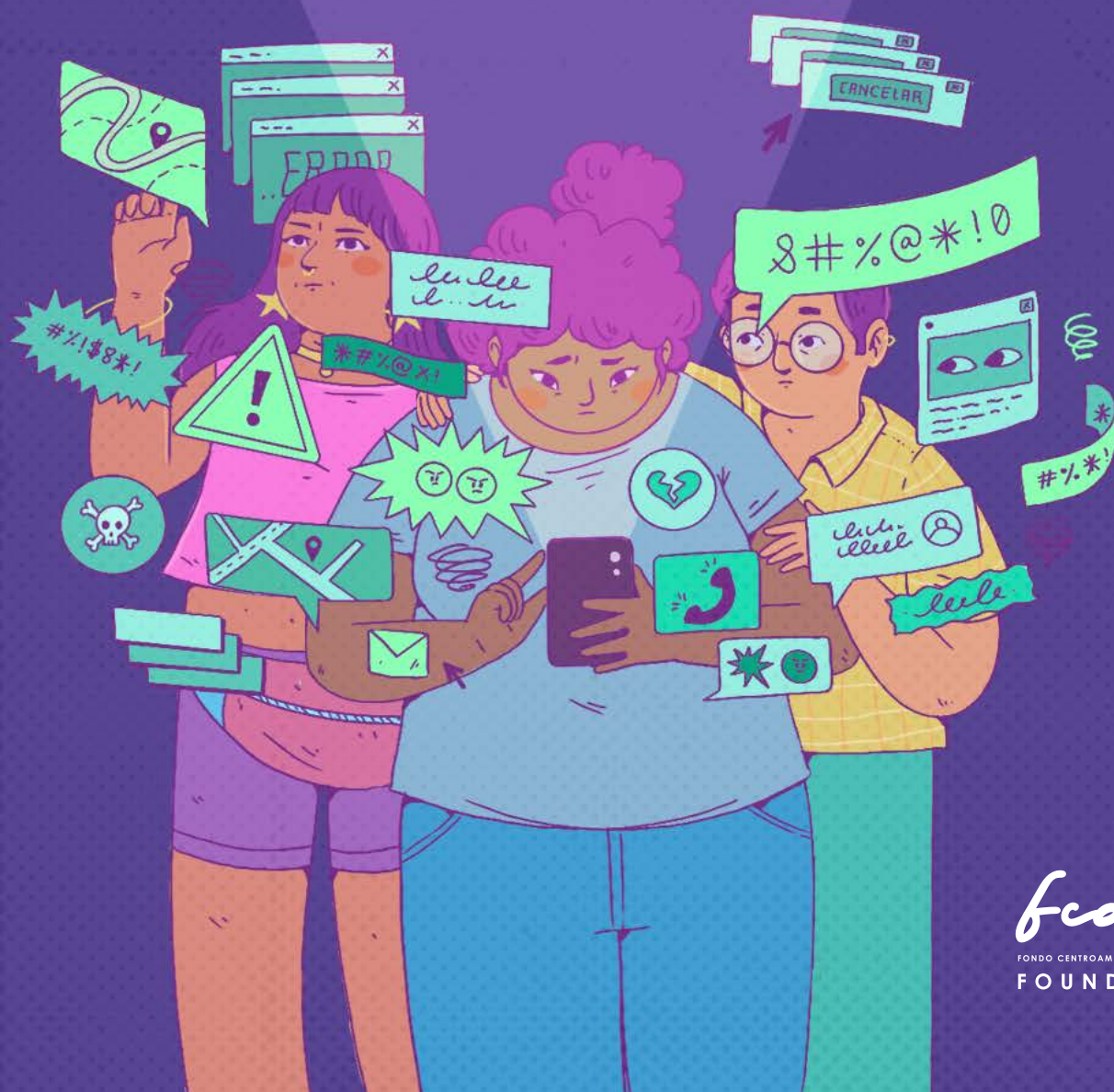
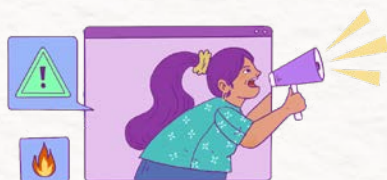


DIGITAL VIOLENCE AGAINST WOMEN AND GENDER AND SEXUAL DISSIDENTS *in Guatemala:*

Impacts on Democracy and Techno-Resistance





Digital Violence against Women and Gender and Sexual Dissidents in Guatemala: Impacts on Democracy and Techno-Resistance.

Amaral Arévalo, lead researcher

Willka Ñusta Taylor, research assistant

Reviewed and edited by FCAM Foundation

FCAM Foundation, 2026

This publication was produced as part of the “Nuestras Redes Funcionan” project, funded by the Digital Democracy Initiative (DDI) and implemented by the Alianza de Fondos de Mujeres y Feministas de América Latina y el Caribe. It forms part of a collection of national and regional studies on technology-facilitated violence developed by the eight funds that make up the Alliance. The initiative seeks to strengthen the production and dissemination of knowledge in order to better understand, bring visibility to, and address the various forms of violence affecting the region from feminist perspectives.

**NET THAT
WORKS**

alliance
of Women's and Feminist Funds
of Latin America and the Caribbean

fcam
FONDO CENTROAMERICANO DE MUJERES
FOUNDATION

Contents



Introduction	4
 Chapter 1:	
Activism and Human Rights in the Age of Netcenters	8
 Chapter 2:	
“It Has Given Me More Strength to Speak Out and Report It”: A National Assessment of Digital Violence	21
 Chapter 3:	
“Algorithms Aren’t Neutral”: Tensions and Consequences of Digital Violence for Democratic Culture	36
 Chapter 4:	
“Give Them Loving Comments”: Techno-Resistance	55
 Chapter 5:	
Concluding reflections	80
 References	86

Introduction

Violence against women and sex-gender dissidents is a complex and evolving phenomenon shaped by diverse historical and cultural configurations. Today, in a context of hyperconnectivity, social media and digital platforms have intensified the circulation and reproduction of misogynistic (Suárez, 2023) and anti-LGBTQ+ practices (GLAAD, 2025). Although these forms of violence unfold in virtual spaces, their consequences are tangible in everyday life. The digital environment, initially conceived as a democratizing space for expression and debate, has thus been reconfigured, particularly over the past decade, as fertile ground for the expansion of symbolic and psychological violence which, depending on the context, can escalate into physical harm and aggression, in some cases with lethal consequences.

Digital violence against women and sex-gender dissidents in Guatemala is an extension of the structural violence that has historically sought to silence, discipline, and exclude from the public sphere those who challenge the patriarchal and cisheteronormative order. Against this backdrop, the relevance of this exploratory study lies in the need to understand technology-facilitated gender-based violence (TFGBV) not as an isolated phenomenon, but as an extension of the patriarchal, racist, and heteronormative structures that have historically legitimized control over women's bodies and sought to suppress the political voices of feminists and sex-gender dissidents.

The internet did not create misogyny or anti-LGBTQ+ prejudice, but it does amplify their persistence and embeds them within new dynamics of power and control. Understanding this context is essential to developing organizational, political, and social responses that go beyond punishing perpetrators. While accountability is important, responses cannot end there; they must also pursue the political and cultural transformations necessary to eradicate these forms of violence.

Using an intersectional feminist approach, this exploratory, qualitative study documented the experiences and lived realities of women and sex-gender dissidents from FCAM Foundation partner and allied organizations in Guatemala, particularly in relation to control over their bodies. The research focuses on the digital sphere, understood as a political space in which technology-facilitated gender-based violence is reproduced and expanded, while opportunities for democratic participation are simultaneously undermined.

The study sought to analyze how digital violence against women and sex-gender dissidents involved in social movements in Guatemala affects the possibilities for building a democratic, critical, and active culture that fosters transformative feminist practices in everyday spaces of digital interaction.

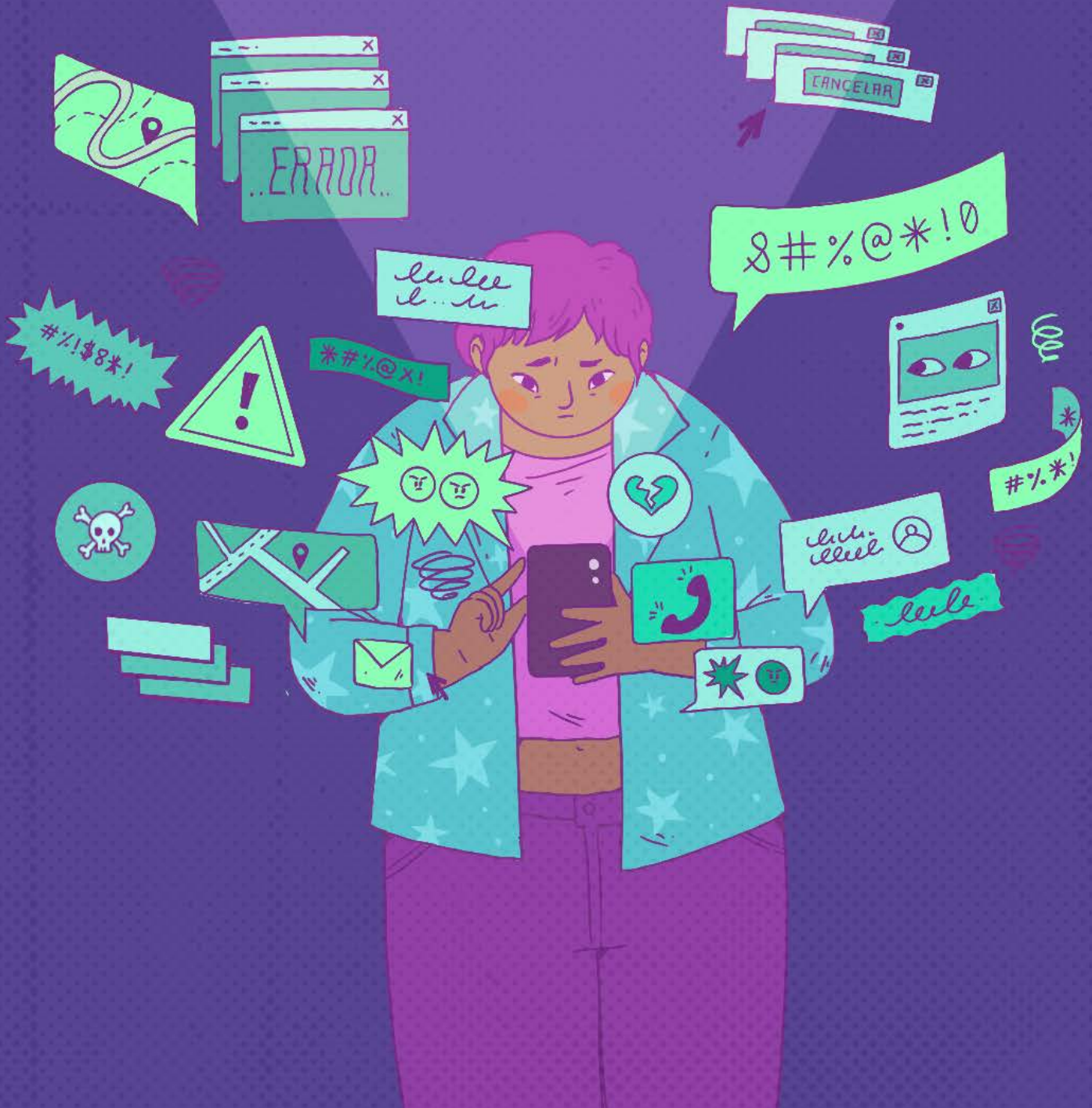
This qualitative and descriptive study was conducted in Guatemala, with participants' identities kept anonymous. Research methods included document analysis, a digital questionnaire, and semi-structured virtual interviews with key informants. The study was conducted between November 2025 and February 2026. FCAM Foundation extends its thanks to the 20 collectives and organizations that shared their reflections, analyses, and experiences throughout the research process.

This report is divided into five chapters.

» **Chapter 1** begins by examining Guatemala's democratic crisis through the lens of "reproductive reconquest" (Arguedas, 2024). It shows how the capture of the state by economic elites, criminal networks, and "hidden" powers reinstates neocolonial privileges and deepens hierarchies of gender, sexuality, and power. This framework provides a basis for understanding how the rapid expansion of Guatemala's digital ecosystem, in a context marked by profound socioeconomic, gender, and ethnic inequalities, has transformed digital platforms into a battleground where patriarchal and racist violence, as well as violence driven by anti-gender ideologies, is both reproduced and intensified.

- » **Chapter 2** explores the concepts and practices that can strengthen digital democracy. In particular, it examines the interactions that facilitate or inhibit pluralistic exchange and democratic openness, as well as forms of resistance to algorithmic closure and fragmentation. The chapter presents the overall results of an online questionnaire designed to gather contextual information on risks, practices, and forms of resistance related to digital security. The questionnaire was administered between November 26 and December 3, 2025, and was completed anonymously by 28 activists from 20 FCAM Foundation partner collectives and organizations in Guatemala.
- » **Chapter 3** draws on five virtual interviews with six activists to examine the effects of technology-facilitated gender-based violence on women and sex-gender dissidents. These effects range from self-censorship and withdrawal from the public sphere to psycho-emotional impacts. Particular attention is given to how the absence of clear tools and protocols to prevent, document, and respond to attacks can lead to self-censorship, including closing social media accounts, reducing one's digital presence, or refraining from expressing opinions. While these responses may serve as immediate protective strategies, they carry significant costs for freedom of expression, political participation, and democratic pluralism online.
- » **Chapter 4** examines techno-resistance as a framework for understanding how women and sex-gender dissidents produce, share, and legitimize contextualized knowledge and practices to protect and sustain themselves in digital environments shaped by inequalities of gender, sexuality, and power. The chapter systematizes the strategies activists and organizations use for individual and collective care in response to digital violence. It considers both forms of collective action and political techno-resistance, as well as the tensions that characterize the digital sphere itself.

» **Chapter 5** offers concluding reflections and traces the historical continuities through which the digital sphere does not create violence, but rather rearticulates existing forms of it. Although the post-conflict transition opened new spaces for women and sex-gender dissidents, these spaces have been weakened by state capture and moralizing agendas. The chapter also examines the challenges organizations face in maintaining digital sovereignty amid democratic closure and limited sustainable capacities. In this context, techno-resistance emerges as a fundamental component of both organizational sustainability and the defense of democracy.

[illegible]

Contemporary analysis of Guatemala's democratic crisis requires situating its political and social dynamics within a theoretical framework capable of explaining, simultaneously, the intensification of inequality, the erosion of public space, and the authoritarian reconfiguration of the moral norms that structure collective life. In this regard, Gabriela Arguedas's (2024) concept of "reproductive reconquest" helps illuminate the particularities of Guatemala's current context, where democratic struggles extend beyond the formal dimensions of the rule of law, the separation of powers, and the exercise of civil and political rights to encompass struggles over bodies, subjectivities, and gendered structures.

Arguedas (2024) conceptualizes reproductive reconquest as a far-reaching political, economic, and cultural process fueled by nationalist, misogynistic, xenophobic, and conservative narratives, as well as religious fundamentalisms. It seeks to reject feminist demands and restore an ideal "good society" that prescribes particular models of femininity and motherhood, masculinity and fatherhood, while reaffirming the sexual division of labor and the authority of the paterfamilias over women and children (Arguedas, 2024, pp. 24–31). In this context, the "reproductive" dimension should not be understood narrowly. Rather, it refers to a reconquest of women's bodies and, above all, their subjectivities, both of which are essential to sustaining the economic and symbolic order being restored (Arguedas, 2024, pp. 27–29).

Reproductive reconquest functions as a mechanism for reinstating privileges and transforming the public sphere into a space captured by elites. This process is legitimized and deepened through a moral offensive aimed at reclaiming the "freedoms" and political power that conservative actors perceive as having been curtailed by advances in women's rights and the rights of sex-gender dissident communities, as well as by legal restrictions on the imposition of religious doctrine, particularly that of neo-Pentecostal evangelical groups, within public institutions (Arguedas, 2024, pp. 25–29). In contexts marked by extreme religious conservatism and machismo, this offensive is not merely incidental; according to Arguedas, it forms an integral part of authoritarian structures and tends to point toward an anti-democratic trajectory (Arguedas, 2024, p. 31).

