

SUMMARY ASSESSMENT REPORT:

THE DIGITAL LANDSCAPE, THREATS AND OPPORTUNITIES.

March 2025 Susana Castaño Muñoz





Table of Contents

INTRODUCTION	2
TERMINOLOGY	4
OBJECTIVE OF THE ASSESMENT	6
METHODOLOGY	7
PRACTICAL CONSIDERATIONS	8
MAIN DATA ON PARTICIPATION	9
SUMMARY OF THE RESULTS	10
Key findings on internet access and digital literacy	10
Internet access and digital literacy by gender	13
Key findings: knowledge and experiences of digital violence and safety \dots	15
Knowledge and experiences of digital violence and safety by gender	20
Key findings on current measures to prevent digital violence	22
Gender differences in current measures to prevent digital violence	24
Key findings on proposals to prevent threats to digital rights	25
Specific proposals to protect against threats of digital violence, especiall women, girls, non-binary people or other minorities	
Key finding on capacities and resources of CSOs	29
ANNEX	34







INTRODUCTION

ReCIPE stands for "Recentering the Civic Internet through Partner Engagement". ReCIPE is a three-year project co-funded by the European Union that aims to contribute to a rights-respecting digital ecosystem that is values-based, people-centred and safe for civil society actors and human rights defenders.

The project puts people, especially women and youth, at the centre of the digital transformation through bringing voices of civil society organisations (CSOs) from both the Global North and the Global South to multilateral digital governance processes.

The project targets CSOs, civil society activists and community members from 10 focus countries. It also targets technology companies and government authorities to promote the creation and enforcement of effective digital rights laws and policies.

ReCIPE is built around three main pillars that complement each other to bring about the desired change:

- Increasing collaboration between organisations in the Global South and Global North to create vibrant and safe online civic spaces;
- Improving digital rights mechanisms and policies that hold governments and corporate actors accountable;
- **Promoting equitable resources** for and access to safe online social and political activity for people and communities at risk of digital harm.

Find out more at:

https://www.oxfamrecipe.eu/

You can also sign up for updates or contact us at:

https://www.oxfamrecipe.eu/contact-us









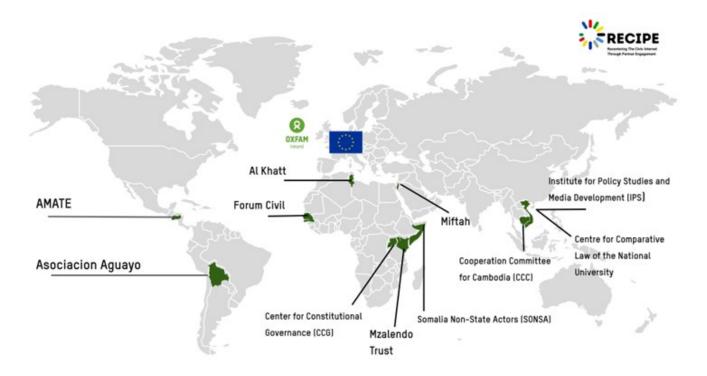




WHO

ReCIPE is led by Oxfam Ireland, alongside CSOs from 10 focus countries:

- Cambodia: Cooperation Committee for Cambodia (CCC)
- Somalia: Somalia Non-State Actors (SONSA)
- Vietnam: Institute for Policy Studies and Media Development in Vietnam (IPC) and Centre for Comparative Law of the National University (CCL)
- Tunisia: Al Khatt
- Kenya: Mzalendo Trust
- Uganda: Center for Constitutional Governance (CCG)
- Occupied Palestinian Territory: The Palestinian Initiative for the Promotion of Global Dialogue and Democracy (Miftah)
- El Salvador: AMATE in El Salvador
- Bolivia: Asociación Aguayo, in collaboration with Fundación Intenet Bolivia
- Senegal: Forum Civil









TERMINOLOGY

- Activist: A person who believes strongly in political or social rights-based change and takes part in activities such as public protests to try to make this happen.
- Blackmail: The act of demanding money from people or forcing them to do something by threatening to reveal private information about them or to harm them.
- Cyber-attack: An attempt by an individual or organization using one or more computers and computer systems to steal, expose, change, disable or eliminate information, or to breach computer information systems, computer networks, and computer infrastructures.
- Cyber-bullying: Bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms and mobile phones.
- Cyber-harassment: Harassment via the use of digital technologies. It can take place on social media, messaging platforms and mobile phones. It is repeated behaviour aimed at threatening, scaring, shaming, and silencing those who are targeted.
- *Digital abuse*: The use of technology to monitor, stalk, bully, harass, threaten, control or impersonate another person.
- *Digital security/safety:* Practices and tools used to protect an individual's or organisation's online identity, data and other assets.
- Digital/online violence: The use of digital technologies or the internet to cause, facilitate or threaten violence against someone, that results in (or is likely to result in) physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstances, characteristics or vulnerabilities.
- Encrypted messages: (also known as secure messaging) Communications using the process of asymmetric, end-to-end encryption in such a way that only the sender and receivers of the messages or files can decrypt them and no third-party controls the cryptographic keys. Examples of tools for encrypted messaging are Signal and Proton Mail.
- Fake news: False or misleading information masquerading as real news.
- Hacking: (also called cyber hacking) The use of unconventional or illicit means to gain unauthorized access to a digital device, computer system or computer network. The classic example is a cybercriminal who exploits security vulnerabilities to break into a network and steal data.
- Human rights defender: Someone who, individually or with others, acts to promote or protect human rights in a peaceful manner.
- Misinformation: Inaccurate information that is unwittingly shared.







- Disinformation: Inaccurate information that is deliberately created and distributed with an intent to deceive or do harm.
- Online Defamation: Also known as "internet defamation" or "cyber-libel," the online publication of one or more false statements about another person that unjustly harms their reputation.
- Online privacy: Freedom of individuals to choose who can access their personal information and data while using the internet.
- Online Violence Against Women: Violence against women and girls that is perpetrated through the internet.
- Technology- facilitated gender-based violence: Any act of violence (or threat thereof) rooted in and enabled by discriminatory gender norms that is committed, assisted, aggravated or amplified by the use of technology. It includes non-internet-based violence such as stalking via GPS devices as well as violence through internet-connected devices and in online spaces such as distributing online intimate images without consent.
- *Phishing*: A technique for attempting to acquire sensitive data, such as bank account numbers, through a fraudulent solicitation in email or on a web site, in which the perpetrator masquerades as a legitimate business or reputable person.
- Zoombombing: When people who have not been invited enter Zoom meetings to cause disruption. Such disruptions can be mild, or can include racist, hate, or pornographic material.







