

⁴² 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/>


⁴³ Reason security. Which antivirus is best for laptops? Available at: <https://blog.reasonsecurity.com/2020/01/12/which-antivirus-is-best-for-laptops/>

 **Check the applications (*apps*).** In order to reinforce the security of your devices, check the applications that are installed in your cellphone (they can be found in the menu of settings). If you find an *app* that is not being used or that you are not familiar with, look on the Internet to learn about its purpose. If you cannot recognize it or it does not belong to the cellphone's operating system, it is preferable to remove it for greater security. In the following links, you can find out how to delete applications in [Android](#) and [Apple](#)⁴⁴.

 **Protection from malware (malicious software).** Attackers may try to gain access to the device to extract information or spy using phishing attacks, in other words installing disguised programs in attachments to emails or message that may seem innocent, but which actually contain malware. These programs can enable the device's microphone or camera, transmit conversations, see what is being written, copy files or messages, monitor movements, or steal passwords. The best strategy to prevent this is **to always be cautious when receiving an email from an unknown sender**, to examine the sender of the file, and to **never open the files attached to these emails from unknown sources**. Do not click on unreliable links or download files with those features.

 **What does encoding or encrypting an information mean?**

It means concealing it in plain sight in order to make it more secure and confidential. It is a process to convert digital data into codes which renders the information illegible except for the person who has the key to decipher it. Devices, files, data, text messages, and any type of information that requires it can be encrypted.

 **Protecting cellphones.** Cellphones are like open windows onto our lives. In them can be found and intertwined a large part of our personal information and social interactions. In addition, they are usually synchronized with other devices. Because of that, it is important to take certain basic measures to protect this instrument which is so closely related to our online and offline lives:

- Put a **blocking password** in the phone so that it cannot be used without inserting a code (preferably a combination of words and numbers) in the case of theft or loss.



 **What is *phishing*?**

It is a technique whereby attempts are made to secure confidential information using fraud (passwords, bank information, etc.) via a misleading electronic communication (email, text message, etc.). As a rule it involves impersonating a person or company so that the persons receiving the communication will hand over private data. These messages can also infect the device with a computer spy program to monitor or rob information.

⁴⁴ 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>

- Make sure not to keep sensitive information on the phone and whenever necessary use the function to encrypt or encode the information. In the following links instructions are included to encrypt data on [Apple devices](#) and [Android devices](#)⁴⁵. Access to applications can also be blocked to protect information and interactions in them with applications such as [Smart App Lock](#)⁴⁶.
- If sensitive information has to be deleted, it is important to remember that it is not enough to merely delete it from the cellphone, because oftentimes that **information may have been uploaded automatically to the cloud, and therefore it must also be deleted there**. Android does not automatically upload information to the cloud, but Apple devices do; therefore that option has to be disabled manually. The guide for [disabling automatic synchronization with iCloud](#) can be consulted in this Apple help center⁴⁷.
- **Check which applications are installed in your cellphone.** If one turns out to be unfamiliar or seems suspicious, look on the Internet for information about its characteristics and, if you do not need it, then disable and remove it. Applications that are not being used should also be disabled and removed, as they may become a source of vulnerability. Keeping only what is necessary enhances your digital protection.



Did you know that?

The average person taps and swipes her cellphone more than 2,600 times a day.

- Every step we take on the Internet is recorded and, over time, the browser we use on the phone or computer becomes a big book of our lives. To strengthen privacy and protect digital identity it is **advisable to delete your browsing history**.

- Our location reveals much about our activities and habits, and applications installed in the phone can record our movements constantly without us being aware of it and can provide information to aggressors. It is advisable to **check and disable location permissions** on the phone so that applications cannot locate you unnecessarily.



What are photo or image metadata?


They are the informative parameters incorporated into all digital photographs that are stored in a device. They show, among other things, details about their geolocation and the day and time they were taken.

Before posting or sending your photos, it is important to keep in mind that this information shall be embedded in them. If necessary, delete the metadata so as not to disclose sensitive information.

⁴⁵ 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>

⁴⁶ Smart AppLock (App Protect). Available at: <https://play.google.com/store/apps/details?id=com.thinkyeah.smartlockfree&hl=en>

⁴⁷ Apple Support. *Change your iCloud settings*. Available at: <https://support.apple.com/es-es/HT207689>

 **Security of the camera. Cover the webcam of the cellphone or computer** when they are not being used (with a post-it or a special lid), thereby preventing anyone from recording or taking photos if they have remote access to the device.