From this perspective, examining Guatemala's democratic crisis requires connecting its institutional dimensions with the everyday and digital forms of violence that disproportionately affect women, sex-gender dissidents, and Maya communities. Digital violence, including harassment, stalking, hate speech, disinformation campaigns, and political surveillance, is neither an isolated phenomenon nor simply an "excess" of online interaction. Rather, these practices constitute contemporary expressions of structural inequalities that are reshaping their repertoires of domination and repression.

Understanding Guatemala's democratic crisis and the forms of digital violence associated with it therefore requires shifting attention toward the margins and recognizing that the domination experienced by women, sex-gender dissidents, and Maya peoples is not peripheral to democratic analysis. These experiences are, in fact, central to understanding the limits and possibilities of contemporary democracy.

1.1. From the Post-War Period to Reproductive Reconquest

The period following the signing of Guatemala's 1996 Peace Accords has been marked by a profound tension between the promises of democratization and the persistence—and, in some cases, deepening—of historical structures of exclusion, impunity, and state capture. Although the Peace Accords represented a milestone in formally bringing the internal armed conflict to an end, Guatemala's traditional political leadership has resisted acknowledging state responsibility for past violence, maintaining instead that the state acted in "legitimate self-defense" against the insurgency during the 1970s and 1980s. According to Bertelsmann Stiftung (2024, p. 40), this position not only denies the systematic human rights violations committed during that period but also delegitimizes contemporary demands for justice, equality, and structural transformation.

One of the defining structural processes of Guatemala's post-war period has been the consolidation of clandestine power networks that have captured state institutions and reinstated a system of entrenched impunity. Hernández (2020,

p. 152) describes these networks as “hidden powers”: informal and amorphous networks of influential individuals who use their positions in the public and private sectors to enrich themselves through illegal activities while shielding themselves from prosecution. These networks form the basis of a political order that operates outside—and, in practice, above—formal institutions.

Within this context, the emergence of the so-called “pact of the corrupt” represents a contemporary manifestation of these parallel power structures. According to Free Press Unlimited (2023, p. 4), the pact consists of a political-economic network that has reintroduced mechanisms designed to obstruct institutional reform and anti-corruption efforts. Monzón (2024, pp. 30–31) provides a more detailed account of these connections, describing a network that includes officials from the Public Prosecutor’s Office, ministries and secretariats of the executive branch, the courts, members of Congress from right-wing parties, economic elites, and political operatives acting on behalf of opaque interests.

This convergence of actors has facilitated state capture, enabling the co-optation of the justice system and the progressive dismantling of democratic institutions. Its effects are both visible and multifaceted. They include the systematic criminalization of justice-sector personnel, including judges and prosecutors involved in anti-corruption efforts; the persecution of journalists and human rights defenders; the weakening of oversight and accountability mechanisms; and the construction of institutional networks designed to guarantee impunity for actors embedded within the state apparatus.

The International Commission against Impunity in Guatemala (CICIG) represented one of the most significant efforts to confront organized criminal structures embedded within the state. Before the termination of its mandate, CICIG identified more than 70 complex criminal structures, prosecuted more than 120 high-impact cases, and brought charges against more than 1,540 people, resulting in approximately 400 convictions (Free Press Unlimited, 2023, p. 5). Its work exposed the depth of state capture. It also generated a strong political backlash.

During the final two years of Jimmy Morales' administration (2018–2020), the government prioritized ending CICIG's presence in the country, a move that Free Press Unlimited (2023, p. 7) describes as protecting elites under investigation, including individuals close to the president. Morales ultimately terminated CICIG's mandate and framed the decision as a defense of national sovereignty against what he characterized as "foreign interference" by globalist agendas threatening the country (Marsicovetere and López, 2025, p. 85). Under the subsequent administration of Alejandro Giammattei, Marsicovetere and López (2025, p. 86) describe a process of authoritarian restoration accompanied by the further dismantling of the justice system and the persecution of activists, journalists, judges, and prosecutors. Free Press Unlimited (2023, p. 4) similarly documents an intensification of repression, censorship, and efforts to silence critical voices during this period.

State capture has manifested in a pattern of criminalization targeting those who defend democracy and fight corruption. The Special Prosecutor's Office against Impunity (FECI), which originally played a key role in combating corruption, has been used to persecute judges, prosecutors, journalists, and activists through seemingly unfounded investigations (IACHR, 2024, paragraph 76). This phenomenon has contributed to the erosion of pluralism and the restriction of democratic participation, generating a climate of fear that affects those engaged in the civic sphere.

Religious fundamentalism is another factor contributing to democratic erosion. LGBTQI+ individuals interviewed in a recent study (Duarte et al., 2020, p. 56) indicated that religion is a direct cause of the violence and rejection experienced daily by those who transgress prevailing norms, as such acts of aggression are justified as "punishments" for transgressing heteronormativity and cisnormativity. Within this framework, religion functions as a coercive mechanism that, when combined with traditional educational models, becomes a structure designed to homogenize social behavior through mechanisms of correction and punishment.

This religious influence is not limited to family or community settings but extends into the media and political spheres. The strong presence of evangelical communities in public debate challenges the secular nature of the state and promotes a

moralizing vision in which non-reproductive sexual practices and dissident bodies are conceived as threats to life, dignity, and the national project (López, 2023, p. 19). This contributes to the construction of restrictive legal frameworks and fuels hate speech that legitimizes symbolic and physical violence, with serious implications for freedom of expression and sexual and reproductive rights.

In 2023, the presidential ticket of Bernardo Arévalo and Karin Herrera represented an alternative to decades of institutional co-optation. Upon taking office, Arévalo and Herrera encountered dysfunctional institutions, widespread corruption, superfluous spending, ghost employees, overpriced projects, rigged contracts, and precarious public services in areas such as health and education (Monzón, 2024, p. 35). Guatemala remains in a context of institutional weakness and distrust in the justice system. With one year remaining in Bernardo Arévalo's term, the struggle for change continues. Patterns of criminalization, surveillance, judicial harassment, and attacks against human rights defenders persist, particularly affecting Mayan leaders and women human rights defenders.

1.2. Overview of the Guatemalan Digital Context

The rapid expansion of Guatemala's digital environment has profoundly reconfigured ways of being, communicating, and engaging in political discourse. In a context of persistent technological inequality, increasing online violence and moralizing offensives seek to discipline bodies and sexualities, particularly those of women and gender and sexual minorities. Digital democracy refers both to a political system and to a culture of participation in which digital technologies and online spaces can either hinder or facilitate inclusive democratic participation and civic engagement.

The "virtual space" should function as a platform for access, expression, and oversight, allowing people to become informed, express demands, and mobilize support around public issues (Congge et al., 2023). When such spaces are appropriated by contemporary non-traditional social movements, such as feminist and LGBTQI+ movements, the *Hashtagora* takes shape: a democratic

agora produced within the virtual environment, where new ways of thinking about democracy emerge not merely as representation, but as a form of society in which violations and demands can be made visible and the right to voice and presence in the public sphere is expanded (Olmedo and Taylor, 2025).

At the same time, the expansion of Guatemala's digital environment does not guarantee digital democracy, given the country's deep socioeconomic and gender inequalities. According to Kemp (2025), at the beginning of 2025, the country had 20.4 million mobile cellular connections, a figure higher than its total population. However, only 11.3 million people—60.8% of the population—had internet access, while 7.28 million remained disconnected (39.2%). Participation in social networks was also significant: there were 10.4 million active user accounts, equivalent to 56.1% of the total population and 89.2% of the adult population over 18 years of age.

These figures demonstrate not only the widespread reach of internet access but also the centrality of digital platforms in everyday life. In January 2025, 92.3% of internet users were active on at least one social network (Kemp, 2025). However, gender gaps persist: of all social media identities, 43% were attributed to women and 57% to men, pointing to an initial gender inequality in access, use, and digital power. Specific statistics on the use of digital platforms by gender and sexual minorities are not available. This distribution across digital platforms reveals distinct patterns of digital socialization that influence both forms of violence and political participation.

Social media platforms are not merely spaces for interaction; they constitute political arenas of struggle in which violence is expressed, narratives are contested, and symbolic political battles are waged through regulation, surveillance, or direct attacks on dissenting bodies. The democratic quality of the digital sphere depends on digital civic knowledge and ethical standards capable of countering disinformation, hate, defamation, and other forms of online aggression (Congge et al., 2023).

With regard to these attacks, Initiative 6280, the Law Against Digital Sexual Violence, offers an initial legal definition. It defines digital sexual violence as any action carried out through digital platforms or information technologies that violates a person's integrity, dignity, privacy, and sexual freedom, causing psychological, physical, economic, or moral harm to the victim and their family (Initiative 6280, 2023). This formulation recognizes the specific nature of online harm and its connection to physical and structural forms of violence.

In 2024, digital attacks reached critical levels. UDEFEGUA (2025, p. 21) documented 3,501 digital attacks attributable to netcenters. Netcenters were defined as “a set of accounts connected directly or indirectly, physically or virtually. Their users may include accounts of real people, real institutions, fake profiles of people, fictitious institutions, and users with names and photographs (IDs) stolen from real people” (CICIG, 2019, p. 3).

These organized digital communication structures are identified as the main perpetrators of digital attacks in the country, surpassing state actors and common criminals. Netcenters operate by professionalizing harassment, disinformation, and intimidation, creating a digital warfare machine whose objective is to silence, wear down, and delegitimize critical voices, especially those of feminist movements, independent journalists, and human rights defenders. They operate primarily on social media platforms such as Twitter/X and Facebook, manipulating public conversation by functioning as “disinformation networks” (CICIG, 2019, p. 5) and employing a modus operandi similar to that of “hitmen” (CICIG, 2019, p. 19).

1.3. Forms of Digital Violence Against Women and Sex-Gender Dissidents

The forms of digital aggression vary by territory. UDEFEGUA (2025, p. 20) notes that in urban contexts, aggression on social media predominates, including defamation and public stigmatization; while outside the capital, violence tends to be more direct, combining digital threats with physical harassment. This territorial differentiation reveals the coexistence of multiple forms of violence in which digital and physical spaces reinforce one another.

Digital violence also extends into the private sphere, where it can be used to undermine networks of affection and personal relationships. This has led many women human rights defenders to abandon their work for fear of reprisals against those closest to them (UDEFEQUA, 2025, p. 27). This form of violence illustrates how digital attacks can produce isolation, self-censorship, and the breakdown of community ties.

Digital violence is also widespread on social media. Tello (2024, p. 71) reports that Facebook was the platform on which the highest number of complaints were registered in 2023. This is consistent with patterns documented by the International Center for Not-for-Profit Law (2024), which notes an increase in complaints involving identity theft, sexual harassment, and defamation on the platform.

Women often respond by blocking aggressors' profiles or reporting accounts used for harassment, although these measures have limited results (Tello, 2024, pp. 81–82). Exposure to violence, however, is not incidental. Tello (2024, p. 63) shows that many women experience the same type of aggression repeatedly, indicating a pattern of recurrence that compounds emotional and social harm. Digital violence therefore does not operate as a series of isolated incidents but as an interconnected ecosystem of aggression.

The intersection between “general digital violence” and “gender-based digital violence” (Tello, 2024) is particularly evident in attacks against women human rights defenders. UDEFEQUA (2025, p. 26) shows that the most common forms documented in 2024 were stigmatization (979 cases), defamation (388), harassment (246), and threats (49), revealing a systematic pattern of aggression aimed at inhibiting their public and community participation.

From an intersectional perspective, the multiple identities and social positions of women human rights defenders in Guatemala—including ethnicity, territory, generation, class, sexual orientation, and gender identity—shape their exposure to violence in different ways, increasing the risks faced by those already in structurally disadvantaged positions (Tello, 2024, p. 19).

The cross-cutting nature of their roles as community organizers, candidates for elected office, advocates, and leaders of social initiatives broadens and complicates the contexts in which they may be exposed to violence. Aggression can originate in both institutional settings and digital spaces, including social media, and it can also take the form of judicial criminalization or defamation campaigns within communities, creating a hostile environment that seeks to delegitimize and silence their work (UDEFEQUA, 2025, p. 27).

Sex-gender dissidents face specific forms of digital violence that combine structural discrimination, hate speech, and mechanisms of moral policing. In a sample of 290 participants, online harassment affected 21.35% of cisgender LGBTQ+ people and 31.82% of transgender people; overall, 22.15% reported having experienced online harassment (López, Batres, and Martínez, 2020, p. 39). “Derogatory humor” is another common and normalized form of digital violence. According to Johnson and Deutch (2024, p. 66), homophobic or racialized jokes function as vehicles for disseminating hate speech without direct accountability, reinforcing stigma and legitimizing more explicit forms of violence.

The impact is even more pronounced in rural contexts. Johnson and Deutch (2024, p. 67) document cases of LGBTQI+ individuals who, after receiving threats via WhatsApp or Facebook, left their communities for urban centers out of fear of physical attacks. This shift from digital threats to territorial displacement illustrates the depth of intersectional violence, in which digital space, gender, sexuality, race/ethnicity, and territory intersect to create extreme conditions of vulnerability.

The continuum between online and physical violence also operates through state criminalization. The IACHR (2024, para. 37) documents the judicial persecution of community and Mayan journalists in Guatemala, including the abusive application of the crime of “utility theft” (*hurto de fluidos*),¹ raids involving work equipment,

¹ Penal Code, art. 249. Utility theft (*hurto de fluidos*). The provision criminalizes the unlawful taking of electricity, water, gas, power supplied by an installation, or other utilities belonging to another person. The offense was traditionally punishable by a fine, but in 2023 Congress amended the provision (Decree 8-2023) to introduce imprisonment and higher fines, as well as aggravated penalties when the offense is committed by organized criminal groups or through illegal connections (Congress of the Republic of Guatemala, 2023).

and criminal proceedings used as punishment for reporting on issues such as environmental degradation caused by monocultures and mining, community evictions, forced displacement, lack of humanitarian assistance, excessive use of public force, and illegal economies in ancestral territories.

1.4. Institutional Framework, Public Policies, and Protection Gaps

The Guatemalan State's response to technology-facilitated gender-based violence is marked by a significant gap between the existing regulatory framework, international human rights obligations, and institutional practice.

Although Guatemala has laws aimed at preventing and punishing violence against women, these laws were designed for analog contexts and do not explicitly address the specific forms of aggression facilitated by digital technologies. This omission creates a protection gap in which online violence remains insufficiently addressed, often rendered invisible or normalized by the institutions responsible for its prevention, investigation, and punishment.

In the area of women's rights, Guatemala has a body of legislation that, in principle, should provide robust protection. Article 6 of the *Law for the Dignification and Comprehensive Promotion of Women* requires the State to establish policies and mechanisms to prevent and eradicate discrimination and violence against women and to promote their comprehensive development.

The *Law against Femicide and Other Forms of Violence against Women*, for its part, establishes in Article 3 a broad definition of gender-based violence, encompassing physical, sexual, economic, and psychological harm, as well as threats, coercion, and deprivation of liberty in both public and private spheres. In addition, the *Law against Sexual Violence, Exploitation, and Trafficking in Persons* seeks to prevent, punish, and eradicate sexual violence and to guarantee care and reparations for victims.

However, these laws have significant limitations when applied to forms of digital violence. None specifically addresses online forms of aggression such as cyberbullying, smear campaigns, the exposure of personal data, the manipulation of intimate images, or digital extortion, nor do they establish specialized investigative protocols for technology-facilitated offenses. This regulatory gap leaves victims without clear reporting mechanisms or effective guarantees of redress.

At the same time, restrictions related to gender and sexuality promoted during the Giammattei administration are also evident. In 2021, the *Public Policy for the Protection of Life and Family Institutions 2021–2031* was approved, reinforcing a heterosexual and biologically defined model of the family. These measures function as instruments of reproductive reconquest insofar as they seek to redefine who may exist publicly as a rights-bearing subject. Women who exercise reproductive autonomy and sex-gender dissidents are treated as threats to the social order rather than as people entitled to full citizenship rights.