OBJECTIVE OF THE ASSESMENT

As part of the ReCIPE project inception phase, several common themes have been identified among the key issues in the focus countries related to the digital ecosystem:

- 1) Citizens and civil society organisations alike lack basic awareness of digital rights, access to digital resources and digital literacy, as well as the knowledge and tools to protect themselves from online threats.
- 2) Governments control the digital space, either to suppress freedom of expression online or to actively target CSOs and digital rights defenders for cyber-attacks, harassment & intimidation and/or surveillance.

The aim of this assessment is to find out more information about the current digital context, the issues people are facing and how these could be addressed from the perspective of civil society organisations, activists and community members in the Global South.

More specifically:

- Gather information on digital literacy and internet use, especially among members of the communities/countries where ReCIPE will be implemented.
- Increase knowledge of the different contexts, challenges and opportunities related to digital rights in the target countries.
- Generate ideas for advocacy activities at national and international level that could be implemented throughout the duration of the project.
- Identify potential partners to work with or be part of a network within one of the main activities of the project.







METHODOLOGY

This assessment is based on a survey launched in 9 of the focus countries targeted by the ReCIPE project in July 2024: Bolivia, Cambodia, El Salvador, Kenya, Occupied Palestinian Territory, Somalia, Tunisia, Uganda and Vietnam. The survey consisted of 87 questions addressed to community members, members of civil society organisations working in the field of human rights and/or digital rights, journalists and digital rights activists.

Depending on the country, the survey was completed by the respondents themselves or by an external consultant hired to collect data from the respondents. In all cases, the framework and objectives of the survey were defined in advance and adapted to the expectations and needs of each country through a Terms of Reference document.

The survey was divided into the following components:

- Information on connectivity and internet access
- 2. Digital literacy and information on the use of the internet and social networks
- 3. Digital violence and digital safety: knowledge and experiences
- 4. Capacity and resources of civil society organisations
- 5. Current measures to address and prevent digital violence
- 6. Proposed actions to address and prevent digital violence

Other reports produced by the various country teams as a result of discussion-based workshops with CSO members were also taken into account to validate and complement the survey results in order to draw more accurate conclusions. These reports are internal, but do not hesitate to contact the ReCIPE team for more detailed information.

It should be noted that not all respondents answered all the questions included in the survey; depending on the profile of the respondent, they answered the components of the survey relevant to them. Therefore, not all questions were addressed to all respondents.

Throughout the report, particular attention was paid to specific gender and age issues, which is why some sections highlight findings related to women and non-binary people who responded to the survey or participated in the workshops.







PRACTICAL CONSIDERATIONS

- As indicated above, the assessment has a geographical component, focusing on the 9 countries mentioned above in 3 regions: Latin America, Asia and Africa, with the exception of Senegal where activities had not yet started at the time of the survey.
- In some countries, focus groups were held to present and discuss the results of the survey and to cross-check information. However, this report is mainly based on the survey with its closed and open questions.
- Given the diversity of contexts, some specific questions or concepts were addressed in a more general manner in order to avoid raising sensitive issues, lack of response or potential threats to respondents or partners.
- Some of the respondents were targeted and pre-identified because we needed their technical expertise, experience or involvement in the field of digital rights. As this is a very specific profile, the number of CSO members or activists interviewed is lower than the number of community members providing information on their access to and use of the internet, which is higher.
- The number of people interviewed, and the profiles were decided by the country teams and were not the same in all countries. The totals for the two main profiles are 29% were members of CSOs or other social groups or collectives and the 71% were community members of the community.
- The sections on connectivity, access to the internet and digital literacy are answered by members of some communities in the ReCIPE countries. The remaining sections are answered by digital rights experts, activists and members of CSOs working on digital rights. The target population varied from country to country, as mentioned in the previous section.
- The study is based on a representative sample compared to the total population of each country. It may therefore be limited in terms of representativeness.
- The impact of digital threats, digital literacy, knowledge of digital rights and the digital context in the country are not the same in all countries. Throughout this report we refer to the general data for all countries together. For more details by country, see some graphs in Annex.
- In some sections of the report, the assessment makes a distinction by gender, including women and non-binary people in one group. However, less than 1% of people identified as non-binary (6 people in total). This percentage of non-binary people may be low compared to other countries; this may be due to some of the contexts where gender is a sensitive issue. This means that some of the men or women who have experienced digital violence or other digital harms may identify as part of the LGBTQIA+ community, which is considered a vulnerable population in some countries, have not been fully identified in this report.

Despite some limitations, we believe that the findings and conclusions of this survey are consistent, and that the data are sufficiently accurate given the diverse experiences of the respondents, the knowledge and previous studies conducted by some of the more technically competent people interviewed, and the neutrality of the process. Overall, it provides a useful snapshot of the current digital landscape, threats and opportunities to inform the ongoing implementation of the ReCIPE project.

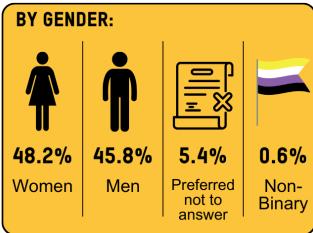


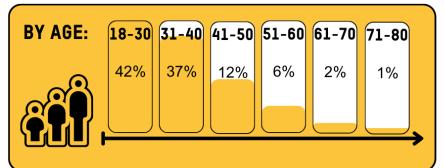


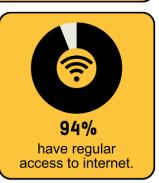


MAIN DATA ON PARTICIPATION









are members of a human rights organisation or 29% involved in human rights work.

77%

of those working or involved in the digital rights sector are members of an NGO.

76%

Do not have professional experience related to digital rights

12%

are members of a feminist collective.

WOMEN'S MAIN OCCUPATIONS:



Business



T_• Social and health



Housewife



Teaching

Other areas of work

MEN'S MAIN OCCUPATIONS:



Business



Social and health



Agriculture/ livestock



Transport



Other areas of work







SUMMARY OF THE RESULTS

Key findings on internet access and digital literacy

This part of the study focused on community members to learn more about how they use the internet and social networks, what knowledge they have and what challenges they face.