Reminder: protection from doxxing

Our information is spread all over the web. Data such as our complete name, address, phone number, email address, names of relatives and friends, or our social security number can be found on various sites of the Internet and a stalker who wishes to dox us can collect them.


You can consult data brokers about what information of yours is on the Internet and ask them to delete it. Some of these data brokers are: [White Pages](#), [Instant Check Mate](#), [Acxiom](#) or [Spokeo](#)⁴⁸. Other services such as [DeleteMe](#) or [Privacy Duck](#) can monitor sites to make sure that the information continues to be eliminated.

A reverse search of our information on Google can be made, placing address, email, or phone, or a reverse image search with [reverse image search](#) with [Google Images](#) or on sites such as [Tineye](#) or [Bing](#)⁴⁹.

04 Security on social media







Social media have become an indispensable means of navigating and expressing ourselves in the new online-offline reality and they make it possible for us to keep in contact with relatives, friends, work, interests, hobbies, etc. Nevertheless, we must not lose sight of the fact that they can also be a means to commit cyberattacks or acts of cyberviolence. For third parties, they can be a gateway to our lives, and therefore it is crucial to make sure we are only sharing our personal information with those we decide to share it.



 First, it is important to ask ourselves: **What information do we want to keep private?** The information and photos we publish online leaves an indelible trace. Because of that, it is important to ask ourselves what we want to be within reach of the public and to assess the risks and benefits of having this information made public. We must keep in mind that a harasser could take advantage of data such as our location, city, or date of birth or photos posted on public profiles.

⁴⁸ *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/>

⁴⁹ *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>

-  Avoid being easily identified, we can consider **using pseudonyms** and profile photographs that do not show physical features.
-  **Be aware of and choose the privacy and security options** of social media. It is important to take time to see what information of ours is exhibited on the web (for example, who can see our profile or postings, what content of ours they can add, and where they can label us), which can be revised and controlled using the privacy setting options. Useful guides can be consulted to explore privacy settings in the OAS publication [Media Literacy and Digital Security](#) (p. 17)⁵⁰, the website *Dominemos la Tecnología (Take Back the Tech)*⁵¹, or directly on Facebook, Twitter, [Instagram](#) and [Tik Tok](#)⁵².
-  **Disable geolocation** in the applications that do not require location to function, as well as the tag of location on social media such as Facebook or Instagram. This is an important prevention measure because whenever something is posted on social media, geolocation data are recorded, which can be used to find our home or the places we visit often.
-  If relatives or friends are sharing our photos or updates on their social media with our information and it is deemed that, for security reasons, it would be better to keep this information confidential, they can be requested to disable the geolocation or the location tag in their postings.
-  Check **what devices are connected to social media**. If there is some unknown person, it is advisable to disconnect that person, because it might mean that they cloned the phone and that another person has access to the applications (and information) from another cell phone or computer.
-  Help services and technical support from the different social media can be consulted ([Facebook](#), [Twitter](#), [Instagram](#) and [TikTok](#)) to talk about doubts or ask specific questions about their functions or problems emerging during interactions⁵³.




⁵⁰ 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>

⁵¹ Take Back the Tech. *Social Media Privacy*. Available at: <https://www.takebackthetech.net/es/privacidad-en-las-redes-sociales>

⁵² 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>.

⁵³ 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 Security for online games

-  Do not use profile information or photos that reveal personal details.
-  For greater security, use one-time gamertags⁵⁴ and different names on each platform. This precaution prevents the others from being easily located, as well when a game account has been compromised.
-  Learn about and **change the privacy settings** of online game systems in order to control the information that is made public (for example, who can see the profile or the real name, who can see the list of friends or send messages, who can see when you are online or videos).



Tip

More advice on how to play games online safely can be found in the guide of the website *Feminist Frequency*⁵⁵.

06 Sexting safely

Technologies have opened up new channels for the expression of intimacy and sexuality. Nevertheless, because of the mindset of gender-based violence and discrimination pervading digital spaces, it is important to learn about related risks and take control over technological tools to protect yourself, knowing that the process is never entirely safe. The platform [Acoso.online](https://acoso.online) proposes highly useful questions to steer persons through three key stages of this process (R.A.P.)⁵⁶:




- 1. Recording:** Who will record it and where? On what device? Does this device save a copy automatically in the cloud? Will the face or another physical feature be shown that would facilitate identification?
- 2. Storage:** Who will store the material and where (in the cloud, on the phone, in the computer)? Who will have access to that recording? For how long? What digital security measures will be taken to prevent a third party from having access to the material?
- 3. Publication:** Has any thought been given to disseminating or posting the material? Is there any certainty about whether or not the material will disappear if it is subsequently deleted? What options are available on the Internet platform to protect the safety and privacy of users?