Institutional weaknesses in responding to digital violence are compounded by a lack of training and awareness among the authorities responsible for investigating these offenses. According to UDEFEGUA (2025, p. 23), one factor contributing to the spread of digital violence is the absence of specific legislation regulating offenses committed through technology. Police and judicial authorities also frequently trivialize online aggression, at times refusing to accept complaints because they regard them as merely “social media problems.”

Johnson and Deutch (2024, p. 69) report that, in countries without adequate legal protections, including Guatemala, police authorities often validate or minimize digital violence against sex-gender dissidents, treating it as irrelevant or justifiable. This institutional dismissal leaves victims in situations of heightened vulnerability while allowing perpetrators to act with impunity.

Paradoxically, while institutions may fail to protect women and sex-gender dissidents from digital violence, they can be highly active in using digital technologies as punitive tools against these same populations. Johnson and Deutch (2024, p. 75) document cases in which state officials use criminal legislation to explicitly target sex-gender dissidents through unauthorized surveillance of social media, the creation of fake profiles on dating applications such as Grindr, and the inspection of electronic devices without authorization.

This punitive use of the state apparatus reveals an institutional approach oriented toward controlling and monitoring dissident groups rather than guaranteeing their protection. Selective criminalization reinforces exclusion and increases the risk that digital violence may lead to judicial or administrative sanctions in contexts marked by high levels of discrimination and corruption.

Chapter II

“IT HAS GIVEN ME MORE STRENGTH TO SPEAK OUT AND REPORT IT”:

A NATIONAL ASSESSMENT OF DIGITAL VIOLENCE.



This chapter presents the experiences of a non-representative sample of 20 Guatemalan collectives and organizations that, for the purposes of this research, described the risks they face, as well as their practices and forms of resistance to technology-facilitated gender-based violence. The information they provided offers insight into some of the ways in which this form of violence manifests. It is important to emphasize, however, that the study does not seek to establish generalizations or identify broader trends in how technology-facilitated gender-based violence occurs in Guatemala.

The digital questionnaire addressed a series of research dimensions closely aligned with the study's analytical framework:

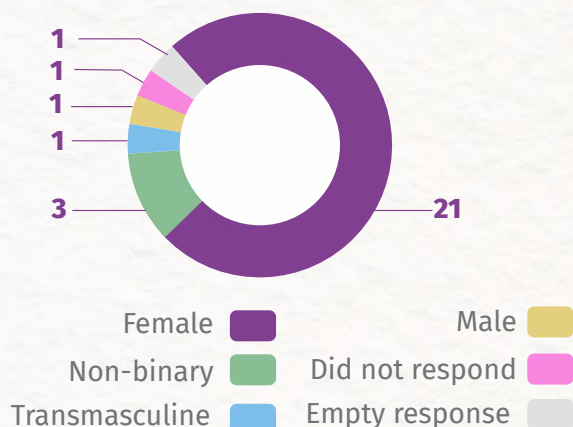
- » It gathered sociodemographic information and data on the use of digital platforms in order to contextualize inequalities in exposure and vulnerability within digital spaces.
- » It documented experiences of digital violence, understood as a factor that directly affects the quality of the online public sphere.
- » It included a section on individual self-care strategies in response to such violence.
- » It documented collective action strategies and forms of political resistance.
- » It included a dimension focused on identifying risks and challenges related to digital democracy in Guatemala.

The following section summarizes the responses received.

2.1. Demographic data and use of digital platforms

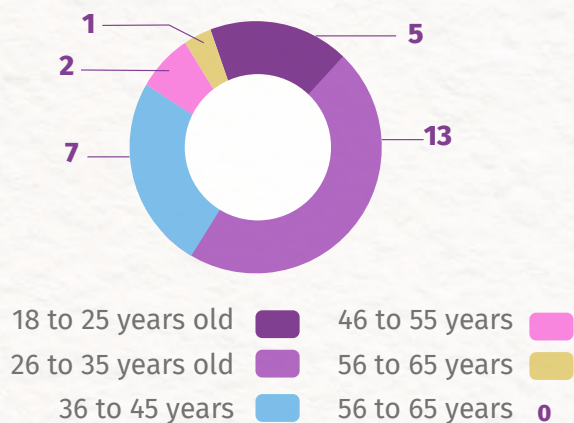
Demographic data

a) Composition by gender identity
(28 responses recorded)



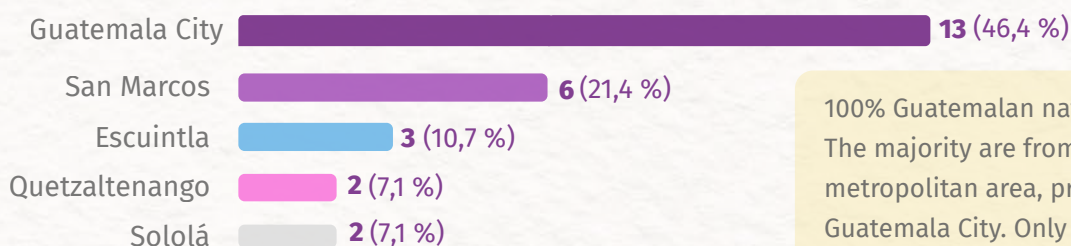
Female predominance with a moderate presence of diverse identities. There were no responses from trans-feminine or agender individuals, nor in the "other" category.

b) Distribution by age range



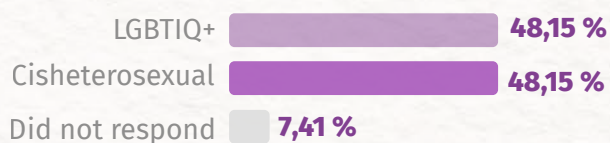
A predominance of young and middle-aged women, with few voices from older and younger generations.

c) Geography and nationality

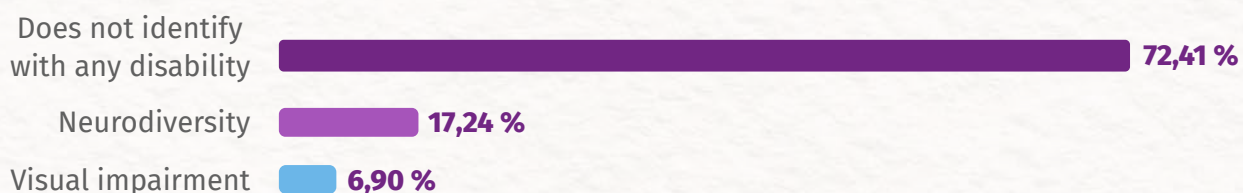


100% Guatemalan nationals. The majority are from the metropolitan area, primarily Guatemala City. Only one person resides in a rural area.

d) Specified gender identity



e) Disability status



Use of digital platforms

Relationship with Technology and the Digital Divide:

The results reveal varying levels of familiarity with technology and internet use among participants. While the majority (22 out of 28) reported feeling very familiar with technology, a smaller group identified challenges and limitations:

- » 10 participants reported difficulties using digital platforms.
- » Two participants reported restricted access.

These findings point to a potential digital divide that may affect some participants' ability to engage fully in technology-based activities.

Use of Mobile Phones and Computers:

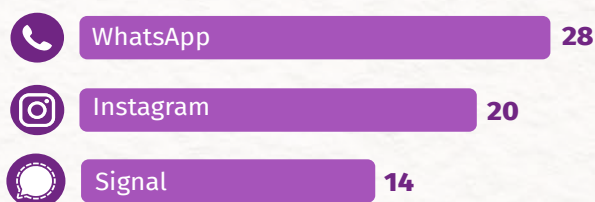
Mobile phones (27 participants) and computers (25) are the primary devices used to access the internet. This preference may influence the design of digital activities and resources, particularly by prioritizing platforms that are compatible with these devices. At the same time, it is important to consider ways to expand the use of other devices, such as tablets (6 participants), in order to diversify connectivity options.

Internet usage:

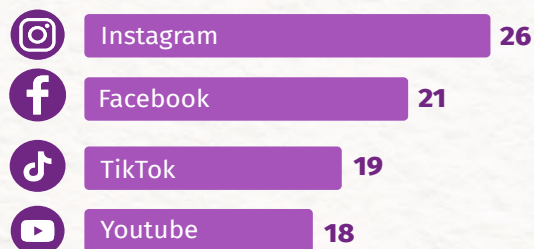


"It Has Given Me More Strength to Speak Out and Report It".

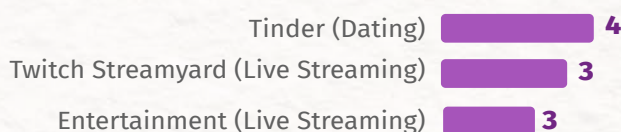
The most used messaging platforms and networks:



Most used social networks:



The least used platforms:



Majority preference for not using video game chats or specialized forums.

This indicates a strong preference for visual, fast-paced content platforms, particularly Instagram and TikTok. This pattern is consistent with national trends in platform use and content consumption, with TikTok reaching up to 89.2% of the population aged 18 and over (Kemp, 2025). Twitter (X) also remains relevant among participants (14), despite no longer being a dominant platform nationally (Kemp, 2025).

Hours per day spent on digital platforms:



This finding reinforces the importance of digital tools in participants' activism and in their daily lives. It also provides a basis for exploring proposals aimed at improving their online interactions and promoting the effective use of technology.

Most activists (21) manage multiple accounts across digital platforms, primarily as a way of organizing their online lives and activities. This highlights the importance of segmenting digital identities across activism, communication, and personal life. The various reasons for doing so—managing accounts for organizations they belong to (15); separating public, family, professional, educational, or work-related accounts from more private ones (13); maintaining backup accounts (5); and selling products (5)—reflect a strategic approach to participation in the digital sphere.

Changes Participants Would Like to See on Digital Platforms

The responses reflect a need for safer, more respectful, and more inclusive digital environments. Suggestions from respondents for promoting these changes include:

- » **Moderation policies** :*“monitoring of content [...] and closing [forums or chats] where sensitive topics are being shared” (Manhathan Bermúdez).*
- » **Control**: *“controls on hate speech” (Andromeda); “That all people who have access are of legal age” (Beatrix).*
- » **Reconfiguration of reporting mechanisms**: *“I would like them to implement faster and more accessible mechanisms to report digital violence” (Anonymous).*
- » **Security**: *“Applications automatically block this kind of [disrespect]” (Philita).*
- » **Restrictions**: *“Digital platforms prohibit any discriminatory, sexist, homophobic content” (Ryale).*
- » **Participants’ visions for the future converge around reducing digital violence and fostering a healthier online environment**: *“I dream of digital spaces where we can express ourselves” (Pau Pau).*

2.2. Digital Violence

Digital Attacks:

With 22 mentions, attacks classified as personal were the most prevalent, suggesting that respondents perceive these attacks as being directed specifically at them and their experiences. Personal attacks range from receiving suspicious messages (15) to physical harassment (9) and sexual harassment (11), as well as the dissemination of false or misleading information intended to cause harm (7) and disinformation related to participants' sexual and emotional lives (7).

Fifteen participants believe they have been subjected to attacks of a political nature, pointing to a connection between activism and the violent reactions it provokes among certain reactionary sectors of society.

Six participants reported experiencing between six and seven digital attacks. Proportionally, this represents 21.4% of the sample (6 out of 28), meaning that approximately one in five respondents experienced a pattern of attacks that extends beyond isolated incidents and approaches a sustained trajectory of harassment.

These are not isolated incidents but repeated attacks of the same type occurring on multiple occasions. This raises questions about where prevention mechanisms failed, where attacks were not contained or sanctioned, and where victims did not receive comprehensive support.

Attacks Against Sex-Gender Dissidents:

The prevalence of homophobic (8) and transphobic (9) attacks reflects a Guatemalan social context marked by resistance to recognizing sex-gender dissidents as full citizens. Transphobic attacks were concentrated among non-binary and transmasculine identities. This confirms that sex-gender dissidents

are exposed to a distinct pattern of online harm, in which digital gender-based violence operates with greater intensity than it does among their cisgender and heterosexual peers.

Most respondents (27, or 96.4%) believe that activists and prominent figures working on gender and LGBTQ+ issues are more vulnerable to digital violence. This perception highlights the importance of both context and the increased visibility associated with belonging to these communities. The absence of negative or undecided responses indicates a strong consensus among respondents regarding the risks associated with activism.

Areas Where Digital Security Attacks Are Most Frequently Experienced:

The survey shows that instant messaging platforms—Messenger/Facebook (17), Instagram (13), and WhatsApp (12)—and social media platforms—Facebook (12), Instagram (11), and Twitter/X (6)—are the spaces where digital security attacks are most frequently experienced. Attacks are less frequent on videoconferencing platforms, video game chat rooms, and online forums, suggesting significant differences in the levels of risk respondents associate with different types of digital spaces.

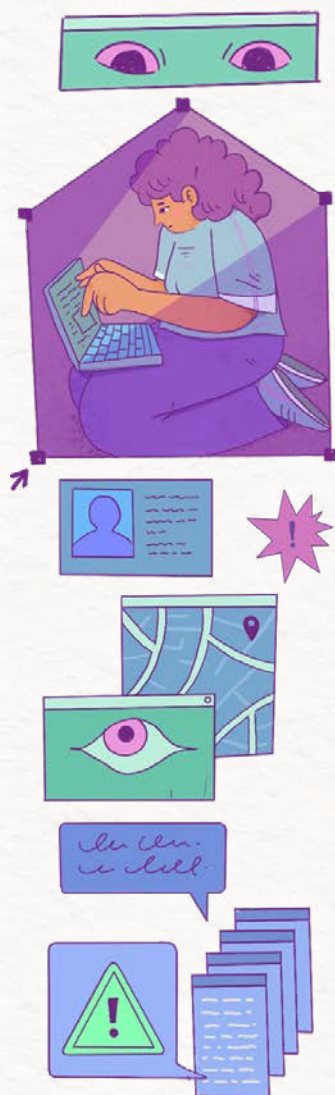
Attacks on Organizations

At the organizational level, the results point to a significant number of digital security challenges. Activists primarily reported discriminatory attacks (12) and the spread of misinformation (10), reflecting risks associated with their activism and public visibility. Suspicious messages linked to fraud attempts (8) were also reported, along with harassment (6) and the dissemination of personal information (6), highlighting vulnerabilities related to privacy and security.

Eighteen participants classified the attacks as organizational, indicating that campaigns targeting particular groups or movements can have collective effects and damage the reputation of organizations.

Some responses indicated that organizations had not experienced attacks (6), suggesting a degree of digital resilience. Other forms of aggression, such as identity theft, were not reported, suggesting that not all potential threats have materialized as attacks against organizations.

Origin of the Attacks



When asked about the identity of the aggressors, the most common response was that they were groups or individuals seeking to harm or disrupt the work of the organization (14), indicating a considerable threat from actors hostile to these organizations' missions.

Fake accounts were identified as a source of attacks by 12 respondents, pointing to a significant problem related to identity and authenticity on digital platforms. It is also noteworthy that respondents identified religious fundamentalist groups or individuals (8), as well as people seeking to harm others for personal reasons (8), as sources of attacks.

Regarding the characteristics of the individuals or groups responsible for the attacks, a significant number of respondents (12) were unable to identify the perpetrators. Among those who did provide an assessment, the predominant perception was that the attackers were older men (8), while women were identified less frequently. Most attacks were perceived as having been carried out by individuals rather than organized groups.

2.3. Effects and Impact of Digital Violence on Activists

Digital violence has had significant effects on respondents. Eleven reported emotional impacts, while a similar number said they felt monitored or unsafe, indicating considerable psychological distress. In addition, five feared for their physical safety, while others reported psychological problems, demonstrating that the effects extend beyond the digital sphere. Social impacts were also reported, including isolation from family (2), as well as physical and self-esteem-related effects (5), although these were less frequent. Only four respondents indicated that they had not been affected. Overall, the findings point to impacts across emotional, psychological, social, and physical dimensions.

After experiencing online violence, the most common response was to block profiles perceived as unsafe (19) and to report or block accounts (14), followed by making accounts more private (11). Some respondents sought support from friends or feminist networks (5), while others filed formal complaints (3). Emotional crises and pauses in activism were also reported (3). A small number left digital platforms (1) or created new accounts (1), while one respondent said they did not know how to respond. One participant described the impact as follows: *“I stopped being an activist, only working in the organization in a nearly secretive way”* (Florencia Rockera), reflecting the profound effects digital violence can have on activism.