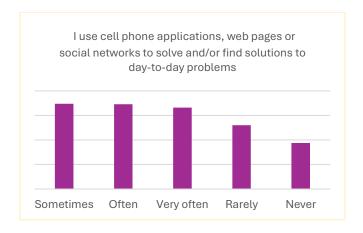
Access to the internet is widespread, with 94% of the population having access to the internet. The most common places to access the internet are at home or at work. However, this is not the case when we zoom in by age: although there are fewer respondents aged 41 and up, 19% of this age group say they do not have access to the internet and they connect from home, work, family or friends' homes, or other places. The amount of people without internet access increased with age; 28% of those aged 51 and up were without access to the Internet. Furthermore, 25% of women aged 40 and up do not have access to the internet, compared to 15% of men in this age group. There is therefore a significant digital divide based on age, and not just between the sexes.

The main purposes for which people use the internet are, for around 90 per cent of the population surveyed, as follows:

- Searching for information, using search engines such as Google
- Communicating (chatting or calling) with others
- Sharing documents such as photos, videos.

For banking transactions, work purposes and/or the management of government services or the mayor's office, the use is less widespread, with the percentage of respondents ranging between 55 and 65 per cent.

According to the data, the use of the internet to solve and/or find solutions to everyday problems is common among the target population, with around 50% of respondents using mobile phone applications, or websites.



The use of artificial intelligence (ChatGPT / Dalle) is less common in the ReCIPE countries where the survey was carried out, with a usage rate of 31%. The same applies to e-learning, with a similar rate of less than 40%. 36% of respondents have taken e-learning courses via

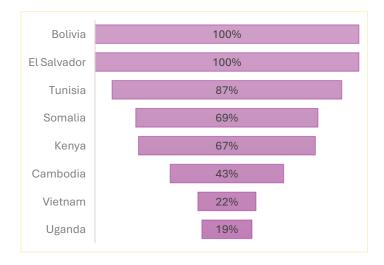






a learning platform.

The most common use is for private purposes and less than 30% of community members surveyed intend to use the internet to publish information on human rights, politics and/or social issues. Below are the members of the community by country, who have the most initiative and motivation to post, in ascending order.



Digital literacy is quite widespread. **The majority of the population is also familiar with the internet and its functions,** with none of the following actions falling below 50%, which means that, with a few exceptions, the use of digital technologies is quite widespread.

Actions	%
Chat using WhatsApp, Facebook Messenger, or similar applications	95 %
Send and receive text messages	94 %
Make a call using WhatsApp, Skype, Telegram, Facebook or similar	92 %
Save contacts, photos, music, videos or web pages and they know where to find them later	91%
Send contacts, texts, photos, music, videos or web pages to other people using a mobile phone	91%
Turn on, shut down, charge, and restart a computer	81%
Send and receive voice memos	80 %
Send and receive emails	60 %

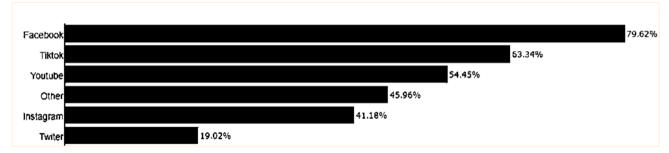
By age, from the age of 40, the percentage of respondents who are familiar with internet functions such as using search engines for information, having a call or chat via WhatsApp, Skype, Telegram, Facebook, sending and receiving texts, closing contacts, photos, music, videos, is lower—ranging from 70 to 85%, and the figures that are closer to 85% are those related to social networks. Again, these figures decrease as we advance in age, from 50 years of age and above.





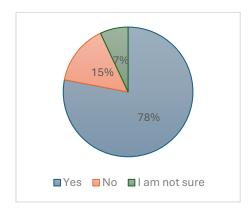


The most used social media network is Facebook, followed by TikTok and YouTube as shown in the table below. The top 6 are as follows:



Perceptions of misinformation and disinformation are mixed when it comes to information circulating on the internet and the risks associated with it. When asked if they know how to distinguish between true and false information when using the internet, some 43% of respondents say they do, and 26% say they sometimes do. On the other hand, 72% of respondents have not shared information on human rights, politics and social issues.

The risks of sharing personal information when using social networks or the Internet, and the precautions one should take, are generally understood by most of the population, as shown the graph below.



The older they get, the less they feel they know about how to distinguish between true and false information when using the internet, and about the risks of sharing information. Over the age of 40, 71% think they know about the risks of sharing information online and 9% are not sure. And around 72% have never posted information about human rights, politics or social issues, this last figure being similar to the overall population surveyed.

The cost and connection to the internet can be expensive or very expensive for more than 60% of the population surveyed. The connection in the target countries is considered as regular or bad by around 68% of respondents. Even if the internet is accessible, it can still be a challenge for a part of the population with lower incomes or in some geographical areas such as rural or isolated locations.







Internet access and digital literacy by gender

When looking at digital literacy and access to the internet among women and non-binary respondents, the main findings are shown below:

26% of women and non-binary respondents are members of a human rights organisation or involved in human rights work, with a similar proportion of men. 27% of the women respondents are members of a feminist collective.

The risks of sharing personal information when using the internet and the precautions to take are well understood by more than 76% of women and non-binary people; 15% do not understand and 8% are not sure. Among men, 80% say they understand the risks of sharing personal information.

The social networks, Facebook, TikTok and YouTube, are the most used by women, while the same platforms are also most used by men. Google is the most used search engine for finding information.

The digital literacy of women and non-binary respondents can be described as good: more than 80% know how to store contacts, photos, music, videos, etc., make calls and chat on platforms, send voice memos or send and receive text messages on mobile phones. On the other hand, less than 50% of women know how to send an email. When it comes to financial and administrative procedures via the internet, they do use it, but not as much as other figures more related to social life. This could mean that respondents are more familiar with using mobile phones and applications, as the figures for mobile phone use are higher.

More than 70% have not used ChatGPT. On this point the differences between the sexes is small, with only a 2% difference in percentages.

More than 66% of women consider the cost of the internet to be expensive or very expensive, similar to men at 60%. The places where they connect are the same as for men: first at home, then at work. Perhaps the perception that the internet is more expensive for women than for men is because women's salaries are generally lower than men's.

Although there is not much difference between men, women, and non-binary people in terms of digital literacy and internet use, women are still less likely to have access to the internet and to use some of its features. While 5% of men do not access to the internet, 6% of women report not having access to the internet and depending on the country, the rate can be higher, such as in Uganda where 7% of women and 6% of men report not having access to the Internet. 42% of women don't know how to send or receive emails, while 37% of men don't know how to send or receive emails. 79% of women know how to turn on, turn off, charge and restart a computer correctly, compared to 84% of men. This gender gap increases with age.