⁵⁴ 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.


⁵⁵ *Feminist Frequency. Speak Up & Stay Safe(r): A Guide to Protecting Yourself from Online Harassment.* Available at: <https://onlinesafety.feministfrequency.com/en/>


⁵⁶ *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:


 **Is there trust?** It is crucial to feel safe with the person who will be receiving the image or video, because that person will also be responsible for protecting the privacy of those who are participating in the exchange.


 **Consent is fundamental.** To reach an agreement about how the photos will be shared and the types of details that may appear in the photo.

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

 **Edit the content** if necessary (for example, with emojis that cover up the features that could reveal the identity).

 **Do not forget the metadata** of the images, which could provide information making it possible to identify the person who took the photo. In addition, make sure the recording is always done in one's own device, learn about and control its setting, and disable the automatic location tags.

 **Choose the media well.** Do not share intimate images on public WiFis. In addition, when using messaging applications such as WhatsApp, you run the risk of having the images or videos resent or disseminated because, although messages are end-to-end encrypted, the content is saved in the devices. Snapchat makes it possible to make ephemeral postings that are deleted after a lapse of time, but the receiver can do a screenshot of the image received and keep it saved on their device.

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



Tip

For greater protection, the following applications⁵⁷ can be used: [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 seen, in addition to blocking attempts at screenshots; or [Wickr](https://wickr.com/) which has the option of detecting and sending a notification if the person who received the image took a screenshot.



Tip

The website Ciberpatrulla⁵⁸ (Cyberpatrol) includes a [tutorial](#) to review and delete the metadata of images in Windows, Mac, iOS, and Android.

It is also possible to use [programs to delete metadata](#), such as Nectar, MedialInfo, Metanull, and Get-Metadata.

⁵⁷ *Signal*. Available at: <https://signal.org/es/>; *Confide*. Available at: <https://getconfide.com/>; *Wickr*. Available at: <https://wickr.com/>

⁵⁸ 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/>



Advice on digital security for women victims of domestic or partner violence

In abusive relationships it is increasingly common for the aggressor to attempt to gain control and extend violence via new technologies, especially cellphones, which are the preeminent medium to ensure connectivity in our daily online-offline lives. When this happens, it is reasonable to assume that our partners or former partners were hackers or technology experts, because they always managed to find out where we were, what we were doing, the messages we sent, the things we looked for on the Internet, or with whom we were in contact. Nevertheless, in various studies, it has been observed that **most aggressors have very rudimentary knowledge of technology which they simply know how to use for their benefit.**



Of course, not all experiences, threats, and risks encountered by victims are the same. It is important to keep in mind, however, that **all women can learn very simple techniques to take care of themselves, reinforce their digital security**, protect their communications, and even resort to technology to be connected with trustworthy contacts, seek help, or document the violence.

Below we provide advice that could be taken if domestic violence from a partner or former partner has included use of a cellphone. Some of the advice picks up on recommendations posted by organizations such as Derechos Digitales and MaríaLab in their *Guide of digital precautions for women victims and survivors of violence during the COVID-19 pandemic*⁵⁹.







Nevertheless, before adopting any of these measures, it is very important to assess the risks themselves and **to do only what leads to safety or comfort.** There are no one-size-fits-all formulas to tackle this type of situation, and digital security is a personal process that every person must carry out at their own pace and in accordance with their own circumstances.

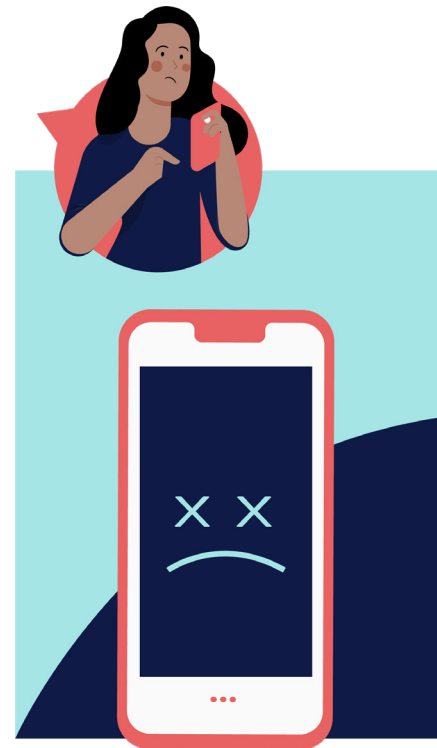
First, to examine the options and security thoroughly, it is important to ask the following questions: Was it the aggressor who provided the cellphone or had access to it for a period of time? Does he still have permanent access to the phone without being able to avoid it?