Digital violence has also limited the participation of several activists: six stopped participating in certain spaces, while seven reported negative effects on their mental health, indicating a substantial emotional impact. Relationships within activist spaces were also affected (5), creating obstacles to collaboration. More drastic consequences were less frequent, including avoiding leadership positions (2) and closing accounts (1).

The open-ended responses reflect a wide range of experiences with digital violence, from strength, *“It has given me more strength to speak out and report it”* (Chocolate), to insecurity, *“I’m more cautious about what I share”* (Luna). They also show how fear has led some participants to limit their use of social

media, affecting both activism and personal relationships: *"By having to close my account, I lost access to my organization's account"* (Anonymous).

In response to digital violence, most participants sought support from people in their close networks, particularly family (13) and friends (14), who emerged as their primary sources of emotional support. They also turned to other activists (9) and members of queer and feminist communities (4), underscoring the importance of support networks within activist spaces. Support from partners was also significant (7), while only a small number sought help from institutions (3), indicating low levels of trust in formal support mechanisms. Four participants did not speak to anyone, suggesting isolation or fear of disclosing their experiences. Finally, three indicated that the question did not apply to them, possibly because they had not experienced digital violence or had not yet identified their experiences as such.

When asked directly whether they had reported the digital violence they experienced, only a small number of participants had done so (4), compared with those who had not (18), indicating a low propensity to report and possible distrust in the effectiveness of existing mechanisms. Among those who did report, only 50% obtained a satisfactory outcome (2), reinforcing the perception that these processes do not function effectively. The number of participants who indicated that the question did not apply remained consistent (4).

The most common self-care practice in response to online violence was muting, blocking, or filtering aggressive accounts (17). Limiting the use of certain platforms (13) and receiving digital security training (13) also emerged as significant practices, reflecting a combination of technical and behavioral strategies. Nine participants sought emotional or psychological support, while four took scheduled breaks from digital spaces. Only three indicated that the question did not apply because they had not experienced attacks. Open-ended responses also mentioned additional measures, such as *"changing passwords and enabling two-step verification"* (Anonymous).

2.4. Impacts on Organizational Culture and Political Resistance

The results show that, while there is widespread recognition of technology-facilitated gender-based violence within organizations, the ways in which it is discussed and addressed vary considerably. The most common approach is the discussion of personal experiences (21), alongside more formal institutional spaces such as work meetings or assemblies (16). Informal meetings or everyday conversations (14), workshops or specific training sessions (14), and public campaigns or actions (11) are also prominent. A small number of respondents indicated that the issue is not addressed in any space (2), while isolated cases are mentioned without further analysis (4).

When examining the effects of digital violence on the internal functioning of organizations and collectives, the most frequently reported response was the modification of internal security protocols (15). This was followed by increased stress, exhaustion, or emotional strain (12), reduced participation among members (9), and distrust or fear surrounding the use of certain platforms (8).

In response to these challenges, organizations placed an active emphasis on political resistance in digital environments, particularly through the creation of safe spaces. Among the most prominent practices were emotional support among members (20), the redistribution of tasks to reduce emotional overload (13), the identification of secure communication channels (12), internal support and response protocols (11), and support networks with other organizations (10).

Perceptions of the effectiveness of care strategies indicate that, despite the challenges they face, activists are finding ways to support one another. This underscores the importance of solidarity and innovation in responding to technology-facilitated gender-based violence.

Collective responses to digital violence are also framed around the creation and dissemination of counter-narratives. This is reflected in public or communication

campaigns (11) and in the production and dissemination of educational materials (11). Also noteworthy is the coordination among organizations through the establishment of alliances (13), political or legal advocacy (7), and coordinated mutual-support responses (4). As in the individual sphere, there is limited interest in filing complaints against digital platforms (4). This can be explained by the absence of specific legislation addressing this type of violence, as well as distrust in the justice system due to its institutional biases and the perception that it constitutes a dangerous space for feminist women and sex-gender dissidents.

Political resistance practices carried out by organizations in digital environments include the creation of safe digital spaces (19), counter-narrative actions (12), artistic or creative interventions (11), the reappropriation of hashtags (8), and the strategic use of anonymity (4). These practices were assessed as somewhat effective (15) or highly impactful (8). These assessments reflect the fact that, although the practices implemented do not eliminate algorithmic manipulation, they help expand the scope for action needed to sustain everyday forms of democratic participation.

With regard to the obstacles to sustaining collective action, the findings show that digital resistance is constrained by asymmetries in capacity, infrastructure, and care. These include a lack of human resources or time (16), insufficient technical resources (14), emotional exhaustion among team members (14), and fear of an escalation in violence (6). These obstacles help explain why many strategies are considered only "somewhat effective": not because they lack relevance, but because the conditions required to sustain them remain fragile.

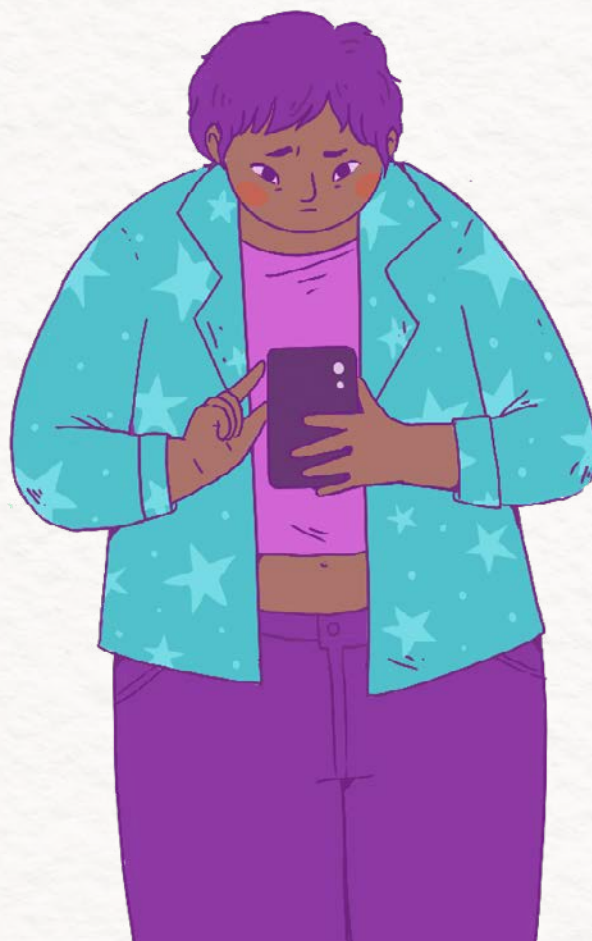
The challenges identified depict a context in which digital political participation is constrained by limited digital literacy within communities (18), a lack of safe spaces for deliberation (17), insufficient human resources (17), economic limitations (16), technological limitations (15), fear of digital reprisals (14), limited coordination with other organizations and activists (12), and obstacles to disseminating reliable information (10). Taken together, these findings suggest that strengthening digital political participation requires understanding digital

democracy as a system of capacities. Simply “being” on social media is not enough; people must also be able to exercise full digital citizenship.

Views are divided regarding the extent to which digital environments can foster fair democratic participation. While one group identifies potential benefits, another expresses skepticism and distrust, highlighting the need to address existing concerns in order to strengthen digital democracy.

Seven respondents expressed confidence that digital environments enable fair democratic participation, indicating a positive base of support. Another nine believed that participation is only partially fair, suggesting that, although they recognize positive aspects, they also perceive limitations and concerns. At the other end of the spectrum, eight respondents expressed little confidence that fair participation can be achieved, reflecting doubts about the effectiveness and fairness of digital environments.

Perceptions of the future quality of digital democracy are similarly divided. A small group expects improvement (7), while another expresses concern about its deterioration (9). Three respondents believe its quality will remain unchanged, indicating that they anticipate little change in either direction. Seven participants did not provide an answer. Taken together, those who expressed a negative outlook, did not anticipate change, or did not express an opinion amount to 19 participants. Discursively, this can be interpreted as a sign of narrowing expectations and structural opacity within the sociopolitical environment. This is not simply a matter of



individual indecision or pessimism; it reflects a climate in which the future is perceived as blocked or difficult to anticipate.

In short, state capture and the reinstatement of privileges of feudal-colonial origin produce a social horizon in which expectations of transformation weaken and citizens experience the public sphere as less legible, less open to contestation, and more heavily conditioned by powers operating beyond democratic scrutiny.

The next chapter examines in greater depth how, within this context of opacity in the public sphere, technology-facilitated gender-based violence operates as a mechanism of exclusion that directly affects the participation of women and sex-gender dissidents in democratic culture.

Chapter III

“ALGORITHMS AREN’T NEUTRAL”:

TENSIONS AND CONSEQUENCES OF DIGITAL VIOLENCE
FOR DEMOCRATIC CULTURE.

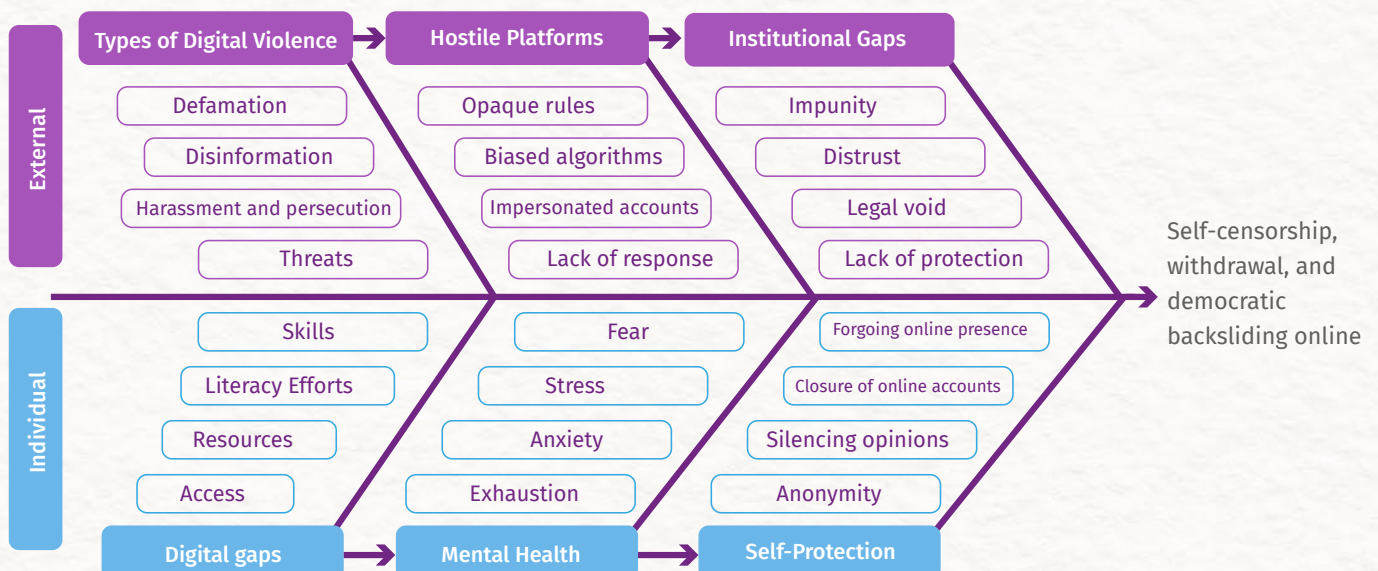


This chapter examines how technology-facilitated gender-based violence directly affects the public participation of women and gender and sexual minorities, from its impact on those who resist it to the political effects it generates within the online public sphere.

Drawing on the voices and experiences of the interviewees, the chapter proposes a model of technology-facilitated gender-based violence in Guatemala (Figure 3.1). This model is organized around two dimensions: the individual and the external. The individual dimension refers to people’s agency in relation to digital access and literacy, as well as to the various forms of self-protection they have identified, including lowering their profile, closing accounts, leaving platforms, and modulating their language.

The external dimension encompasses forms of aggression, hostility, and violence, intensified by the limited responsiveness of digital platforms and by institutional gaps in regulation, research, and support, all of which are further compounded by territorial inequalities. The interaction among the various elements within these two dimensions operates as a set of mechanisms that undermine freedom of expression, political participation, and democratic pluralism online. In this context, self-censorship and digital withdrawal among women and gender and sexual minorities in Guatemala cease to appear as isolated individual decisions and instead emerge as a structural condition.

Figure 3.1. Model of Digital Violence in Guatemala



Source: Virtual interviews.

3.1. Online Violence and Hostilities

In the everyday practice of digital activism, participants describe a contested terrain in which online violence is not confined to the symbolic realm but can escalate and reshape the material lives of those who defend rights.

Misidente: For us as an organization, exposing ourselves and identifying ourselves on social media means exposing ourselves within our community. [...] They were saying, “Women who dress in drag used to only go out at night, and now they dare to go out during the day too.” I remember someone commenting that when they saw us on the street, they were going to run us over [...]. For at least three months, we tried to go out as little as possible. How is it possible that, besides taking away our digital space, they are now also restricting our physical space, again!

Malinche: My Twitter handle has nothing to do with me; I don’t have profile pictures, everything is closed, it’s private... I know a friend who was fired from her job because of the things she tweeted. It was literally something HR didn’t tell her directly; they just said, “We saw your Twitter and decided you had to leave.” So I admit that I’m afraid of how my feminism and activism might be perceived in professional settings. I do make an effort to keep those parts of my life separate.

GA: Suddenly, some posts that were directly targeting our media outlet included the “white van” emoji, the vehicle used in the 1980s to abduct and disappear people, and the hashtag #panelblanca [white van].

Trixie666: If a woman decides to speak out about any kind of violence, we see that the first thing that happens is that most of the comments come from men and are insults. These are very serious things. It goes far beyond simply disagreeing with a point of view; it becomes insulting and degrading the person, even creating fake images or going to their profiles to mock them... As soon as a complaint is made or these comments are exposed publicly, there is a backlash from the people who made them, and they start saying things like, “So why are you posting this if you don’t want anyone to say anything to you?” And it’s like, “No, it’s not that I don’t want people to say anything to me; I want you to stop insulting me.”

These testimonies demonstrate that the digital realm is not an “outside” separate from the social sphere, but a threshold through which access to public space can be restricted and threats normalized as a disciplinary technique. Along these same lines, public visibility becomes a distinct risk factor, particularly for activists who make themselves visibly identifiable in social media campaigns.

Taken together, the testimonies allow us to understand this persecution as a form of selective violence directed at identifiable and highly exposed bodies, linking digital attacks to dynamics of surveillance, harassment, and potential offline escalation, particularly in territories outside the metropolitan center. In this regard, **(GA)** states:

Some have already been targeted, especially if they are very vocal or have a strong presence on social media; therefore, they experience these attacks more frequently. Many of them prefer not to express their opinions anymore. They prefer not to post; we can’t measure it, but there is a setback in the “democratization” of freedom of expression on social media, because those who are attacked most often choose to become more anonymous or maintain a much less public profile.

3.2. Digital Platforms as Hostile Territory

Participants’ accounts reveal a persistent perception of digital platforms as ineffective in responding to reports of violence. This generates frustration and forces organizations to manage and contain the resulting harm largely on their own.

*[...] Regarding the march here in June, this happens quite often to trans women. When they post that a trans woman has been murdered—most of these cases are motivated by hate—some people start mocking them, using male pronouns, and so on. Even when it is reported, it is very difficult for these platforms to do anything, to have protocols in place, or to respond to the reports. It has taken us quite a while to get certain content taken down and certain profiles reported. **(Trixie666)***

This points to a gap between the existence of formal mechanisms, such as reporting procedures, and their actual effectiveness in producing action. The result is a sense of structural inaction that prolongs exposure to harm and intensifies its effects. **GA** offers an interpretive lens for understanding why platform responses may be so limited:

The media needs to be present to reach a wider audience, but we know that algorithms are not neutral because they increasingly hide journalistic content, because people are more interested in seeing entertainment and happiness than news or information that may not necessarily be more enjoyable for them.