As mentioned above, the figures are more similar between women, non-binary people, and men in regards to using social networks. Though a slightly higher percent of men surveyed are familiar with social networks, the difference is minimal, with more than 85% of all gender groups using them

However, women are slightly more likely to use the internet for administrative purposes - this could be due to the fact that women are more likely to be responsible for this task at







home. More specifically, 67% of women make enquiries or manage services provided by the government, the mayor's office or organisations, and 59% carry out banking transactions or use platforms such as TIGO Money¹, local banks or Western Union to make payments or withdrawals. Among men, 63% make enquiries or manage services provided by the government, the mayor's office or organisations, and 51% carry out banking transactions. The breakdown by country is as follows

Women who make enquiries or who manage services provided by the government, the mayor's office or by organisations.

Women who bank or use platforms to pay, transfer or withdraw money

	organisations.	
Bolivia	100%	100%
El Salvador	100%	100%
Cambodia	65%	100%
Vietnam	100%	83%
Kenya	50%	100%
Somalia	75%	56%
Uganda	65%	55%
Tunisia	84%	42%

This table also shows that, with very few exceptions, there is general trust and acceptance of digital government services and digital financial platforms in all countries. In almost all countries, usage of these services is above 50%.

_

¹ Tigo Money is a digital wallet that sends and receives money, pays bills and utilities, and tops up.







Key findings: knowledge and experiences of digital violence and safety

This section is based on responses from people working or involved in the field of human and digital rights, activists, or journalists and members of civil society organisations.

Digital violence has not been experienced by all respondents: only 28% are sure that they have not experienced any kind of digital violence in the last year, while **35% have been victims, 20% are not sure and 19% prefer not to answer**. In addition, 32% think they have been affected because of their gender and 35% are not sure. These figures are quite significant given the widespread use of the internet by the population. The number of people who are not sure if they have been a victim of digital violence is also relatively high, with some respondents to the question 'What do you understand by digital violence?' - that they didn't know or weren't sure.

Another significant data point is that 44% of people who have spoken out about social issues have been the target of digital violence. Depending on the country, this figure increases significantly. By profile, the percentage of people who have been the target of digital violence because of their position or profile in certain campaigns is as follows:

Working in an NGO, collective association for the	37%
defence of human rights	
Working in an NGO defending digital rights	54%
Political activist journalist and/or parliamentarians	69%
(individual person or freelancers involved in digital	
rights)	
Women candidates for elections, and women local	29%
council members	
Member of Oxfam	31%

The most common forms of digital violence they have experienced, in percentage terms, are as follows:

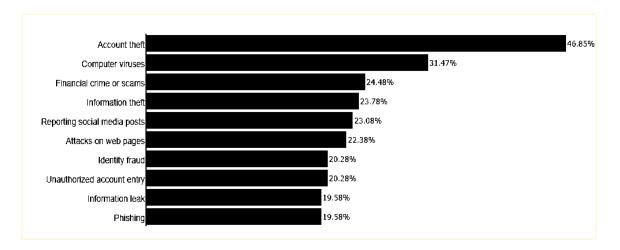
Actions	%
Insults through messages or social networks	73
Harassment	50
Bullying through messages	44
Public defamation on the internet	41
Direct or indirect threats of physical or sexual violence	33
Being spied on by a close person	26
Threat of publication of intimate, erotic or sexual content	12
Dissemination of intimate images	9
• Other	7





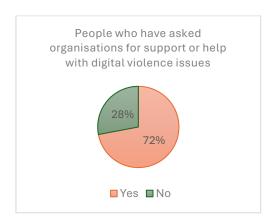


In terms of digital security problems, around 50% of respondents claim to have experienced different types of problems. The most common digital security problems are account or information theft, computer viruses, financial crime, identity fraud, website attacks or phishing, as shows the table below.



Related to the frequency, over 50% of respondents experienced these problems either frequently (defined as every three months) or occasionally (twice a year). The number of people who have never experienced a digital security problem is 4%.

In the case of the digital security problems mentioned above, only 28 % of respondents have sought support or help from CSOs and 29% reported these problems to an official authority.



Protective measures: 62% of respondents do something to protect themselves, while 38% of people currently do not take any measures to protect themselves from external attacks. This is notable, considering that most respondents say they are aware of the risk of sharing information. The most common protective measures are

- 1. Block and report.
- Do not share personal information.
- 3. Do not reveal my passwords to anyone.
- 4. Have a hard-to-guess password and unlock pattern.
- 5. Do not install unknown applications.
- 6. Verify profiles of those who receive invitations or friend requests.
- 7. Update device.







- 8. Do not chat with strangers.
- 9. Configure the privacy of my social networks.
- 10. Encryption of content and/or use end-to-end encryption messaging applications.
- 11. Contrast the information and make sure if it is fake news.
- 12. I use end-to-end encrypted messaging applications.
- 13. Constant review of my banking transactions (Ensuring that in my bank account there are no movements that I have not made).
- 14. If you receive sexual or violent content, do not share it, report and denounce.
- 15. Talk about what happened.
- 16. Report people who make you uncomfortable.
- 17. Ask for help.
- 18. Report to the authorities of my country.
- 19. Remote wipe.
- 20. Document attacks.

In terms of digital violence at an organisational level, the most common cases reported, in descending order, by respondents who were aware of it in their organisation or among the people they work with, are:

Actions	%
Harassment	33
Insults through messages or social networks	32
Fake news	31
Bullying through messages	29
Public defamation on the internet	24
Blocking of accounts	22
Removal of social media content	20
Direct or indirect threats of physical or sexual violence	19
Violation of privacy	18
Illegal use of personal data	16
Blackmailing	11
Being spied on by a closed person	11

Around 75% of people do not know how these cases had been dealt with. For those who do know how the case was handled, the information that they have is that the most serious cases, such as rape or abduction after contact through fake profiles, were reported to the authorities; in the cases that were reported, respondents claim that there were no major consequences for the perpetrator, which makes them distrust certain institutions. In other cases, websites were restricted, the content was removed, or accounts were blocked.