If the answer is yes, it is possible that the aggressor has access to the cellphone via spyware; in that case it is advisable to disconnect the device from the Internet, revise the setting, and to the extent possible stop using it and look for another phone to communicate with.



⁵⁹ Goldsman 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 whether or not the phone has a spyware program installed** (whereby photos, chats, location, and phone calls can be seen) using applications such as [Root Verifier](#) for Android⁶⁰.
-  Furthermore, **oftentimes aggressors use applications that might appear to be harmless**, but in fact they reveal the victim's location, such as applications to find the device in the case of loss or theft, which are already installed in many phones (for example, Find my Phone). If this application is found and the access account is not recognized, it is possible that they are using it to track the phone; it is therefore advisable to disable it. On these links, you can find out how to disable applications in [Android](#) and how to disable [Find my iPhone](#)⁶¹.
-  It is also possible **to check whether or not one of the applications on the phone has a permit** for a superuser⁶², because it could be a *spyware*⁶³.
-  It is important to recall that much of our information is stored in the cloud, and because of that it is crucial **to change the password of the Google or iCloud account on the phone**. It is also recommended to start a session on a device that is deemed to be safe and to change the passwords of all the accounts. On the Google and Apple websites, there are instructions on how to change the password of the account of an [Android](#) device and the [ID of Apple](#)⁶⁴.
-  Even after having done the above, if you still suspect there is spyware, you can go back to the original factory default settings, which can disable all the programs installed. You have to keep in mind that this will also delete [photos](#), information, and contacts, and therefore it is important to copy them beforehand⁶⁵. In the following links, you can consult a [guide to ensure information backup](#)⁶⁶ and how to restore the factory default settings of an [Android](#) and an [iPhone](#)⁶⁷.
-  If you prefer a much more thorough revision, it is suggested you disconnect the device from the Internet, stop using it immediately, and take it to a digital security expert who will be able to discover further details about any potential spyware.



It is important to have a strong lock code in the phone. If that is not feasible because of pressure from the aggressor (for example, if that would make him violent), you can install an application that simulates an error appearing in the phone whenever someone attempts to use the applications without a password.

⁶⁰ Google Play. *Root Verifier*. Available at: https://play.google.com/store/apps/details?id=com.abcdj.rootverifier&hl=en_US

⁶¹ 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/>

⁶² 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.

⁶³ 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

⁶⁴ 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>

⁶⁵ Mayores conectados. *Cómo pasar fotos del celular a la computadora*. [How to transfer photos from cellphone to computer]. Available at: <https://mayoresconectados.com.ar/descargar-fotos-del-celular-a-la-computadora>

⁶⁶ ESET-LA. *Guía de Backup*. [Backup Guide]. Available at: <https://www.welivesecurity.com/wp-content/uploads/2017/03/guia-backup.pdf>

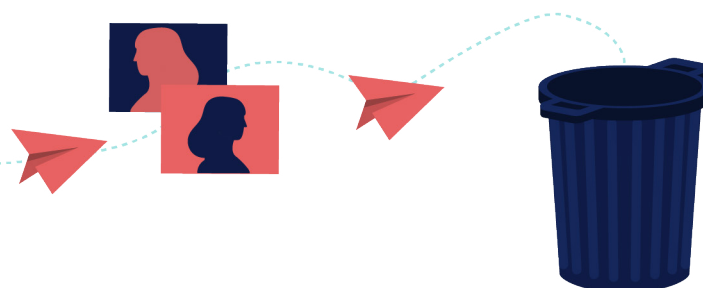
⁶⁷ Google Help Center. *Reset your Android device to factory settings*. Available at: <https://support.google.com/android/answer/6088915?hl=es>; Apple Support. *Restore your iPhone, iPad, or iPod to factory settings*. Available at: <https://support.apple.com/es-es/HT201252>



It may also happen that the aggressor frequently checks the cellphone, without the victim preventing it. In those cases, the following can be done:



If you are thinking about asking for help, **remember do not leave any traces of it on the phone** which could be identified by the aggressor: delete photos, videos, messages, or the history of visits or Internet searches that might provide them with clues to how you are thinking of seeking help.



It is important to recall that all information searched on the Internet or the websites that are visited remain registered in the cellphone or computer. If sensitive information is being searched but you wish to conceal this (for example, numbers for calling emergency or support services for cases of violence), you can **delete your browsing and search history** and use the incognito or private mode so as not to leave any traces. On the Google website, you can consult how to [delete browsing history](#) from Chrome⁶⁸.