This observation helps explain the difficulty of removing harmful content or curbing attacks as part of a broader technical logic that privileges mass circulation while disadvantaging minority voices, reinforcing the perception that platforms do not function as impartial intermediaries. The effects of this form of intermediation therefore extend beyond the digital sphere into relational and organizational life.

*When the campaign was launched, the number of messages that started coming in was incredible; it seemed like the campaign only reached these people. It was really interesting to see how Meta is working there. So, we see another barrier, because we don't have much influence over how these platforms work. What have we tried to do? Well, for example, give some guidelines on how to post stories, and also how to respond to messages. Or simply not respond and delete them, because, to a certain extent, it can also be a waste of time. With our colleagues, we've sometimes tried to run workshops on self-care and feminist self-defense. **(Marta)***

Given the limited effectiveness of—or lack of response from—digital platforms when addressing online attacks, the burden of support falls on the collective, which accompanies those affected, provides emotional support, and seeks to repair politically and emotionally what the platforms fail to resolve.

3.3. Institutional Gaps, Impunity, and Failures in the Reporting Process

Closely linked to the lack of guarantees provided by digital platforms, technology-facilitated gender-based violence is also shaped by institutional gaps operating at multiple levels, including social recognition, regulatory frameworks, investigative capacity, and public policy. Taken together, these gaps contribute to the weakening of digital democracy.

Misidente identifies a fundamental starting point: “People don’t recognize digital violence as violence.” This lack of recognition not only renders the harm invisible but also limits the possibility of activating collective and institutional responses.

When violence is not recognized as such, social demands for protection are weakened and aggression becomes normalized as an “expected” feature of the digital environment. This leaves women and gender and sexual minorities more exposed and with less legitimacy to demand safeguards from platforms and protection from the State.

At the legal level, interviewees describe a clear regulatory gap resulting from the absence of specific legislation on digital violence:

While there have been attempts to create commissions or laws to address this type of discrimination, both physical and digital, the State offers very little protection. If someone files a complaint, it’s not followed up; they claim it’s due to a lack of information or that there’s no legal framework to regulate these kinds of violations. I haven’t seen a single case where a digital complaint has been successful. (Flor de Café)

There is a lack of institutional support and widespread impunity surrounding these online attacks because, at the national level, one of our biggest limitations is the absence of legislation regulating this issue from a gender perspective. For example, the proposed law on preventing sexual violence in the digital environment is certainly an achievement, but it’s important to remember that digital violence isn’t limited to sexual content. For instance, there’s identity theft,

doxing, hacking; the spectrum is much broader. It's quite complex when the Public Prosecutor's Office lacks a division with a gender perspective for understanding and addressing this violence. Furthermore, the lack of clear legislation means there are no public policies in place to address this issue. (Marta)

The testimonies indicate that the problem lies not only in the absence of regulation, but also in the absence of a regulatory framework capable of recognizing and addressing the gendered and sexual dimensions of this violence, its forms, and its impacts. The result is an institutional gray area in which acts of aggression remain without clear classification or an adequate framework for effective reporting, protection, and redress.

Participants identified another institutional gap within law enforcement responses to technology-facilitated gender-based violence. This gap begins with mistrust and is compounded by limited knowledge and training, ultimately resulting in insufficient support for those seeking to report violence or obtain guidance. At the core of the problem is a lack of both conceptual and practical understanding of gender-based violence in digital environments.

[...] It is sad to see how even the Ministry of Communications and SENACYT, the Secretariat of Science and Technology in Guatemala, are not trained in cybersecurity; they are unaware of the dangers involved and lack the infrastructure to ensure even minimally good quality internet access. These questions, while necessary, reflect a state that should have already overcome the basic challenge of connectivity, which Guatemala has not. If there isn't even internet access, I don't think they can ask what happens to people in cyberspace. (Malinche)

[...] They lack knowledge about technology-facilitated violence, they are unfamiliar with the terminology and the different types, but above all, they don't know what to do after someone approaches them. They don't know how to guide them or how to mediate the complaint. That's what's currently happening in law enforcement agencies, and it's something they told us: "We would really like you to come and train us, to strengthen our skills, because we don't know what to do

after someone approaches us, we don’t know how to guide them, and we don’t know how to mediate the complaint.” That’s what’s currently happening in law enforcement agencies. (Marta)

GA provides an example from the critical moment of filing a complaint: “They had no idea about Twitter, they had no idea about absolutely anything. We gave them the information, they had no idea about anything.” Taken together, these accounts describe an institutional void in which law enforcement lacks the language, categories, and basic competencies needed to recognize, classify, and understand the phenomenon. In practical terms, this means that technology-facilitated gender-based violence lacks an operational framework within these institutions through which it can be recognized and addressed as a form of violence.

3.4. Digital divides: structural vulnerabilities and inequalities

Technology-facilitated gender-based violence against women and gender and sexual minorities does not manifest uniformly; rather, its forms and intensity are shaped by whether it occurs in rural or urban settings and by the density of local community networks. This directly affects how violence is recognized, how it becomes “public” within the community, and how feasible it is to activate security protocols.

The testimonies point to a structural difference:

In an urban area, there might not be significant repercussions if a neighbor finds out something about another neighbor, but in other environments, the stigma created by the community based on what is circulating online is much more detrimental to the person facing this violence. **(Marta)**

In rural areas, social life is typically organized through close-knit networks: neighborhoods, kinship ties, churches, schools, local authorities, and others. This makes reputation both a central and a fragile resource. Here, the decisive factor is not only the *online attack* itself, but its immediate translation into a system of social surveillance: the community “finds out,” identifies, comments on, and punishes. In contrast, greater social segmentation in urban areas can provide some degree of anonymity or allow information to circulate in a more fragmented way.

A conflict of legitimacy also emerges, affecting both how violence is interpreted and how response strategies are received. **Malinche** describes a dynamic of *gaslighting*² and disavowal originating in rural sectors:

Often, it was people from rural areas, unaccustomed to encountering such discourses, who responded to the videos saying, “This isn’t true,” “This isn’t real,” “You’re talking about the women here, but you don’t know them.” That was the idea: “These are city women talking about things they don’t understand.”

These formulations function as a stigmatizing mechanism. Rather than engaging with the content itself, violence, rights, or security, the speaker is discredited on the basis of her presumed origin as a “city woman” and her supposed lack of understanding of the territory.

Security protocols therefore emerge as a necessary tool, but one whose effectiveness is conditioned by the territory:

We hope that the protocol we’ve supported can be useful in some way to fill that existing gap. Another challenge is the delegitimization that feminist organizations face, as well as adultcentrism, which seeks to silence those outside of those conservative patriarchal power structures. (Marta)

The central point highlighted by these testimonies is that digital violence is not simply a technological event; it is a social practice whose intensity increases

² Gaslighting: An expression referring to a form of emotional violence in which one person manipulates another into doubting their own perceptions and questioning their sense of reality.

or decreases depending on the type of community that receives, reproduces, or sanctions it.

Gaps in Access, Resources, Literacy, and Skills

Based on the testimonies gathered, gaps in *access, resources, literacy, and skills* do not appear as neutral contextual conditions, but as factors that stratify digital democracy. They determine who is able to access information, deliberate, organize, and demand accountability online, and who is excluded or able to participate only under precarious conditions. In Guatemala, this inequality is reflected in the significant proportion of the population that remains disconnected, as well as in internet access that, even when available, is often intermittent, expensive, and geographically concentrated:

Guatemala is a very unequal country. There are people who definitely don't have internet access. Perhaps 70% of the population has internet access, and of that percentage, most have to speak Spanish because there are no websites or platforms, and not even IDNs, to create URLs with Mayan or Xinka characters.
(Malinche)

[...] For community leaders, for example, when you buy a mobile data package, WhatsApp is often included for free. So it makes more sense to keep communicating through WhatsApp and to keep the groups there rather than, for example, installing Signal. Signal apparently uses more data, and once your data runs out, you can no longer use it. **(Trixie666)**

[...] Internet access is concentrated in departmental capitals and the central region. Inequalities in the exercise of the right to internet access become even more pronounced when we consider access to technology itself, and this gap exists in both rural and urban areas. In some households, for example, a single device or phone may be shared among several family members, which creates a number of limitations. Having less access to technology certainly does not mean that people are less likely to become victims of an attack. On the contrary, it can make them more vulnerable because they have less access to information and less knowledge about how technologies are evolving. **(Marta)**

The testimonies indicate that the digital public sphere tends to be constructed from areas with greater infrastructure, leaving peripheral communities with a form of low-intensity digital citizenship.

In addition, several constraints directly affect democratic deliberation:

- » **Linguistic mediation:** “People with internet access are often forced to have online experiences that aren’t in their mother tongue” (Malinche), limiting understanding, appropriation, and participation among communities whose first language is not Spanish.
- » **Lack of resources:** “Many leaders don’t even have a computer and work only with their personal phone” (Trixie666).
- » **Digital literacy,** including access to information and the ability to navigate and interpret content-saturated environments:

One issue that young people have been raising a lot is artificial intelligence. As usual, there isn’t enough information, and even when information is available, we don’t always know how to access it, especially from a community perspective. We’re seeing two extremes: either people are very afraid of it, or they’re using it irresponsibly. I think we can encourage more responsible use, because AI is already here, it exists, and it is a tool. We also want to make a real effort to better understand how artificial intelligence works. And I think it’s something we will inevitably have to engage with, talk about, and name. (Misidente)

Marta frames this as a problem of cognitive justice: “This lack of digital and technological literacy seems quite serious to me, because we start from a context in which not everyone has access to the same information, or to information in an accessible language.” **GA** adds the framework of “media and information literacy.” In the context of digital democracy, this is important because deliberation depends on the ability to understand, verify, and contextualize information. When these skills are distributed unevenly, the risk increases that public discourse will be captured by disinformation, manipulation, or hate speech, while citizens’ capacity for oversight is weakened.

3.5. Impacts on Mental and Physical Health

Digital violence is not separate from the body. On the contrary, its effects on activists’ mental and physical health constitute a central dimension of these forms of aggression.

This is something our research allowed us to see, including the way these attacks operate. They are not necessarily directed at the activist herself. Often, they may begin by targeting a family member or even a partner, precisely because of the impact this can have on her. The intention is ultimately to cause harm that can have serious consequences for the person’s mental health. (Marta)

From this perspective, emotions become an important analytical field for understanding how aggression seeks to disrupt relationships and spaces of support, undermine the continuity of activism, alter perceptions of safety, and produce bodily consequences that, over time, erode the capacity to sustain collective action.

The experience of shock and alarm is clearly reflected in **Trixie666’s** account of extortion and threats involving her digital identity:

Around that time, they called me and said, “Am I speaking with Trixie666?” And I said, “Yes?” The person said, “Oh...” The voice was male and quite friendly. When he asked for my name and then also used Trixie666, I thought it must be someone close to me, or someone who knew me. Then he started saying, “Listen, girl, I’m going to kill you if you don’t transfer this much money.” Of course, I froze when that happened. I just stayed quiet and listened. Then he started repeating information I had put on my [missing] cat poster: “I know you live near such and such. I know you hang around here; we’re watching you.” And I thought, “Oh! That’s the information I put on the poster.” Then they said, “We’re going to post your pictures,” and I was like, “Okay, go ahead,” because I knew my social media profiles were completely private, I didn’t have any public photos, and there were very few pictures of me. So it was pretty obvious that it was just a threat. Even so, it scared me quite a bit because it meant that someone close to me had done it.

Frustration emerges as a direct challenge to activists' ethical and political identities. **Flor de Café** describes this through the tension between the desire to separate the personal from the professional and the material impossibility of doing so when attacks are moralizing and delegitimizing:

[...] There was a time when we launched a campaign without having this set of responses in place, and after receiving them, I think we did notice a change, both in the number of hateful responses we were receiving and in the team's composure, which is something we really need to maintain. Because it's inevitable to feel frustrated, to feel personally attacked, no matter how much you try to separate your work from your personal life. It directly affects our morals, our ethics, and the things we believe in and fight for. It's inevitable that it affects us deeply. The community manager, in particular, had very strong feelings about it.

Marta expands on the cumulative effects of this pressure on the body:

Being exposed to violence leads to psychological and emotional distress. This, in turn, triggers other problems, such as sleep deprivation, anxiety in public, poor eating habits, and then health issues begin to emerge. Anxiety itself can also cause physical health problems. I think this was something that really affected us: realizing that it's not just about calling it digital violence, but about understanding all the effects of that violence. This includes self-censorship in digital spaces, but also all the implications for a person's daily life, their community networks, and the stigma that can emerge within the community itself.

Fear is explicitly framed as a legitimate part of the emotional repertoire in response to threat and as evidence of the disciplinary function of violence. Misidente describes it this way: “[...] consciously exposing ourselves to something we knew would eventually come. Second, it has also intimidated us. And we’ve named fear as something we experience too, recognizing that it is valid to feel fear, anguish, and anxiety.”

Here, fear ceases to be abstract. It becomes linked to the possibility of physical harm and to the extension of risk into close personal networks, showing how digital violence expands its radius of impact and produces relational vulnerability.

In response to these impacts, organized efforts have emerged to restore agency and sustain continuity. **GA** expresses this through an institutional decision that serves as a counterweight to the imposed logic of silence: “Are regards our publication, our editorial position is to continue doing the journalism we do and not stop publishing because of this hostile environment.” This response does not dismiss the effects on mental health, fear, or burnout. Instead, it points toward persistence, framing the continued production of public-facing work as an act of resistance even when the psycho-emotional cost is high.

3.6. Self-Protection

In the everyday practice of digital activism, strategies for containing violence are developed within a context of constant tension: energy that would otherwise be directed toward social transformation is diverted toward self-protection, defense, and risk management. This reallocation of resources is not marginal; it reshapes priorities, alters work rhythms, and forces collectives to make security a central political concern. Within this context, participants describe self-protection practices that do not eliminate violence but seek to reduce its impact, prevent its escalation, and preserve their capacity for action.

A first layer of containment involves visibility. **Misidente** describes it as a concrete strategy for reducing risk:

Once we recorded ourselves and uploaded some videos, a friend of ours was recognized at work. It was a really intense experience because, obviously, it wasn’t intentional, but it did draw attention to him, and it became a really big issue. So we said, okay, how do we avoid this kind of thing? Because our friends want to talk about it. What do we do? That’s when we started showing our faces less often. We began creating more images and other types of content instead.

This adjustment in the management of public exposure reflects the role of the face as a means of identification that can facilitate doxing³ and targeting. Reducing

³ Doxing: The non-consensual disclosure of a person’s private, personal, or sensitive information —such as their home address, email address, telephone number, or the contact details of family members or employers— with the intent to cause physical harm.

visibility, therefore, can sever or weaken the connection between a digital attack and a person's offline location. It does not amount to withdrawing from the public sphere, but rather to negotiating vulnerability.

Activists had also previously adopted other defensive anonymization strategies, such as using anonymous public profiles (**Malinche**) and keeping personal social media accounts private (**Trixie666**). These practices make clear that, in certain contexts, sustaining activism requires separating identity, image, and digital footprint.

A second layer of self-protection involves the separation of spaces and control over access. **Marta** and **Flor de Café** describe internal discussions and measures aimed at restricting audiences and reconfiguring the circulation of personal and institutional information:

[...] On the website, we had a section listing the names of all the board members. So we thought that perhaps some information had been leaked, so we took that information down; we removed it. Even so, information about those coordinating fieldwork or holding coordination roles is still exposed. And then there is the visibility of the work itself, because I think organizations also use that as a tool for credibility, right? Self-managing projects is so difficult that we have to seek donors and partners, and that credibility is built, in part, through the information we share, for example, on Instagram or LinkedIn. So there, once again, we are exposed. (**Marta**)

*It happened to me: they published a fake story about me, and I didn't know who to turn to. That led us to question how real the damage and consequences could actually become. There are so many journalists in exile, and you always wonder, "Is it really worth expressing myself on social media? The consequences for me could be extremely serious, and there may be no way to defend myself." We've discussed this internally: the possibility of having private or closed accounts where these kinds of opinions or communications can be shared. But that is a very personal decision. I feel it shouldn't have to be this way. But the fact that I feel it shouldn't be this way doesn't mean the State doesn't have all these mechanisms: netcenters, digital spies, and an entire structure devoted to planting narratives on social media, especially on Twitter. (**Flor de Café**)*

These testimonies allow us to understand containment as a low-profile strategy: less exposure can provide greater protection, but it can also mean less public visibility and a reduced capacity to exert influence openly.