When looking at the victims, according to the respondents the most common victims of digital violence are women and girls, members of civil society organisations/NGOs and young people:







Companies	44
Public figures (elected officials, celebrities, intellectuals, business leaders)	120
Public institutions and government	120
Young people	133
Civil society organizations/NGOs	156
Women and girls (including women's rights organizations)	215

By age: Minors were not included in this survey. From respondents aged 18 to 30 years, there are no major changes compared to the general figures; about 38% have experienced some form of digital violence in the last year, more than those who have not experienced any form of digital violence, and 25% are not sure. A high proportion of this age group reported experiencing other types of digital problems — 60% experienced digital problems including account theft. If we look at the rest of the population aged 30 to 40, the percentage of those who have experienced some kind of digital problem is around 26%. However, 45% of those aged 40 and over have experienced some form of digital violence in the last year, and 38% have experienced some form of digital violence because of their gender. 26% are not sure if they have experienced digital violence. Also, 64% of respondents from the age of 40 have experienced some form of digital security problem (e.g. account theft, social networking, etc.). Adults in their 30s are therefore less likely to be affected by digital violence, and as people get older, the risks associated with using the internet may increase, which may be related to the fact that they are less familiar with the features of the internet, as shown in the previous section of the report.

In terms of their understanding of digital violence, the majority of respondents have some idea of what it is. There are some who don't know or think of specific apps or websites when we talk about digital violence, but generally they have a sense of what the term 'digital violence' refers to:

"Abuse of data and information to serve another person's pleasure"

"Any form of intimidation from the use, sharing of images, rude comments, information, clips, etc. causing the victim to be hurt, abused, worried...."

"Basically, when others (peoples or entities) threaten or harass you or use your personal information or privacy for their own benefits in order to harm"

"Behaviour that uses technology, the internet, or online platforms to harm, threaten, harass, or abuse others. Exemples: Cyber-bullying, online sexuel harassement"

"C'est la violence à travers les réseaux sociaux comme l'incitation à la haine ou la diffusion des messages dangereux qui touchent aux droits des hommes »

"Cuando se hace difamación o criminalización de las mujeres u hombres, se hackean archivos confidenciales"







"Digital violence is basically a type of gender-based violence by using technical devices and digital platforms. Such violence may include cyber-bulling, online harassment, cyber stalking, non-consensual sharing intimate photos and videos, etc."

"Digital violence is the act of abusing or harassing others over the internet, causing psychological and emotional harm"

"Es la agresión a través de redes sociales o medios digitales hacia otras personas o una persona en específico"

"This is an act of insulting the honour and dignity of individuals or organizations in the online space, both indirectly and directly"







Knowledge and experiences of digital violence and safety by gender

This part specifically includes information from women and non-binary people working or involved in the field of human and digital rights

In the case of digital violence, around 50% of women and non-binary people surveyed say they have been victims of digital violence in the last year, while around 20% are unsure and 33% say they have not been a victim of digital violence.

Around 50% say they have experienced **gender-based digital violence**; around 15% are not sure and 36% say they have not experienced gender-based digital violence. **This means** that half of women and non-binary people have been victims of digital violence due to their gender, which is a significant figure.

Again, the percentage of women and non-binary people who are unsure whether they have experienced digital violence or technology-facilitated gender-based violence is quite high at 20%, which suggests that many respondents may have limited awareness and understanding of digital rights and the risks on the internet, which in turn limits their capacity to take appropriate measures in order to protect themselves and report it. This data shows that although people claim to be aware of the risk of sharing information online and feel comfortable online (as shown in the previous figures), the percentage of all respondents (including women, non-binary people and men) who are unsure whether they have experienced digital violence is relatively high at 20%, and 19% saying they 'prefer not to answer'.

Among men, around 35% consider themselves to be victims of digital violence and 27% have experienced some form of gender-based digital violence. Women are therefore more likely to be victims of digital violence in general and gender-based violence in particular. This also confirms respondents' perceptions of the most common digital rights violations.

Another key data point is that more than 50 % of these women and non-binary people believe they have been the target of digital violence as a result of their work or lending their voice to certain campaigns. In the case of men, around 40% of men think they have been the target of digital violence because of their work in human rights or digital rights, or because they have lent their voice to certain campaigns.

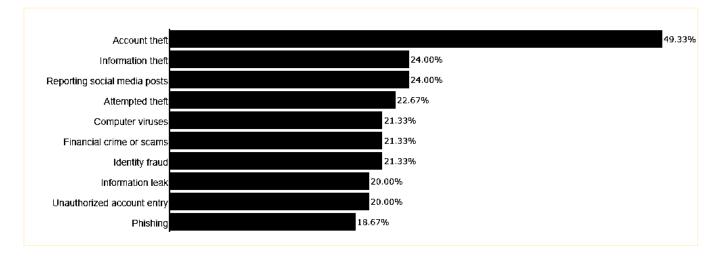
In decreasing order, the main issues facing women and non-binary people are:

Insults through messages or social networks
Harassment
Bullying through messages
Direct or indirect threats of physical or sexual violence
Public defamation on the internet
Being spied on by a closed person
Dissemination of intimate images
Threat of publication of intimate, erotic or sexual content

Around 60 per cent of women and non-binary people surveyed have experienced digital security problems, and below are the main ones:







In terms of age, 38% of the total population of women surveyed have experienced digital violence in the last year, while 25% don't know if they have. Amongst women surveyed aged 18-30, these figures are slightly lower; 36% of women aged 18-30 have experienced digital violence, while 16% don't know if they have. However, this figure rises to 44% when we look at women under 30 who have experienced digital violence as a result of lending their voice to certain campaigns.

In the case of women over 40, 58% said they had been a victim of digital violence in the last year and 15% were not sure, which also means that **women under 30 are more unsure if they have experienced digital violence**, meaning they are potentially less able to categorise. For those aged 40 and over, 62% have experienced digital violence because of their gender, which is a significant figure.

It is important to note that **most of the women and non-binary people did not seek support or help from a CSO after experiencing any type of digital violence;** only 21% did. Some of them asked their friends for support or who to turn to, rather than a professional expert. 27% reported it to a formal authority such as the police.

A high percentage (82%) of women and non-binary people say they do something to protect themselves in the digital world. The main practices are:

- Block and report - Don't give your password to an anonymous person - Don't share personal information - Have a password that is hard to guess - Check the profiles you receive invitations from - Don't chat with strangers - Update your devices - Configure your social network's privacy settings - Don't install applications you don't know - Encrypt content - Constantly check your banking - If you receive sexual or violent content, don't share it, report it and denounce it.

Digital rights competencies

41% of women and non-binary people have received digital rights, compared to 26% of men. And the most common modality for both genders was face-to-face.







Key findings on current measures to prevent digital violence

This section details the measures taken by governments, companies and other institutions to protect the population from digital violence, as well as respondents' perceptions of these measures.