You can agree on a “**secret code**” with **persons you trust** to call for help via specific emojis. For example, grapes (emoji) 🍇 would mean “he’s attacking me.” Learn these codes by heart and delete the message after sending it.



Make sure you **delete the history of chat messages** and use communication codes agreed upon with your support network.



Do not keep names on your phone that can provide the aggressor with clues that you are asking for help. For example, instead of writing “shelter,” write “Mrs. Martínez.”



Jot down on a piece of paper the contact phone numbers of persons you trust and put it away in a safe place. This will be useful if the aggressor prevents you from using your phone.



⁶⁸ 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'm being the victim of acts of digital violence?

Every woman and girl has unique needs and experiences and experiences online violence differently, and because of that it is important to avoid generalizations when drawing up strategies to prevent violence. Taking into account this diversity, practical advice is provided below that could be of use when encountering digital violence.

Stop momentarily and remember: The victim of violence is NEVER to blame



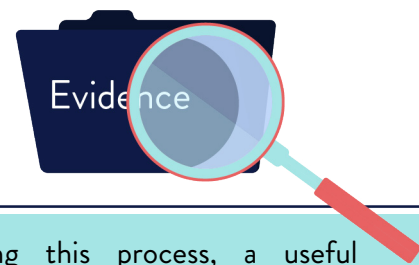
If attacks, harassment, or threats are received and if intimate images or videos are posted on the Internet, it is never the fault of the victims, even when they did not take the necessary digital precautions.

Online violence experienced by a woman or girl **is not her fault**, regardless of whether she has taken the precautions that are needed for that situation or shared intimate pictures in a context of a relationship of trust. **The burden of responsibility always lies with the aggressor, not the victim.**

In situations such as these, engaging in personal practices of digital self-care or hygiene can be of great help for survivors of violence. It is advisable to stop momentarily, go for a walk or rest your eyes, talk to a friend, or take a break from social media. Online violence can be overwhelming and giving yourself time to take care of yourself can help you better steer your way through the media and the situation.

Document

If you are a survivor of some form of online violence, it is advisable to **document, register, and keep, in a safe and orderly fashion, all evidence of the violence** that might be relevant (emails, messages received on social media, SMS messages, voice messages, or phone calls). This will not only help you feel in control of the situation, but also it can be useful if you decide to go to the authorities or report it on Internet platforms. It can be done manually, saving the hyperlinks of the websites where the material appears or taking screenshots of the violence received via the functions of Windows or Mac or with applications such as Snapfiles or Evernote⁶⁹.



During this process, a useful support tool is the table of evidence drawn up by Aceso.online.

⁶⁹ 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>.

It is important to keep the evidence in folders in an orderly fashion and chronologically. Precautions must also be taken to keep the evidence safe, whether in a digital format with a password or even as a printout.



If you are the victim of nonconsensual distribution of intimate or sexual content, it is important to keep and back up the evidence before deleting the material: taking screenshots of the websites where the material, text messages, or emails received appear (with time and date and group members) and, if necessary, downloading the video and keeping it.

If you are the victim of domestic violence perpetrated by a partner or former partner, it may be very important to document the acts of violence when reporting them to the authorities. For this purpose, you can resort to the cellphone or diverse applications to save recordings or videos, take photos, take screenshots of violence on social media, or keep a log of hostile text messages. Nevertheless, before doing so, **it is crucial to ascertain if that might jeopardize you even further** (for example, if the partner or former partner has access to the device). If a risk is perceived, it might be more advisable not to keep a log or to consider the possibility of sending the evidence to a person of trust or to a relative who can keep it for you (and after resending it, deleting it from the phone and cloud). It is also important to jot down the time, day, and place of the incident. Further information on documentation can be found in the [Guía de Derechos Digitales and MariaLab](#).

Blocking or reporting violence on social media

Blocking aggressors and online harassers on social media can be of help to protect yourself from harmful, unwanted, and inappropriate behaviors, especially if the extent of online violence is causing much anxiety or negative feelings. Nevertheless, the **decision to block or not block is exclusively personal** and shall depend on each context.

- **Blocking and silencing on Twitter.** As indicated by Amnesty International, Twitter is the social media with the highest volume of online harassment and stalking against women. In this context, it is important to know how to use social media safely; for example, knowing how [to block and silence potential harassers](#) or [share blocking lists](#)⁷⁰. The OAS publication [Media Literacy and Digital Security](#), also has recommendations for tools to navigate safely on Twitter and to report tweets, messages, accounts, and violations of the rules.
- How to block aggressors can also be consulted on the websites of [Facebook](#), [Instagram](#) and [Tik Tok](#).