This is not concealment for the sake of convenience, but a rational response to environments in which visibility increases both social exposure to punishment and material vulnerability. Ultimately, these testimonies show that self-protection can also involve *planning for scenarios of extreme escalation* that extend beyond the digital sphere. **Flor de Café** describes this critical threshold:

We’ve reached the point of considering whether someone might need to go into exile. I mean, if someone in the collective needs to leave the country, who do we need to contact? How quickly can they respond? And how do we stay informed if anyone becomes involved in an investigation by the Public Prosecutor’s Office, which, unfortunately, is compromised?

Exile emerges here as an emergency measure—not a desired solution, but an extreme protocol in response to the risk of criminalization, persecution, or physical violence. This concern forms part of a broader context in which digital violence intersects with judicial criminalization and defamation campaigns within communities, creating a hostile environment aimed at delegitimizing and silencing human rights defenders and dissident voices.

These testimonies also portray Twitter/X as a particularly hostile environment, where hate is concentrated and posting is perceived as a source of risk. **Misidente** frames the decision to leave the platform in terms of security:

Yes, well, after all this, and since we had already stopped using the platform... one of the first decisions we made was to leave X. It was like, “X is no longer a space we want to inhabit... because of who runs it,” because the policies changed, because it became too violent. We also said, “Making these kinds of decisions is political now, and it’s also valid to do so.” Then the younger people in the organization were the ones who said, “Look, we believe the organization can no longer remain on X [Twitter] because it’s not a safe space, and many things have changed.”

GA characterizes three social media platforms in these terms:

And I would say that Twitter is the space in Guatemala where the most hate is concentrated. That anonymity—the anonymity of the accounts, that swarm-like activity I mentioned involving netcenters—is much more prevalent on Twitter. Then there is also the misleading information they generate, for example using artificial intelligence to defame certain people, which also circulates on Facebook. And then there is the underworld of WhatsApp, where it is very difficult to monitor or to trace malicious activity back to its source.

Trixie666 explains the practical consequence: “For the people and activists we’ve supported, it’s quite difficult and even dangerous to post anything without receiving these kinds of comments.” Silence thus becomes a defensive response that, while protecting individual integrity, impoverishes the public sphere and severely restricts the exercise of fundamental rights, particularly freedom of expression and digital political participation.

3.7. Self-Censorship, Withdrawal, and Democratic Deterioration Online

In the testimonies gathered, self-censorship appears not only as an emotional consequence of harassment but also as an effective mechanism of political control that reshapes which issues can be discussed, who can discuss them, and under what conditions.

There is also self-censorship because of the lack of tools and protocols to follow. Many people choose to withdraw from digital spaces in some way, and perhaps the quickest response is silence. But I also think it is important to recognize that, when we talk about how this digital violence affects women’s political participation in Guatemala, there are multiple structural barriers that contribute to it. (Marta)

This form of control becomes particularly evident when the debate intersects with what Arguedas (2024) conceptualizes as “reproductive reconquest”: the reimposition of a moral and political order that seeks to restrict the sexual and reproductive autonomy of women, gender and sexual minorities, and Maya peoples.

But I do believe that Indigenous people who are content creators are more likely to become memes. Digital culture is often like, “Oh, look at this person who said this, or did this,” and then it goes viral in a patronizing way. So that’s a very fine line that I think is difficult for these creators to navigate. (Malinche)

Malinche’s testimony suggests that the visibility of Maya content creators can be used as a vehicle for digital attacks on Maya identity through the irony and satire of memes. This can be characterized as a form of “soft attack.” **Misidente** by contrast, describes attacks that can be characterized as “hard”:

We had stopped posting and knew that we had greatly reduced our presence on social media because there had been so much harassment, so much hate speech, and so much exposure. Last year, for example, they took photos and videos of us and posted them on larger national platforms, saying that we were spreading gender ideology to children, that people should look for us, and even sending us death threats... telling us where we lived so they could find us and all that.

These testimonies show that digital violence does not merely target content; it also pressures dissident bodies and political agendas out of public view, directly affecting democratic pluralism and the right to occupy the virtual public sphere. In this context, self-censorship emerges not as a lack of commitment, but as a survival strategy that reshapes activism and impoverishes public discourse. **GA** explains this clearly:

They are keeping information to themselves, preferring not to publish it, and then we really can’t measure it, but there is a setback in the “democratization” of freedom of expression on social media, because the people who are most attacked decide to become more anonymous or maintain a much less public profile.

Although this practice severely restricts freedom of expression, it also reflects a process of forced adaptation: to survive, people must lower their profile, fragment their presence, and move deliberation into less visible channels. Self-censorship, understood as a technology of power, operates through hate speech, persecution campaigns, and the absence of effective safeguards on digital platforms, limiting democratic deliberation and reducing the presence of women and gender and sexual minorities in the spaces where public opinion is formed.

The result is not merely individual discomfort, but a structural reconfiguration of participation: fewer voices, fewer visible bodies, fewer issues entering the public agenda, and more energy redirected toward care and security protocols simply to sustain participation in the face of violence.

Chapter IV

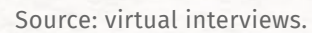
“GIVE THEM LOVING COMMENTS”: TECHNO-RESISTANCE.



The previous chapter examined the effects of digital violence against women and gender and sexual minorities, with particular attention to impacts ranging from self-censorship and withdrawal from the public sphere to psycho-emotional effects.

This chapter focuses on techno-resistance (see Figure 4.1), understood as frameworks of knowledge, interpretation, and validation through which women and gender and sexual minorities produce, share, and legitimize knowledge and practices that enable them to protect and sustain themselves in digital environments shaped by inequalities of gender, sexuality, and power. This knowledge is embodied, rooted in experiences of violence, surveillance, and exclusion; collective, built through networks, organizations, and communities; and pragmatic, oriented toward action and bringing together technical, emotional, ethical, and political dimensions.

The interviews revealed that organizations are implementing techno-resistance strategies through internal reflection and the adaptation of their communication practices. These include prioritizing accessible language, carefully constructing narratives, and making strategic decisions about what to say, how to say it, and which platforms to use. These strategies are complemented by techno-protection and co-care practices that integrate digital, physical, and emotional security, including content moderation, anonymity, response protocols, reporting attacks, and the use of technological tools to reduce exposure. Emotional and community care also plays a central role through spaces for listening, psychosocial support, and support networks grounded in collective awareness.



4.1. Strategies of Political Resistance

This section analyzes the individual and collective practices through which the organizations interviewed contest power relations and build digital citizenship⁴.

A. Contesting and Reclaiming Digital Space

Contesting digital space involves simultaneously redefining it, denouncing the harms that occur within it, and opening public debate about how people inhabit digital environments and how cyberspace shapes everyday life. As one interviewee puts it: *“Who am I in cyberspace? And how do I exercise my rights in cyberspace?”* (Malinche).

Activists understand digital space as a territory that must be reclaimed and transformed into a space of agency, where everyone has the opportunity to be heard.

A core function of these organizations is to inform, translate, and make information accessible in order to broaden its social reach.

We believe that finding government information on how to file a complaint in cases of abuse or what steps to take to report harassment is difficult. Therefore, we believe the most important thing is to create shareable images and accessible links, making this information available online in a way that eliminates the need for users, audiences, and the public to sift through ten pages of Ministry of Health documentation. Our goal is always to inform. (Malinche)

The groups describe developing strategies for the political and communicative appropriation of digital media, centered on maintaining control over their own narratives as a form of resistance and collective care. Within this framework, the aim is not simply to “be” on digital platforms, but to intervene in the symbolic conditions that shape both social and subjective life.

⁴ Digital citizenship: Competencies that enable people to access, understand, analyze, produce, and use digital environments in critical, ethical, and creative ways.

Therefore, it's important to speak out regarding the influence cyberspace has on the construction of our identities, our self-esteem, and our work. It's about reinterpreting these experiences, but also rendering these realities visible so that a conversation can take place. (Malinche)

B. Communication Strategy and Platform Selection

The appropriation of virtual space is also reflected in collective decisions about which platforms to use, which formats to prioritize, and which audiences to target. Language itself becomes a strategic resource: organizations favor accessible, creative, and non-technical vocabulary and avoid highly politicized terms that may attract hostile groups, while still preserving clarity and the perspective of the experiences being communicated. **Misidente's** testimony clearly captures this logic of translation and public engagement:

It's not just about posting on social media or showing what we're doing, but about creating narratives and emancipatory imaginaries that allow us to envision other ways of living; that allow us to share our voices on platforms that have also been opened up to us and historically taken away from us, and that we want to reclaim. We want to show that narratives can also emerge from a place of tenderness, dignity, well-being, and community, in relation to different issues.

The testimonies also show how these dynamics are experienced as a daily struggle for attention and as an operational decision to remain present in the spaces where audiences already are. **GA** frames this in terms of the attention economy:

Achieving that reach and impact is increasingly difficult because people are more easily distracted, so we draw somewhat on the logic of the attention economy: trying to get people to spend more time with our content, engage with it, and reflect on it.

In parallel, **Misidente** explains the importance of selecting a platform: The second question was, “Well, which platforms are we going to stay on? TikTok, Instagram, Facebook, because those are also the places where we reach people... Our main territory is Facebook, Instagram, and TikTok.”

GA points out that impact is not always visible through public metrics such as comments or shares, but can instead be reflected **in less visible forms of circulation** that are strategically significant:

We know that we publish topics that may be of interest and people don't comment on the posts or, for example, share the published article publicly. However, internally, we can see that many people have saved it or shared it privately. Our conclusion is that people don't want to say publicly, “I agree with this” or “I want you to see this,” but the information is still circulating privately.

Along similar lines, **Malinche** explicitly identifies control over the conversational environment as a condition for sustaining digital engagement without allowing confrontation to take over:

[...] Our activism is digital; it takes place on social media and sometimes reaches only a limited audience. But there have also been cases where we've reached a much broader, unsegmented audience, and that has been a real exercise for us: segmenting, hiding, and moderating the hateful comments we receive. There is always a certain vulnerability involved in working in digital spaces.

These practices reflect a dual strategy. On the one hand, organizations seek to expand their reach and activate core audiences through content that is consumed and shared even when people do not engage with it publicly. On the other, they seek to reduce the hostile noise that discourages participation and intensifies polarization, protecting the communicative space so that dialogue can continue and persuasion can build over time rather than through direct confrontation.

C. Language as Resistance

Following processes of collective internal reflection that prioritize care in response to digital violence, organizations are seeking more accessible forms of communication. This includes simplifying their language in order to reduce exposure to risk and avoid unnecessary attacks:

I think that, in a world where TikTok has become one of the main places people turn to for quick information, we also have to think about how we present what we produce. The idea is to create narratives in formats that are accessible and easy to understand—to translate highly scientific or technical digital terms into more everyday language, as Malinche was saying. That makes the information easier to access and consume, and it’s something we need to consider when conducting research: first the information is processed, then translated, and finally adapted into a format that is accessible to everyone. (Flor de Café)

This is understood as a way of engaging audiences who may be unfamiliar with debates on sexual and reproductive rights and gender and sexual dissidence, expanding the reach of messages beyond activist circles, lowering the barriers created by specialized jargon, and preventing communication from being drawn into polarized frameworks, without abandoning its underlying political content.

In this context, “speaking, naming, and selecting a platform” is strategically redefined through narratives centered on love, dignified life, tenderness, and resistance. These narratives allow organizations to position the struggles of young people and dissidents without necessarily relying on discursive frameworks that may generate greater hostility:

In Guatemala, the Ministry of Education issued a circular saying that organizations associated with “gender ideology” should not be allowed into schools. And guess what? After that, we started going into educational institutions. We started finding other ways to name things. And I’m telling you, we’ve questioned ourselves a lot, because we’ve had to change words that are important to us—words that we knew, if we continued using them, could close off other spaces to us. So the

question became: “How do we do this without losing our essence?” Because we are LGBTQ+ people, because we are feminists, because we are transfeminists, but we also don’t want to lose access to those spaces. That’s when we started talking about “dignified lives.” We said, “We’re going to talk about dignified lives for everyone.” And for people to live dignified lives, they need to be able to exercise their right to autonomy and their right to comprehensive sexuality education.
(Misidente)

The choice of words, language, and communication style is itself a strategy. While organizations may decide not to use certain terms in order to protect themselves, they simultaneously select other language according to the audiences they seek to reach. Far from being superficial, these choices are the result of careful reflection and reveal the tensions between preserving feminist, transfeminist, and LGBTQI+ identities and maintaining the ability to influence and engage broader audiences.

D. Awareness, dissemination and outreach

An organization’s ability to identify its audiences and adapt its language accordingly is what allows its messages to resonate effectively. Beyond technical definitions, organizations facilitate the circulation of information in their everyday practice by adjusting tone and format so that content is useful to both specialized and general audiences. This flexibility enables knowledge to be shared more effectively and allows each message to connect with the realities and interests of those receiving it:

There have been people and situations where we’ve managed to have a conversation, or they’ve even sent us direct messages saying things like, “I want to know more about this,” or “You were saying this; can you explain it to me?” And then we direct them to a resource. **(Malinche)**

Collective actions are also strengthened through practices such as joint publications aimed at reducing harm, the development of support networks,

and collaborative efforts to counter phenomena such as shadow banning⁵ by strategically working with the algorithm:

And it’s also something we can use as a tool, like, “Look, we’ve been shadow-banned.” Because that happened a lot. When you talk about certain topics, they don’t get much reach, so people can help by sharing, retweeting, or sending the post to friends. In a way, it’s about working with the algorithm and going back to more organic ways of circulating content online. (Flor de Café)

The ability to identify and reach specific audiences also requires a certain degree of technical proficiency in the use of digital platforms. This means translating strategy into concrete actions, such as:

- » Knowing how to use functions such as “hide from everyone except the author.”
- » Blocking keywords.
- » Restricting profiles or segmenting audiences.

This is not a matter of sporadic or improvised moderation, but of establishing clear protocols for determining what should be deleted and what should receive a response, turning an otherwise chaotic task into an operational process. This technical clarity reduces the amount of time activists are exposed to hate[2], providing an additional layer of protection for their mental health.

E. Networking

Communication on social media often takes horizontal forms of interaction similar to the ways feminist organizations and organizations of gender and sexual minorities coordinate and interact offline. This can make it easier for some organizations to appropriate social media as an extension of their

⁵ **Shadow banning:** the practice of limiting the visibility or reach of a user or their content without removing it or explicitly informing the user that such restrictions have been applied.

existing ways of working. **Flor de Café** describes the logic of rapid coordination in response to attacks:

[...] It's happened to me that we're in several chats connected to projects we've been involved in, and people ask us to help create counter-narratives. Like, "Look, this post is getting a lot of hate—give it loving comments." And we've gotten messages saying, "Look, someone is DMing us like this," or "Please, if you can, leave a nice, positive comment." It's about figuring out how to bring positive, loving comments into posts that are usually full of hate, especially when the influencer is trans or feminist, has a strong point of view, or is talking about a very sensitive issue. I think Guatemala is ready for this conversation, and we're going to turn things around—not just for the sake of it. A lot of it comes down to the support network we've built among different collectives and like-minded people through WhatsApp groups or Instagram groups. (Flor de Café)

Malinche describes the need for a guide for responding to hate messages:

I know people don't want to talk about this and that they're going to get angry. I don't want to overwhelm the girl who is going to have to come up with a response to every one of these comments. So we create Word documents with possible prewritten responses. If the message is outright hate, in some cases we try not to engage. But if it seems like someone is open to dialogue, when are you supposed to find the time to write a response without feeling hurt, sad, or angry? So you go to the document, where the responses have already been discussed, reviewed, and edited, and you know how to proceed. (Malinche)

Guides for responding to hate speech are an important tool. Their effectiveness, however, is limited in the face of coordinated swarm attacks. In these situations, **GA** describes a strategy of temporarily distancing the person responsible for communications from the violence:

When the attacks have been particularly vicious, what we've done is have the social media person step aside and let someone else take over. [...] Someone

with a bit more distance comes in and handles all the incident reporting so that the social media person isn't constantly exposed to that violence. (GA)

These strategies illustrate forms of collective agency that move away from direct confrontation and instead seek to reshape the emotional climate and visibility of content through coordinated acts of support that help sustain a public presence in digital environments.