The perception about government action: 66% of respondents believe that governments are not doing enough to prevent and combat digital violence and protect people. 48% believe that the current implementation of policies and regulations in their country is not effective, and 35% are not sure, which is a significant figure in terms of people's knowledge of these issues, given that this question was answered by people involved in human rights field. In some countries there is unanimity on the lack of government action.

Regarding questions about government action, given the context in which the survey was developed, we consider that some respondents did not want to question the government's role in digital rights because of possible repercussions against them.

The main reasons why respondents think the government is not doing enough are:

- Lack of specific policies or inadequate legislation.
- Existing laws are not enforced.
- Governments do not have the resources or institutions have limited capacity.
- Bank fraudsters are never detected or apprehended.
- Impunity and need for more sanctions.
- Lack of awareness leads to under-reporting, leaving the judicial system with very few reference cases to work with.
- Lack of cooperation and coordination.
- Some governments use digital violence against their citizens.
- Lack of real interest.

In terms of **perceptions about private sector action**, respondents think that the private companies are putting in place some actions to address digital violence, such as:

Creating courses on digital violence

Raising awareness

Content moderation, i.e. deleting violent content

Mechanism for reporting violence

Encrypted messaging on messaging networks

Restrict connection times, views, photos...

Complaints committee

Some social networks do not ask for a phone number

Spreading prevention strategies with fraud attempts related to your company

More specific privacy settings







However, from the respondents' point of view these actions by both the private and public sectors are not enough. They see that the issue is being addressed, but not in a sustainable way, with sporadic actions rather than a continuous strategy, leading to the reproduction of gender and cultural stereotypes and a significant digital divide. In addition, respondents report that companies do not have protocols, are not transparent with their information and do not have a privacy policy. For about half of the people surveyed, the current implementation of policies and regulations in their country is not effective.

Civil society organisations and other social groups are currently focusing on preventing and responding to digital violence. Their actions include:

- Awareness workshops
- Educational campaigns
- Working on literacy programmes to reduce the digital divide
- Trainings
- Prevention and awareness campaigns
- Victim support and monitoring
- Protection mechanisms and tools
- Direct support to and monitoring of victims of digital violence
- Investigations/enquires
- Identification and blocking of potential aggressors
- Artistic activities for awareness building e.g. theatre, exhibitions
- Proposals for legislative reform







Gender differences in current measures to prevent digital violence

The current implementation of policies and regulations to protect people from digital violence is not seen as effective, and respondents generally don't know what policies public institutions have in place to prevent and respond to digital violence. The ones they are most aware of are related to cybersecurity. They also don't believe that these laws have identified male violence and other gender factors. For them, many people are not aware of digital violence and the victims are often afraid to report digital violence. Some of them feel that the government uses violence against its opponents and that there is no point in reporting it. Furthermore, even if women and non-binary people feel that they are more affected by digital violence, they don't report it because they feel that no one will be arrested and it is not a priority for the institutions, there is no prosecution of the digital crime.

To respond to digital violence, some feminist organisations support victims of digital violence; others are currently working on cybersecurity, providing digital literacy training to reduce the digital divide, and proposing legislative changes. And in some cases, they are proposing political advocacy to develop policies to address digital violence.

Men have a similar view of current policies and regulations and are also sceptical about their effectiveness and the real prosecution of the perpetrator. They also feel that data protection is not respected and that there is a lack of equipment.

Finally, when asked how the organisation they work with promotes women's economic empowerment, feminist principles on digital platforms and the right to live free from violence in the digital environment, the population surveyed reports the following actions: workshops, media campaigns, public awareness and digital education programmes, such as organising webinars and providing materials to improve understanding of cyber violence, supporting victims, and promoting specific policies and regulations, which is very similar to the response also given by men.

"My organization plays a vital role for promoting women's economic employment feminist principles on digital platforms and the right to live free from violence in digital environment by giving them a platform to talk and give a voice to them sharing their ideas and information for people"

"From the transversality of feminist principles in all the actions, to the access of women in some of the trainings" "We conduct research on the impact of digital violence on gender and publish reports to raise awareness and drive action"







Key findings on proposals to prevent threats to digital rights

The actions proposed in this section are based on the views and contributions of respondents in the field of human and digital rights and are presented in the form of a set of recommendations for action.

According to the respondents, there are actions that could be taken by different actors to raise awareness about the fact that digital violence is a form of violence, discrimination and a violation of human rights, and other actions that could prevent or reduce this type of violence. These include:

By civil society actors:

- Identify the most vulnerable population.
- Bring together organisations in a network that aim to share and strengthen information on digital rights and violence and share information and empower civil society.
- Develop protocols for responding to digital incidents, i.e. for information, treatment and care in cases of digital violence.
- Focus on prevention rather than protection, have clear information and understand what aspects we need to protect in the digital environment.
- Share general data/statistics on digital threats and violence with other organisations to generate a public and media agenda.
- Propose definitions of what is meant by digital violence and, from these standardised definitions, generate prevention and awareness strategies for citizens.
- Develop advocacy strategies and identify existing public policies.

By social and/or educational actors:

- Identify the most vulnerable groups, which have also been indicated by civil society actors.
- Set up a victim support programme 24-hour helpline with a range of solutions tailored to victims.
- Focus on psychological support.
- Systematise support, complaints procedures, reporting channels and communication formats.
- Work on comprehensive content to address online violence and training teachers.
- The development of specific materials adapted to each population group and in their mother tongue.
- Reinforce and disseminate educational content.
- Make digital literacy compulsory in schools.
- Ensure access to prevention and care information for different sectors of the country, including more isolated areas or rural populations.
- Classify cases and take appropriate actions.

By governments or local authorities:

- Carry out a diagnosis of the state of the country in terms of digital violence.







- Develop a legal framework specific to digital violence and protocols.
- Increase sanctions, i.e. for those found guilty of perpetrating digital violence.
- Strengthen data protection legislation (not all countries have it).
- Establishment of a neutral, non-governmental body that has control over the management of a database of cases of digital violence, underpinned by legislation.
- Strengthen police and community response capacity.
- Increase resources for protection and justice.
- Socialise and research digital violence to make it visible with evidence.
- Further research and disseminate the effects of digital violence.
- Penal reform.
- There is still a need to improve the implementation of laws and to raise awareness of them.
- Need for anonymous reporting channels.