Social media also have **specific tools to report information or behaviors** that are harmful, abusive, or detrimental and violent threats. They are required to analyze the report and take the necessary measures, ranging from a warning to the user responsible for the behavior to termination of his account. Although much still needs to be done to improve the response of Internet platforms to cases of violence, what is certain is that reporting incidents makes it possible to document patterns of aggression and contribute to highlighting the online violence that is affecting millions of women online.

⁷⁰ 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.

If you decide to report the violence, as a rule you will have to **describe the incident or the type of threat or send a screenshot** with the violent content or a link. On platforms like Twitter or Facebook contents can also be reported directly clicking on the upper right-hand part of the article just when it appears. Guides can be consulted to report incidents on [Tik Tok](#), [Instagram](#), [Twitter](#), [Facebook](#) and [YouTube](#)⁷¹.

Looking for help

If you are a victim of online violence or suspect you might be a victim, it is advisable to request help from relatives, friends, or other persons you trust. When you are in a situation of major stress, you can even ask a friend, man or woman, to monitor updates on social media or in abusive postings, so that you won't have to do it yourself directly.

On the Internet you can also a large **network of digital security support and collective practices** that women have created for mutual support in cases of ICT-facilitated violence. Many organizations have emergency numbers that you can call if you are a victim of the nonconsensual distribution of intimate images, and they can help you file reports on Internet platforms, track images or videos that are circulating online, and call for them to be removed (a list of some of these organizations can be found in P. 71).

It is also important to make efforts to go to mental health services. Digital violence can be overwhelming and may have serious psychological impacts, ranging from feelings of anxiety and depression to suicidal tendencies, and therefore emotional or psychological support during this process must not be underestimated.

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.

⁷¹ 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 you respond to aggressors?

There is no correct answer to the question, no single formula that might be applicable to interactions with harassers and perpetrators of online violence and keeping in contact or not shall depend entirely on each person's priorities and what makes them feel more comfortable and safe.

For example, in cases of ICT-facilitated domestic violence, it may be that the failure to respond will lead to even greater physical violence from the partner or former partner, in which case interactions may be kept online or, on the contrary, you may feel safe enough to block all online communication with him. As indicated earlier, each experience is different and, to the extent possible, it is best to weigh the options available within the context of each person.

In other cases of online violence, such as in incidents of online harassment, priorities have to be decided on. If, for example, it is a priority to protect your psychological and emotional health, it may be best not to interact with the aggressor or aggressors so as to prevent attacks from escalating. On the other hand, if it is important to expose the harassment or face the aggressors and if it is possible to accept the risk of receiving more attacks or online

harassment, one feasible option is to write directly to the aggressors, re-Tweet their comments, or resend them to friends, activities, organizations, or journalists to make them go public and viral. In the [guide of PEN America](#) and on the website [Ciberseguras](#) advice can be found on how to respond safely to harassers⁷².

Another technique is “to reply conscientiously” to the attacks, using a proactive and non-violent style of communication to highlight the sexism and gender-based violence of the aggressors (for example, incorporating irony or humor into the replies).

In short, there is no one-size-fits-all response to this question; it shall depend to a large extent on what each person deems is best for their physical and emotional integrity.

Should you report the aggression to the authorities?

Women and girls have the right to live a life without violence both online and offline and to obtain justice when this right is violated. To report violence to the authorities may make it possible for acts of digital violence to be duly logged and substantiated, thus speeding up the process of removing the harmful contents by Internet platforms, especially in cases of online harassment, doxxing, or the nonconsensual distribution of intimate images.

Emergency numbers to ask for 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)



⁷² 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/>

Furthermore, in cases of reports of intimate or domestic violence, in view of the recurring use of technology to extend the reach of abuse and control, it could be important to notify authorities about all online violence events occurring during the relationship or afterwards, so that they can take them into consideration when reviewing the case and, if necessary, issue protective orders.

Pursuant to the provisions of the Inter-American Convention for the Prevention, Punishment and Eradication of Violence against Women (Convention of Belém do Pará), states have the obligation to prevent, investigate, punish, and redress online gender-based violence against women and girls with due diligence.

Although the authorities still have much to do in order to improve services and monitoring of online violence, the fact is that progress has been made in the region, with recent efforts to provide training to civil servants and even the establishment of special cybersecurity laws and units in many countries.