F. Key Actors and Decision-Makers

Another strategy used by organizations involves awareness-raising and educational work directed at key actors and decision-makers. This work operates along two complementary dimensions: political and institutional advocacy, and technical and pedagogical training.

At the institutional level, the project highlights direct participation in the updating of municipal violence-prevention policies, resulting in the formal recognition of digital violence as a priority crime. This work is reinforced through awareness-raising campaigns aimed at institutional personnel and senior authorities, including departmental governors:

In Guatemala, there has been an interesting political shift—I don't know if it's positive, but it's certainly interesting. There are also more women in politics. At one point, there were several young women in the current ruling party, and the harassment, intimidation, and violence they faced was shocking. It was very intense. That was also when we began to understand what it means, especially for women, to be public figures in politics. Our departmental governor, who is a woman, has experienced this as well. We went to speak with her about the importance of naming it, because she has lived through it herself. It was like, “Look, Governor, you have witnessed and experienced this kind of violence [gender-based and digital political violence], right? So we believe it is important for you to help us raise awareness, to name it, and to use your position to call on institutions to take action.” (Misidente)

Likewise, the use of explicitly gendered terms such as “young women” or “female witness” goes beyond conventional inclusive language and becomes a practice of resistance. By deliberately using these feminine gender markers, organizations reclaim and “occupy” virtual space, turning language into a political tool for challenging patriarchal norms.

In the area of education, organizations promote media and information literacy programs, develop specific educational content, and offer workshops on cybersecurity, digital security, and online safety. Education thus becomes a fundamental strategy for expanding civic autonomy:

And that is why we create this kind of content. We offer courses on media and information literacy, with a focus on security. It is about making people more aware of the power they have as citizens—both their rights and their responsibilities as digital citizens. (GA)

The range of tactics deployed by organizations extends from grassroots training to sustained engagement with the public agenda. Within this repertoire, inter-organizational alliances function both as a force multiplier and as a protective mechanism against risk. **GA** frames this in terms of cooperation:

I think those partnerships with organizations are absolutely crucial. In the case of [our organization], when there is research that may be somewhat complex, we have a network of media outlets with whom we propose joint publications in order to reduce the impact and the risk.

Misidente in turn, describes efforts to engage actors with the capacity to influence cultural and community dynamics:

There was a meeting last year. An evangelical church provided the space, and it was a self-care meeting. They told us, “The only thing we don’t allow is lighting candles, because for us candles have a different connotation.” But we were able to bring our sprigs of rue and our essential oils, and we carried out the ritual, and it turned out beautifully. The pastor was incredibly kind. He has opened

doors for us, we’ve done everything, and it has been a really beautiful change. Because it’s about saying, “We’re not doing anything wrong, nobody is doing anything wrong, so how can we promote a dignified life?”

Taken together, this framework confirms that responses to digital violence are not limited to defensive measures, but require integrated strategies of training, coordination, and advocacy capable of sustaining collective action.

G. Expansion to Other Territories in Guatemala

Interviewees emphasized the need to expand and sustain support and accompaniment strategies, both in person and virtually, through close collaboration with local organizations rather than concentrating efforts solely in the capital or departmental capitals. As **Marta** explains: *“Part of what we did last year was to form a national committee of young women from different departments of Guatemala to ensure diverse representation.”*

In this regard, **Malinche** also reflects:

This year I had the opportunity to work with an influencer from the Guatemalan highlands who is quite conservative by my standards. She got a tattoo, and she has around 50,000 or 100,000 followers, including people from Indigenous communities. A lot of people attacked her for it, saying things like, “How could you get a tattoo? What’s wrong with you?” She had her dog’s name tattooed, and there were even comments from religious organizations telling her it was a sin. She asked me, “Do you know what I can do?” So I helped her set up filters on her comments so that not just anyone could comment, and helped her hide certain keywords. But what I see is that these kinds of steps are being taken while these conservative communities are still clashing over very basic issues. And because she creates content in K’iche’ and Kaqchikel, she reaches audiences that we probably never will, but they also need this kind of basic digital security training.

Marta presents this as a cross-cutting consideration in project implementation: “[It is necessary] to also incorporate Maya languages. This is something that

is present across all the projects carried out nationally in Guatemala, because Spanish is not the only language spoken here; in many communities, a Maya language is the mother tongue.”

4.2. Co-Care Spaces

Among the organizations interviewed, emotional and community support strategies are structured around two pillars: active solidarity and open communication. Activists describe how co-care becomes possible when spaces of trust are created in which emotional impacts are neither minimized nor treated as an individual burden, but instead shared as an integral part of collective work. In this regard, **Malinche** emphasizes the political and emotional value of creating opportunities to share these experiences: “Digital safety issues aren’t really discussed, and I’ve sometimes gone to meetings organized by [...] where only eight people show up. So I think any opportunity to share, to build community around these issues, is valuable.” Responses to burnout, violence, and trauma arising from this work are therefore not understood as solely individual matters, but as issues to be addressed through support networks and a comprehensive, though still developing, system of collective co-care and mental health support.

This support takes shape through practices such as listening circles, psychosocial support, and safe spaces where fears can be named and personal experiences validated. Marta describes this as an internal practice grounded in trust and openness, in which care also becomes part of the organization’s infrastructure: “Within the organization, we try to foster open communication and trust, so that if something happens to you, you can share it. This is a safe environment and a safe space.”

Co-care also involves bringing affective and family networks, including mothers and other caregivers, into the support system in order to strengthen immediate emotional support and sustain the continuity of the work:

We created a space with our mothers, our caregivers, our support network—the people who care for us and protect us. It was such a beautiful and interesting

process to listen to our mothers. Our mothers didn’t have a support network. My mother, for example, thought she was alone in this, carrying that fear with me. I think it’s also very important to say that, within the organization, almost all of us have the support of our families, and we know that this has also served as a protective factor for us. (Misidente)

A. Spaces for Collective Listening

The interviewees agree that managing hostility and risk cannot be reduced to technical measures; it is also, fundamentally, an emotional and communal process. In response to exhaustion, fear, and distress, collectives have created supportive spaces in which words themselves become a form of care: documenting experiences, naming emotions, and genuinely listening to one another become tools for healing and, at the same time, for resistance.

Misidente describes this as a concrete practice for organizing internal support: “We documented how we felt, what the experience made us feel, and we held listening circles to talk about what had happened to us and how we felt.” Within this framework, care is not an accessory practice, but a way of sustaining the capacity for political action when a hostile environment seeks to undermine participation through emotional pressure.

At the same time, activists emphasize that collective care requires a practical ethic of setting limits and managing energy, in which personal autonomy forms part of the protection system. **Trixie666** describes this as a necessary process of reflection for sustaining participation without becoming overwhelmed: “Within collective and individual care, it was also about sitting down to talk and asking: How much time can I dedicate to this space? How much can I do? What specific activities can I take on?”

This reflection shows that safety and care are not only about configuring tools or establishing protocols, but also about the ability to set sustainable rhythms, distribute workloads, and sustain a community that provides support, respects individual limits, and enables the work to continue in an adverse environment.

B. Psychosocial care

Organizations emphasize that psychosocial support is becoming an essential component of co-care and protection. The need goes beyond abstract notions of “well-being” and responds to concrete requirements, including dedicated budget allocations and partnerships that can provide specialized therapeutic support for members dealing with trauma, direct threats, and the complex emotions that arise from their work and the multiple intersections of their lived experiences.

Everyday work is shaped by a persistent tension between the urgent need for protection and the lack of resources required to sustain that protection over time. As **Marta** explains: “We are also supporting the team with mental health self-care. But this is something very recent; as I say, this care can’t be implemented every year, and it also requires resources.” Along the same lines, **Flor de Café** frames the issue in practical terms: “We need external help to support us in navigating all these situations.”

The testimonies also describe an ethic of care grounded in a humanitarian and empathetic approach to violence, recognizing that emotional impacts directly affect the ability to sustain activist responsibilities. **Marta** makes this connection clearly by linking care to temporary disengagement and rest:

We take great care to understand that if you are experiencing violence, you will need to disconnect from your work activities. This is a humanitarian and empathetic approach, and it’s important to understand that you need to give yourself space, a few days, to process what you are going through. This is part of some of the actions we have tried to incorporate into this collective care. (Marta)

While some collectives are able to manage and allocate resources for collective care measures, including professional therapeutic support, others rely on lower-cost strategies to reduce burnout and provide emotional support.

We’re going to promote and distribute some small planners for emotional and digital self-care. They’re really nice. I hope I can show them to you someday. The idea is for people to make the planners their own. They include some recommendations for what to do if you experience cyberbullying. For example, one suggestion is to draw anywhere on the page and express how you feel, and there are also pages you can cut up or tear out if that’s what you need. It’s a very interactive planner, and that’s the idea behind it: to provide emotional support. Because we all know how much a post, a comment, or something like that can affect people. (Misidente)

4.3. Security Protocols

Inhabiting digital space involves, simultaneously, speaking out about harmful realities, sustaining the circulation of information that is valuable to communities, and activating care, digital security, and support protocols that make continued presence possible without unnecessarily increasing exposure to harm.

Although the organizations interviewed do not always describe these practices in methodological terms, their testimonies reveal actions consistent with a logic of planning and risk reduction, including strengthening internal capacities, securing organizational infrastructure, and establishing minimum conditions that allow public denunciation to continue.

Along these lines, **Misidente** describes a concrete measure aimed at protecting the organization’s digital channels: “We created a space to strengthen our communications area, to safeguard it and be 100% sure that our website was secure.” This type of decision demonstrates that occupying digital space is not limited to “publishing”; it also requires secure infrastructure capable of ensuring the continuity and availability of content.

Trixie666 emphasizes the organized and transferable nature of these practices:

They have certain digital and physical care protocols for the compañeras, and we have supported the development of those protocols, offered workshops, kept the

girls updated, accompanied them in purchasing secure devices, recommended other organizations, and connected them with organizations that can provide more support than we are humanly able to offer.

Here, security emerges as a collectively built capacity that brings together digital and physical protection in order to sustain public action without compromising the integrity of those who carry out and support the work.

A. Protocols and protection measures

Those consulted agree that the development of protocols should be treated as a strategic and collective priority, integrating digital security, physical security, and emotional well-being. Marta explains: “The latest development—the most recent initiative we’re finalizing this year—is the creation of a digital care protocol aimed primarily at civil society organizations.” The goal is not only to protect members of these organizations, but also to build shareable capacities that can strengthen broader protection networks.

In practice, these tools include specific protocols for situations of public exposure, field coverage, and the day-to-day management of digital security, as well as manuals for organizations and initiatives aimed at strengthening “digital citizenship” in ways that help mitigate risk.

GA describes the different components of this security framework: “We have one protocol for physical security during field reporting and another for digital security.” From an operational perspective, this means establishing clear communication channels and mechanisms designed to reduce vulnerability.

Flor de Café emphasizes the importance of anticipating contingency plans and alliances in situations where an incident exceeds the collective’s capacity to respond: “Having mitigation strategies as a collective in case there is a breach, and knowing which organizations we can turn to if things get out of hand.”

B. Managing Hate and Other Tools

To manage harassment and hate speech, collectives describe a range of technical moderation practices that combine hiding, deleting, reporting, and setting up keyword filters, with the aim of reducing vulnerability in digital spaces and limiting the time and energy consumed by hostile interactions. **Malinche** illustrates this with an example: “I helped her activate filters on her comments so that not just anyone could comment, and helped her hide certain keywords.”

At the same time, some organizations choose to ignore or minimize engagement with insults and aggression as a de-escalation strategy, particularly when responding could amplify the conflict or contribute to burnout. **GA** connects a perceived decline in the intensity of hate to the broader political context:

We basically ignore insults and violence. I think it's important to tell you that, I would say, the levels of aggression have decreased. We believe this is because state violence has somehow lost momentum under the new government [Arévalo's], because the presidents themselves were the ones fostering hate speech. So we have noticed a decrease in that kind of violence.

The testimonies show that moderation is not merely a technical decision, but also an assessment of the surrounding environment. Levels of aggression fluctuate, and strategies are adjusted according to the circumstances and the costs of exposure. Beyond the technical dimension, risk management also operates as an organizational strategy aimed at protecting the team. This includes discussing risks before publishing sensitive content and preparing sets of predefined responses in order to avoid improvising under pressure and to reduce cognitive strain.

What do we do when people start leaving hateful comments? Because we believe in not deleting them. We feel it's important for the people who follow us to see that this is still happening. At least in my case, people tell me, “This isn't necessary anymore.” But it is necessary; those messages are still there, from people who are angry and insulting us. So we don't delete them, but we do hide

them, or we try to have a set of prepared responses ready to push back against the hate. (Malinche)

In terms of technical recommendations, participants also describe explicit guidance on tools and safer browsing practices. **Trixie666** summarizes this approach: “We’ve already given them tools and told them, for example, not to use Google Chrome, to use DuckDuckGo, or to download Firefox and install this.” These practices reflect a preventive approach aimed at reducing exposure, ranging from more secure website infrastructure to everyday communication and browsing habits.

C. Data protection and exposure

In terms of **data protection and exposure management**, activists describe a range of self-protection strategies aimed at reducing their digital footprint and, in turn, limiting risks that could translate into offline harm for those who participate in public spaces or sustain activist work.

Another common strategy involves segmenting one’s digital life in order to separate different areas of exposure and reduce the overlap of information between public and private spheres. In practice, this may involve using separate accounts, one for activism and another for personal life, as well as quickly removing information when a potential leak is suspected.

Flor de Café describes this practice as a functional separation between roles and spheres of circulation: “Most members of the collective have a personal account and a public one; all activism is handled through the public account, and everything else through the private one.” This segmentation not only organizes their online presence but also serves as a protective barrier, reducing the unintended exposure of personal and affective networks and limiting the potential for digital risks to spill over into everyday life.

Misidente describes the appropriation of digital tools to reduce exposure, particularly through audiovisual anonymization strategies:

Discovering that there are ways to resist together has allowed us to create these networks, these safe spaces, and other possibilities as well. For example, someone uploaded a video a few days ago but didn’t want their face to appear. They used a voiceover and only showed short clips of the activity, and they were even able to alter their voice using artificial intelligence. So the question is also: how can we take ownership of these tools and use them safely for ourselves?

This example of techno-resistance shows how technical innovation can be combined with ethical, emotional, and political considerations in order to sustain public participation without compromising the safety of those involved.

D. Incident Logs

With regard to documenting incidents, interviewees acknowledge that there is no standardized system across organizations. While some collectives prioritize documenting the subjective impact of violence—how people felt and the emotional effects of attacks—through practices such as the listening circles described earlier by **Misidente**, others maintain more technical records that include screenshots and the identification of profiles:

[...] They took photos, they took screenshots, and even though the post was deleted, they had the screenshots and began uploading them from their own profiles and sharing them in other groups. It took about three or four days to map the profiles and groups where those photos might reappear so that they could be reported and taken down.

In more sensitive cases, screenshots and profile information are collected as evidence for potential reporting procedures. As **GA** explains: “What the organizations advised us was to keep a record of those specific threats, to include screenshots and all the evidence in the incident log in case anything happened. That’s what I keep in mind when there has been a threat that could escalate into physical violence.”

This variation reflects both differences in organizational capacity and distinct ways of understanding harm. In some cases, violence is processed through shared emotional experience; in others, it is documented as organized evidence that may support formal legal action.

The documentation process nevertheless appears to remain at an early or relatively rudimentary stage, often relying on individual screenshots or specific incident reports and constrained by limited time and heavy workloads. Even where documentation is inconsistent, however, there is a persistent awareness of its strategic value. Recording incidents is not only about “preserving evidence,” but also about building an organizational memory of violence that can help prevent responses from remaining purely reactive and fragmented.