"The development of specialized legislation on digital violence" "Regulation needs to be supported, but with an intersectional feminist and human rights-based approach"

"Punishment according to the Criminal Code"

By technology companies:

- Improve collaboration between technology companies to improve online safety in communities and countries.
- Improve internet governance policies.
- Take responsibility for investing in prevention and support.
- Establish agile response mechanisms so that content can be removed immediately.
- Develop culturally relevant content monitoring policies.
- Improve reporting mechanisms and design protocols for information treatment.
- Tackle the digital and security divide.
- Have a more effective response when cases of digital violence do occur.
- Provide information to society at large to educate people on how to protect themselves.
- Be more accountable and transparent.
- Train staff, including outsourced staff.
- Respond more quickly to police requests in cases of gender-based violence, including for telecom companies.
- Have a mobile application to access and create the report quickly and instantly. It must be available at all times.
- Access stakeholder meetings with specific demands.

By activists:

- Actively advocate for laws that criminalise all forms of digital violence, including cyberbullying, online harassment and hate speech.
- Influence on policies related to digital rights.
- Attend court cases and raise awareness among police and judicial officers.
- Support victims through to the end of a trial and resolution of the case.
- Amplify voices to raise awareness and disseminate evidence of abuse or digital violence.







- Starts with a better understanding of their needs and proposing laws and policies in a collective action between civil society organisations and independent activists.
- Work with legal experts to ensure proper investigation and prosecution.
- Collect data and research.
- Educate the community and run workshops to build citizens' capacity on the issue.
- Monitor and redress rates.
- Raise the issue with digital policy makers and regulators.
- Engage victims to share their stories.

"Activists need to be empowered to give a voice to the voiceless" "Support the victims until the cases are resolved, and demand that the resolutions are conclusive" "Los activistas podrían investigar y conocer como comunicarse con la población meta sobre violencia digital de género"

By the media and social networks:

- Produce and disseminate audiovisual materials on social networks to identify, detect and report digital violence.
- Carry out social media campaigns by segmenting and identifying the most vulnerable populations, for example: rural migrants, LGTBI activists, etc. These campaigns will also serve to identify, detect and report digital violence.
- Raise awareness of the potential dangers of social networking and what we can do to protect ourselves.
- Make the information in the social media more accessible, reliable and factual.
- Share general data/statistics on digital threats and violence with other organisations to generate a public and media agenda.

"There should be media coverage of the dangers of these social networks and how we can protect ourselves" "Undertake citizen driven campaigns, Civic engagement for civic actions (petitions and memos) to drive enforcement"

"Organisation des campagne de communication autour des droits numériques et de la sécurité numérique (podcasts, articles)."

By all actors to be people-centred:

- Respondents felt that there is a need to think about victims and to reach out to people who have been digitally abused and provide them with appropriate care and support, avoiding revictimization and giving priority to psychological support.
- Address the root causes of digital violence.







Specific proposals to protect against threats of digital violence, especially against women, girls, non-binary people or other minorities.

- Facilitate access to information, prevention and support for populations at risk, paying particular attention to rural areas, indigenous populations, women and non-binary groups, who feel very often neglected and underrepresented.
- Making the patriarchal sphere visible in the digital world. Increasing the fact of verifying that the content does not reproduce violence, misogyny, machismo, discrimination.
- Work with parents to accompany them in the use of technology by their children and young people.
- Develop specific legislation on digital violence with an intersectional feminist and human rights approach that addresses the root causes of digital violence.
- Take into account vulnerable communities, such as LGBTQ people in any proposals to investigate and punish acts of digital violence.
- Ensure that internal policies on digital violence and gender discrimination are clear, public and strictly enforced.
- Civil society organisations and feminist collectives should have a better understanding of what digital violence is and should organise themselves collectively to respond to it. It is important to have very clear, specific feminist training.
- Establish clear criteria for content policing. These should be non-discriminatory and based on human rights and the inclusion of vulnerable groups.
- Ensure that content monitoring policies are culturally relevant and verify that content does not reproduce violence, misogyny, machismo, discrimination, etc.
- Carry out a kind of classification of social networks in order to know what action to take according to each person's situation, trying above all to prevent. It is essential to offer a response adapted to the specific needs of the victim.
- Representation of civil society organisations before the state to make visible cases of gender-based violence.
- Strengthen the justice system by working with prosecutors, judges and police.
- Work on gender bias in companies.



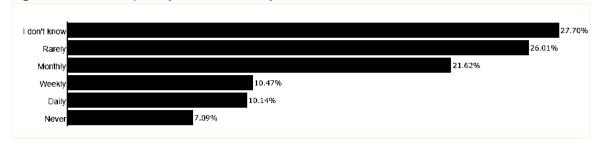




Key finding on capacities and resources of CSOs

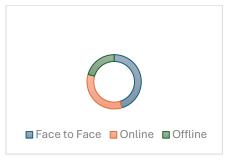
In terms of knowledge or handling of digital rights issues, it depends on the organisation— whether they have strong knowledge and solid experience or whether they feel they need to strengthen this area. But, in general, their perception of the organisation/group's knowledge or handling of digital rights issues is low, and they feel that CSOs have a base but need to deepen their knowledge and understanding of digital rights issues, more information related to data protection and prevention of gender-based digital violence and external threats. They would also like to increase their knowledge of national and international regulations, receive support for political campaigns and the prevention of external threats (hackers, government surveillance...) and receive staff awareness training.

The most common platforms and tools used by organisations are, in order of use: social networks such as Facebook, Instagram; email; website/blogs; cloud storage and finally collaboration tools (Teams, Trello...). Websites are generally hosted locally and around 50% have an IT support team, while 41% do not. In terms of organisations backing up their digital data, the frequency with which they do so is as follows:



Knowledge on digital rights, with the exception of some people working on digital rights in CSOs or activities also involved in this area, most respondents think that their organisation has no specific experience in work/actions/projects related to digital rights.

Around 28% of respondents reported having received training on digital rights and/or digital security and a similar proportion reported having received training on digital security or with a digital security component. Some areas for improvement in such training were identified as: improving the contextual factors of such training to make it more relevant to reality, practical exercises, sufficient time for practice, with a clear learning plan and objectives, and not just focusing on technical aspects. Broadening the knowledge to include protection and human rights and to include people with disabilities and other minority groups. Staying updated on emerging trends - AI, Chat GPT etc. This is the breakdown of the training modality they had:









In terms of age, 26% of respondents under 40 years old have already attended a training on digital rights and 49% of them were face-to-face. From 40 years old, the percentage is slightly higher with 33% of people having attended a training on digital rights. However, 68% said that they have not attended any training on digital security or training that includes modules on digital security.