It is also important to keep in mind that, even when addressing behaviors that could be viewed as “new,” the statutory frameworks currently in force (including those in which no standards have been drawn up or they have not been categorized as criminal offenses) make it possible to provide a legal framework for various online acts of violence against women in laws against cybercrime, laws on violence against women, criminal laws, and laws on data privacy and protection, as well as to investigate, prosecute, and punish them. This probably requires somewhat more advanced knowledge about legal concepts and techniques, but it does not mean that survivors of online violence cannot use them if they receive proper guidance. The organizations indicated in “To explore further” have drafted a paper regarding this and it can be consulted in case the option of going to the authorities is taken.



Creating a community

Talking, sharing, and socializing the experience can be highly useful; by highlighting this form of violence, we can contribute to talking about the issue and implementing tools to support the victims and survivors.

Tackling online violence can also be an opportunity to learn more about digital security technology and measures. Although they may seem to be far removed from one another, cybersecurity, gender equality, and the prevention of violence are very closely intertwined, and by learning to protect our identity and sharing those lessons with other women and girls, we will contribute to making the Internet a space that is more inclusive for all women and girls.



To explore further

By providing the following resources, the OAS or its member states are not endorsing their contents or the organizations identified. The resources are being offered as examples of organizations, guides, tools, etc., that are available in the region so that readers can broaden their information on the subject being addressed in the present 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](#)

[ClAandestina](#) (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 (also referred to as app). It is a computer program created to carry out or facilitate a series of specific tasks (professional, leisure, educational, etc.) which runs on smartphones, tablets, or other mobile devices. There are free and paid applications. As a rule, apps are available on specific distribution platforms or from the companies owning the operating systems of the electronic devices.

Blackout. An Internet outage caused by an attack on a website, an Internet service provider (ISP), or the Internet Domain Name System (DNS). It can also involve an interruption because of an incorrect setting of the web server's infrastructure.

Blog. It is a website in which to write and post brief articles on specific or open subjects.

Chat. Digital communication method in real time conducted between various users whose computers are interconnected via a network.

Child grooming, or online sexual grooming of children. Child grooming involves deliberate actions taken by an adult to approach a minor for the purpose of engaging in a relationship and exerting emotional control over the victim, making it possible for sexual abuse to be perpetrated, virtual relationships to be initiated, child pornography to be obtained, and trafficking in the minor to be carried out.

Cloud. The term designates the global network of servers designed to store and administer data, run applications, or deliver contents or services.

Creepshot. A creepshot refers to any photo a man takes of a woman or girl in public without their consent. The photos usually focus on the victim's buttocks, legs, or cleavage.

Cyberflashing. Cyberflashing involves sending obscene photos of a woman without her consent for the purpose of pestering, bullying, or embarrassing her.

Cybermobbing. The action of groups organized online that post offensive or destructive contents on a massive scale with the intent to embarrass someone or force them to remove their profile from social media.

Data encryption. Data encryption is a method to convert digital data into codes, which make the encoded information illegible except for the person who has the correct key to decrypt it.

Deepfake. Artificial intelligence technique making it possible to edit fake videos of persons to make them look real, using learning algorithms and pre-existing videos or images.

Denial-of-service attack. A denial-of-service (DoS) attack is a cyberattack flooding a server with service requests to prevent legitimate users from using it. A more sophisticated method of this kind of disruption is the distributed denial-of-service (DDoS) attack, where the requests flooding a server are coordinated from many different sources.

Downblousing. Downblousing involves taking unauthorized photographs down the top of a woman's blouse.

Doxing, or doxing. The term comes from the phrase "dropping docs" and consists of extracting and posting online personal information without authorization.

Emoji. Small digital image or icon used in electronic messages to represent an emotion, an object, an idea, etc.

Equality between women and men (gender equality). Gender equality refers to the equal rights, responsibilities and opportunities of women and men and girls and boys. [Source: UN Women, *OSAGI Gender Mainstreaming - Concepts and definitions*].

Firewall. A physical or digital system aimed at enabling or preventing access from or toward a network in order to guarantee that all communications between the network and the Internet are carried out in conformity with the security policies of an organization or corporation.

Gamertag. Unique identifier for persons who play games and share contents on the online gaming service platform Microsoft Xbox Live. It is created on the basis of an alias, avatar, or image and information about the player's preferences.

Gaslighting. Gaslighting is a form of psychological abuse that involves manipulating the targeted victim's reality so they will question their sanity, memory, or perceptions.

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

Gender gap: It refers to any disparity between the condition or status of women and that of men in society (differences in access to resources, rights, and opportunities).

Gender perspective. Analytical mechanism consisting of observing the impact of gender on the opportunities, roles, and social interactions of persons [Source: UN Women, OSAGI *Gender Mainstreaming - Concepts and definitions*].