4.4. Organizational limitations and restrictions

Organizations’ efforts to protect the people they work with come up directly against material and financial constraints. Security is not only a political decision; it also carries financial costs that can be prohibitive. This begins with the high price of licenses for encrypted services such as Proton: “The Proton license isn’t cheap, even with the discount for being a non-profit. So those costs also have to be factored into the budget.” **(GA)** Collectives also face broader challenges in sustaining themselves financially over the long term, sometimes to the point of being unable to afford rent for a physical space or provide fair compensation for their work.

The lack of funding described by collectives is not merely a contextual constraint, but a structural factor that shapes their capacity for action. It determines what they can sustain over time, which skills they can professionalize, and which risks they are forced to assume. Within this context, the continuity of activist work becomes closely tied to external grants and specific projects that provide both operational and political support.

Misidente’s testimony illustrates this clearly, identifying funding as “the other challenge” and showing how dependence on a particular project can become

a factor in both organizational survival and the ability to keep an issue on the public agenda: “The other challenge would be funding. Right now we do have some, and that helps us a lot to continue positioning the issue. But there isn’t much available either, since what happened with USAID.”

This same precarity shapes technical decisions that are driven not by an ideal standard of security, but by the need to keep costs as low as possible. When resources are scarce, organizations are forced to rely on free or low-cost tools, even when these come with limitations and potential vulnerabilities, in order to maintain basic operations. This increases their exposure to risk and weakens their capacity for prevention.

In one testimony, the use of Google services emerges as a pragmatic response to the lack of affordable alternatives: “We use Gmail, which is the most economical option; these things require resources, and when there aren’t any, it’s a bit difficult to think about how to prevent other types of risks.” **(Marta)** In this sense, precarity operates through a lack of resources that constrains the very possibility of anticipating and preventing harm, shifting risk management toward reactive responses that can, at times, impose a greater emotional burden on the collective.

4.5. The Future: Guatemala as a Mirror of Resistances

In the interviews, participants were asked to imagine the digital future through three possible scenarios—ideal, realistic, and dystopian—and to consider the conditions, risks, and actions that could either support a transition toward a fairer and safer environment or, conversely, deepen patterns of control, inequality, and rights violations.

Interviewees tend toward a predominantly dystopian outlook, or suggest that we are already entering an era in which social media offers few genuinely democratic spaces, except those created through the resistance of social movements and their reappropriation of virtual space:

The realistic scenario is where we are now: artificial intelligence can also be useful in making our work more efficient—ethically and transparently, of course—and in helping us find tools and narratives that are appealing to audiences and can build lasting engagement. The challenge is to make these issues, which are not necessarily the most popular, accessible to a mass audience. (GA)

The future that organizations consider most likely, if no structural transformations take place, is one marked by intensified surveillance, greater state and corporate control, the concentration of technological power, and increasingly precarious conditions for activism, particularly in contexts of democratic erosion.

In this sense, the interviews reveal a prevailing sense of urgency and concern. Organizations recognize that, without ethical, regulatory, and community-based intervention, the current trajectory of the digital ecosystem risks moving toward increasingly oppressive scenarios. This reinforces the need for civil society to actively contest and shape that future:

And then, in the catastrophic scenario, this logic of capital becomes more and more entrenched, while spaces for regulation, sanctions, and even protections for minors are gradually rolled back, as has already happened with Twitter. That would be the most catastrophic scenario: one in which the law of the jungle increasingly prevails, while organizations that produce information, knowledge, and content that can be useful to people are pushed further and further out of view. And I include journalism in that. (GA)

They censor us to the point where we can no longer use the platforms; the internet becomes an uninhabitable space for dissident people, for people who create content, for people who talk about these issues, and that this also prevents us from building community. (Misidente)

The ultimate dystopia is that the government in power takes control of digital tools, gains access to all this personal information, and uses it against the population. (Flor de Café)

By contrast, the desired future is one of an ethical, regulated, inclusive, and accessible digital environment, supported by an informed digital citizenry, equitable infrastructure, media literacy from an early age, and feminist and intersectional regulatory frameworks that protect rights and limit the power of large digital platforms:

The breakdown of the system means that the rules of the game are increasingly being dictated by these large platforms, whose sole (or ultimate) purpose is to generate profit and extract money and data, which is also money, from all users. On the internet, we are becoming less like citizens and more like consumers. (GA)

In the best, best possible scenario—oh, we’ve imagined it—what we talk about is a safe space, a habitable space, one where, when you enter, what you find is love. (Misidente)

I would like platforms to work with feminist and LGBTQI+ organizations to create community standards that truly understand our realities and educate young people in the responsible, ethical, and caring use of technology. (Pau Pau)

An empowered Guatemala, one that truly has digital citizenship and can therefore ask these questions: Who am I in cyberspace? How do I exercise my rights in cyberspace? (Malinche)

These visions articulate aspirations that require sustained action, political pressure, and collective coordination. They are not presented as an automatic extension of the present, but as futures that must be actively contested and constructed.

In this context, as Adrienne Maree Brown states: *The future is about collectively shaping what does not yet exist.* The future becomes habitable through practices of care, community, and solidarity.

Chapter V

CONCLUDING REFLECTIONS.



Guatemala's post-agreement transition was not a linear "post-conflict" progression toward democratization, but an ongoing struggle in which the promise of peace coexists with a historical order of exclusion, racialization, and patriarchy, rearticulated through impunity and clandestine networks of power.

While formal democracy opened spaces for the political participation of women and gender and sexual minorities, it also created conditions in which anti-gender offensives, the theocratization of politics, state capture, and the restriction of civic space could take hold.

The expansion of Guatemala's digital environment produces a fundamental tension: it broadens opportunities for access, organization, and public expression, while simultaneously consolidating a contested space marked by technological and gender inequalities and moralizing attacks. Digital democracy depends on conditions that prevent widespread digital adoption from devolving into a "digital war" driven by disinformation, hate, defamation, and *online troll farms*. Online violence extends historical patterns and memories of terror, producing silencing and self-censorship.

Digital violence is frequent and takes multiple forms, including harassment, disinformation related to sexual and emotional life, and homophobic and transphobic attacks, with consequences ranging from emotional distress to fear for physical safety. One in five activists surveyed experienced more than six forms of digital violence, indicating a pattern that extends beyond isolated incidents and approaches a sustained trajectory of harassment. Institutional responses remain weak: individual protective measures and support from close networks predominate, while organizational resistance, although effective, is constrained by limited resources and burnout.

Responses to the digital violence questionnaire revealed a dual digital ecosystem: respondents depend heavily on major platforms and manage multiple accounts, while at the same time perceiving significant insecurity associated with privacy, fake profiles, discrimination, theft, and extortion.

Following processes of reflection prompted by experiences of digital attacks and violence, organizations are adopting more comprehensive approaches that seek to move beyond the logic of fragmented projects and exclusively technical responses.

Technology-facilitated gender-based violence operates as a political mechanism of exclusion: it reshapes who can speak, about what, and at what cost. Decisions such as reducing one's online presence, closing profiles, or moderating language must therefore be understood as forms of self-protection in the absence of effective tools and protocols.

Drawing on their experiences and trajectories, organizations identify the need to explicitly incorporate feminist and intersectional approaches into their actions, projects, and plans. These approaches should be grounded in human rights, non-discrimination on the basis of sexual orientation, gender identity and expression, and territorial and cultural relevance, in order to avoid seemingly neutral interventions that, in practice, remain blind to the structural inequalities that heighten exposure to harm.

The interviews confirm that digital violence is a structural and differentiated phenomenon, intensified by public visibility and intersecting identities and compounded by inequalities in access, literacy, and resources.

Technological inequality determines what forms of participation are possible and how effectively participants can protect themselves, resulting in limited digital autonomy. Platforms and the State emerge as weak links: reports go unanswered, algorithms change constantly, and institutional reporting pathways can themselves be intimidating. As a result, the burden of managing and containing harm falls largely on organizations, shifting the defense of rights toward the day-to-day work of digital survival and physical safety.

Techno-resistance emerges in practice not as a set of isolated instrumental responses, but as a framework of knowledge that helps make digital spaces habitable for women and gender and sexual dissidents. It produces shared understandings



of risk, harm, evidence, and safety, and guides decisions about visibility and self-protection without requiring withdrawal from public participation.

Digital political resistance is sustained through a combination of soft infrastructures—support networks, listening, and solidarity—and hard infrastructures—protocols, tools, documentation, anonymity, and control over narratives. Inhabiting the digital sphere is therefore not simply a matter of “being on social media,” but of sustaining a public presence under hostile conditions: continuing to publish, generating counter-narratives, and building community, among other practices. Techno-resistance thus functions as a strategy for organizational sustainability by distributing burdens, allowing for pauses, documenting attacks, and establishing response pathways rooted in collective life.

One of the central challenges organizations face in responding to digital violence is moving from reactive responses—blocking, managing harm individually, and relying on their own limited resources—toward sustainable capacities for digital democracy. These include civic and digital literacy, safe spaces for deliberation, stronger technical and human capacities, and care infrastructures that reduce burnout and fear of reprisals.

With regard to digital platforms and their reporting mechanisms, organizations face the significant challenge of demanding accessible, timely, and effective



procedures; moderation policies that are responsive to feminist and gender-diverse realities; and greater platform accountability for the structural factors that intensify technology-facilitated gender-based violence, including fake profiles and coordinated attacks, rather than treating such incidents as isolated events.

At the national level, extending beyond the participating organizations to the broader network of civil society organizations, the challenge is to transform fragmented defensive practices into a more coordinated system of prevention, documentation, response, and support. This includes shared protocols; media and information literacy adapted to Maya territories and languages; care and mental health networks; and stronger inter-organizational coordination in response to harassment campaigns.

Flexible funding is important for reducing gaps in digital access and power and for supporting initiatives that address inequalities in access to devices, barriers to training, disparities between urban centers and peripheral territories, and linguistic and cultural exclusion. Digital democratization requires both access to resources and programmatic innovation.

The digital future appears increasingly marked by surveillance, censorship, and the concentration of technological power, placing growing strain on organizations.

In this context, it is essential to recognize and value the extensive work that social movements are already carrying out at the local and community levels. Through considerable effort, self-management, and sustained political commitment, these organizations not only defend and advocate for norms, policies, and technological infrastructures that protect human rights—including freedom of expression, privacy, security, and non-discrimination—but also strengthen community networks on a daily basis, expand digital sovereignty, and produce narratives of hope. Supporting these efforts with flexible resources is necessary to ensure that resistance and collective action can be sustained over time.

References

- » Arguedas, G. (2024). “Gender ideology,” refeudalization, and the reproductive reconquista: A (g)local perspective. *LASA Forum*, 54(4), 24–33.
- » Bertelsmann Stiftung. (2024). *Informe de país BTI 2024: Guatemala* [BTI 2024 country report: Guatemala]. Bertelsmann Stiftung.
- » Comisión Interamericana de Derechos Humanos (CIDH). (2024). *Observaciones preliminares: Visita in loco a Guatemala* [Preliminary observations: In loco visit to Guatemala]. Organización de los Estados Americanos.
- » Comisión Internacional contra la Impunidad en Guatemala (CICIG). (2019). *Bots, netcenters y combate a la impunidad: El caso de Guatemala* [Bots, netcenters, and the fight against impunity: The case of Guatemala]. CICIG.
- » Congge, U., Guillamón, M.-D., Nurmandi, A., Salahudin, & Sihidi, I. (2023). Digital democracy: A systematic literature review. *Frontiers in Political Science*, 5, 972802. <https://doi.org/10.3389/fpos.2023.972802>
- » Duarte, G., Aguilar, A., Batres, M., & Lanz, A. (2020). *Violencias contra la población LGBTIQ+: Vivencias y dinámicas que la sostienen* [Violence against the LGBTIQ+ population: Experiences and dynamics that sustain it]. Visibles.
- » Free Press Unlimited. (2023). *Informe de hallazgos de la misión internacional sobre libertad de prensa y de expresión en Guatemala* [Report on the findings of the international mission on freedom of the press and freedom of expression in Guatemala]. Free Press Unlimited.
- » Gay & Lesbian Alliance Against Defamation (GLAAD). (2025). *Social Media Safety Index 2025*. GLAAD.
- » Hernández, G. (2020). Inseguridad y poder político en el Triángulo Norte de Centroamérica [Insecurity and political power in Central America’s Northern Triangle]. *Perfiles Latinoamericanos*, 28(55), 143–169. <https://doi.org/10.18504/pl2855-006-2020>

- » International Center for Not-for-Profit Law. (2024). *Informe final sobre derechos digitales en Centroamérica: Enfoque en Honduras, Guatemala, El Salvador y Nicaragua* [Final report on digital rights in Central America: Focus on Honduras, Guatemala, El Salvador, and Nicaragua]. ICNL.
- » Johnson, O., & Deutch, J. (2024). *Acceder a la conexión: Cerrando la brecha digital de las comunidades LGBTI en el mundo* [Accessing connectivity: Closing the digital divide for LGBTI communities worldwide]. ILGA Mundo.
- » Kemp, S. (2025). *Digital 2025: Guatemala*. DataReportal.
- » López, A. (2023). Género, sexualidad y educación en Guatemala: Disputas, discursos e imágenes [Gender, sexuality, and education in Guatemala: Disputes, discourses, and images]. *Espacios en Blanco. Serie Indagaciones*, 33(2), 15–30.
- » López, T., Batres, M., & Martínez, S. (2020). *Realidades compartidas: Experiencias de violencia y exclusión de las personas LGBTQ+* [Shared realities: Experiences of violence and exclusion among LGBTQ+ people]. Visibles.
- » Marsicovetere, N., & López, T. (2025). Erosión democrática en clave antigénero: La influencia de actores conservadores españoles en Guatemala [Democratic erosion through an anti-gender lens: The influence of Spanish conservative actors in Guatemala]. In S. Corrêa & J. Elman (Eds.), *De España al mundo: La proyección global de la ultraderecha española contra los derechos sexuales y reproductivos. Los casos de Argentina, Guatemala, El Salvador, Chile y Kenia* [From Spain to the world: The global projection of the Spanish far right against sexual and reproductive rights. The cases of Argentina, Guatemala, El Salvador, Chile, and Kenya] (pp. 79–99). L'Associació de Drets Sexuals i Reproductius.
- » Monzón, A. (2024). Una crónica inconclusa: Entre la promesa de la primavera y la realidad del pacto de corruptos [An unfinished chronicle: Between the promise of spring and the reality of the pact of the corrupt]. *Tramas y Redes*, 7, 27–36.

- » Olmedo, R. A., & Taylor, W. Ñ. (2025). La hashtágora en construcción: Reflexiones desde la ciudadanía asexual en Chile [The hashtágora under construction: Reflections from asexual citizenship in Chile]. In A. Arévalo (Ed.), *Ciudadanías sexuales vivibles en América Latina y el Caribe* [Livable sexual citizenships in Latin America and the Caribbean] (pp. 191–223). CLACSO.
- » Suárez, M. (2023). Feminist strategies against digital violence: Embodying and politicizing the internet. *Studies in Social Justice*, 17(2), 241–258. <https://doi.org/10.26522/ssj.v17i2.3417>
- » Tello, S. (2024). *Límites y oportunidades del paradigma de seguridad ciudadana del Estado de Guatemala en su aplicación al espacio virtual como respuesta a las violencias digitales contra las mujeres* [Limits and opportunities of the Guatemalan State's citizen security paradigm as applied to the digital sphere in response to digital violence against women] [Undergraduate thesis, Escuela de Ciencia Política, Universidad de San Carlos de Guatemala].
- » Unidad de Protección a Defensoras y Defensores de Derechos Humanos de Guatemala (UDEFEHUGUA). (2025). *Situación de personas, organizaciones y comunidades defensoras de derechos humanos en Guatemala, 2024* [Situation of human rights defenders, organizations, and communities in Guatemala, 2024]. UDEFEHUGUA.



**NET THAT
WORKS**

alianza
de Fondos de **Mujeres y Feministas**
de América Latina y el Caribe

fcam
FONDO CENTROAMERICANO DE MUJERES
FOUNDATION