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

Gender stereotyping. A gender stereotype is a generalized view or preconception about attributes or characteristics, or the roles that are or ought to be possessed by, or performed by, women and men [Source: OHCHR, *Gender stereotyping*].

Gender trolling. Posting of messages, images, or videos, as well as creating hashtags (tags), for the purpose of pestering women and girls or instigating violence against them.

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

Geolocation. Geolocation is the capacity to obtain the real geographical location of an object, such as a radar, cellphone, or computer connected to the Internet.

Hacker. A hacker is a person who secures unauthorized access into a computer system.

Hacking. Hacking involves a hacker using techniques and procedures to break into, without authorization, third-party computer systems for the purpose of manipulating them or obtaining information or entertainment. Cracking is a practice related to hacking but entails breaking into third-party systems for criminal purposes to invade the privacy of the targeted person or the confidentiality of their information or damaging information or physical platforms.

Hashtag or tag. Chain of characters prefaced by the hash symbol #. It is used on social media to identify the subject of a conversation or message. It also enables the automatic creation of a hyperlink that provides access to all contents that include the hashtag concerned.

Hate speech. Hate speech involves using language to disparage, insult, threaten, or attack a person because of their identity and/or other features, such as their sexual orientation or disability.

HTTPS. This acronym means Hypertext Transfer Protocol Secure and consists of a network protocol aimed at ensuring the secure exchange of encrypted data.

Internet of things (IoT). The Internet of things describes the network of daily physical objects and devices connected to the Internet for exchanging data between these devices.

Keylogger, or keystroke recorder. It consists of a malware placed between a keyboard and operating system to intercept and record information from each key struck on a device without the person using the keyboard being aware they are being monitored.

Malware, or malicious software. The term comes from bringing together the words “malicious” and “software” and refers to a type of software that aims to infiltrate and/or damage an information system without the consent of the person using the system.

Metadata. Metadata are data about other data, in other words, information used to describe the data contained in a file, document, photograph, webpage, etc.

Online gender-based violence, or gender cyberviolence against women. The term means any act of gender-based violence directed against a woman because she is a woman and/or which affects women disproportionately, facilitated either partially or entirely by information and communication technologies or heightened by them, such as cellphones and smartphones, the Internet, social media platforms, or email [Source: *United Nations Special Rapporteur on violence against women*].

Sex (biological). Refers to the biological features that define human being as females and males.

Sexting. Sexting is a practice that involves generating and exchanging sexually explicit material between two persons. It can include the creation and sending of images with consent or the consensual creation of images that are distributed without consent.

Sextortion. It consists of threatening a person with the disseminating of their intimate images or videos for the purpose of obtaining further material on explicit sex acts, engaging in sexual relations, or extorting money.

Social media. An information society service that provides users with a communication platform via the Internet so they can generate a profile with their personal data, facilitating the creation of communities based on common criteria and enabling communication, so that users can interact via messages and share information, images, or videos, making it possible for these postings to be immediately accessible to all persons belonging to a group [Source: Royal Spanish Academy].

Software. Set of computer programs, instructions, and rules that enable electronic devices to execute certain tasks.

Spyware, or spying malware. A type of malware infecting a device and secretly recording, without the consent of the legitimate user, browsing data, personal information, device location, log of calls or messages, among other personal data.

Trending topic. It refers to the word or phrase most often repeated on social media at a given time.

Troll. An unidentified person who is posting messages online with the intent of pestering users, provoking them to give an emotional response, or altering online conversations.

Upskirting. Taking photographs up the skirt of a woman or girl without their consent.

URL. URL is the acronym for Uniform Resource Locator and refers to the specific web address allocated to a web resource available on the Internet (webpages, websites, documents) specifying its location so that it can be identified and retrieved.

Violence against women. Violence against women is any act or behavior of gender-based violence that results in death or physical, sexual, or psychological harm or suffering to women, whether occurring in public or in private life [Source: Article 1 of the Inter-American Convention for the Prevention, Punishment and Eradication of Violence against Women].

Virtual private network. Also referred to by its acronym VPN, it extends a private network computers of a local area network (LAN) across a public or uncontrolled network, enabling users of those computers to send and receive data across public networks as if they were private networks (ensuring the connection is safe by encrypting the information).

Virus. A computer virus is a self-replicating computer program that alters the normal operation of an electronic device. Viruses are different from other types of malware in that they replicate automatically, in other words, they are capable being copied from one file or computer to another without the consent of the user.

WiFi. WiFi is a family of wireless network protocols used for the networking of devices connected to one another and generally connected to the Internet as well via wireless access points (WAP).

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
- 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
- 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.