Security issues can result from the work of CSOs, who do not share their work for security reasons and to protect themselves. It is also important to note that all CSO members and activists interviewed agree on the importance of working together to strengthen their voice on this issue and would like to be part of a network.

Digital rights network: Almost 90% of the CSOs surveyed believe that there is a need for a network and that they would be willing to be part of such a network. The respondents think that this network should be interactive, contribute to raising international awareness of human rights issues, take more measures to be protected in the face of digital threats, actively participate in or create multisectoral working groups focused on policy advocacy related to women's rights and digital security, consolidate efforts to ensure that grassroots organisations are well informed about the various leeks in the digital sector, research, campaigns, creation of resources...

Organisations need to strengthen their capacity on digital security, in particular to prevent external threats (hackers, state surveillance, etc.) and gender-based digital violence, and to increase their knowledge on the protection of personal data. Their work now focuses on raising awareness through social media, organising digital workshops and trainings, and communicating with beneficiaries through secure digital platforms.

The CSOs interviewed also believe that they should work more on a common understanding of freedom of expression in the virtual space, deepen the understanding of legal texts specific to rights and better understand the algorithms of each platform / digital space (trends).

They also identified a need in terms of resources: CSOs highlight the **lack of financial resources** for the development of technical equipment such as software.

Finally, there are also activists who don't belong to any organisation, but they are also asking for support, and made some suggestions, such as developing a digital security handbook, a crisis line and referral routes in critical cases.







RECOMMENDATIONS SUMMARY

This section is a summary of the main suggestions made by the respondents, but also by the participants in the workshops organised by some of the consortium members to collect more data and to cross-check and verify information. The following recommendations do not necessarily reflect the views of Oxfam but will be considered by the ReCIPE project team in the next phase of project implementation.

- Awareness-raising and training through a variety of means is therefore key, with information about the risks and how to deal with them when they arise targeted at different social groups, i.e. strengthening digital literacy and training in digital rights. Based on the mapping, this is a key point, as the percentage of respondents who are unsure whether they have been a victim of some form of digital violence ranges from 15% to 30%—a significant figure given the widespread use of the internet and the impact that this violence can have on our lives.
- Have networks or mappings of digital rights advocates with a collaborative and crosssectoral approach to address the complex and changing challenges of the digital environment.
- Put the issue of digital rights and safety on the international agenda, recognising that not all countries have the same problems, in order to protect people who feel insecure.
- Call for greater engagement and social responsibility by technology companies in the prevention of risks online.
- Call on governments to develop or **strengthen policies and laws that regulate the digital environment** and protect people.
- Request **governments to consult and consider the input of civil society actors** to improve and adapt laws and procedures to the real problems of digitalisation.
- **Promote policies that protect freedom of expression** online and ensure that technology policies and practices are consistent with the **principles of justice**, **equity and respect for human rights**.
- Improving coordination between government ministries, the media and civil society.
- **Identify the most vulnerable groups** and develop specific instruments to protect them, from the different levels of government (regional, local, etc.) to civil society. According to the mapping, women over the age of 40 are also part of the vulnerable population and there is an age and gender gap.
- Strengthening support and assistance mechanisms for victims of digital violence, abuse or any kind of threat on social networks.
- Support civil society organisations and/or activists who may need more information or training on digital rights, resources available to protect against threats and to use digital tools effectively, digital security, data protection, etc.







- **Enhance the ability to anticipate risks** associated with emerging technologies and to propose more robust and effective regulatory frameworks in response to developments.
- **Bridge the digital divide:** Advocate for policies that promote affordable and accessible Internet access; Improve infrastructure to expand access especially in rural and underserved areas. And, provide technical assistance and support to civil society organisations to build and maintain their digital infrastructure.







ACKNOWLEDGEMENTS

The ReCIPE project team would like to thank all the **individuals, activists, community members, journalists and members of civil society organisations** who took the time to answer the questions and share their personal and professional experiences, expertise and, in the case of those working in the digital rights field, their commitment to defending digital rights.

Oxfam offices and consortium partners who conducted the survey in their countries and also held workshops to cross-check information and consider further qualitative data.

Yahya Hussein and Juan Orellana from Oxfam for their ongoing technical support and availability throughout the process.

My colleagues Mia Marzotto and Daniel Pasquini for all their contributions to the document, to Fiona Kennedy for her help with the design of the document and Vera Melgari for her external review.







ANNEX













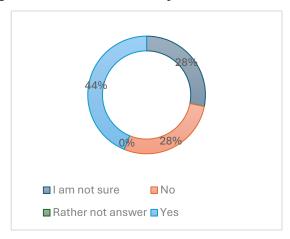




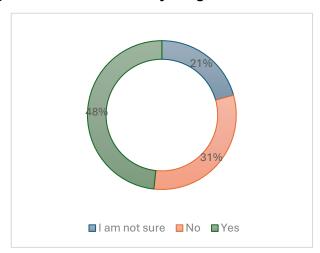


El Salvador

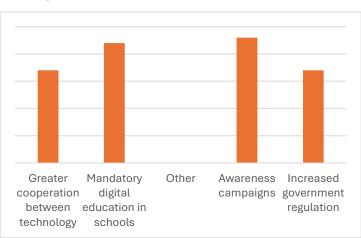
% of respondents who have experienced any type of digital violence in the last year



% of respondents have experienced any form of digital violence based on your gender

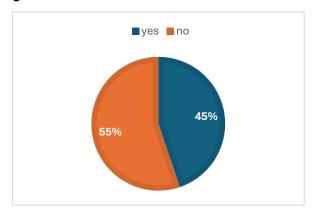


Actions that could be taken to improve online safety and security in your community or in your country

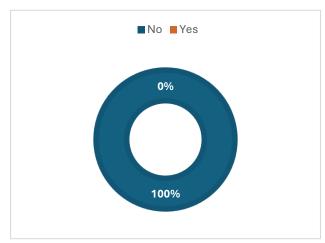


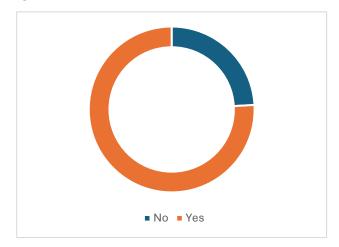
Tunisia

As a result of your work or lending your voice to certain campaigns, have you ever been the target?



% of respondents who think their government is doing enough to prevent digital violence



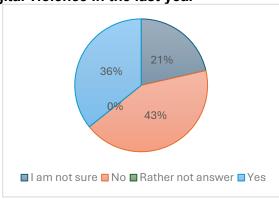




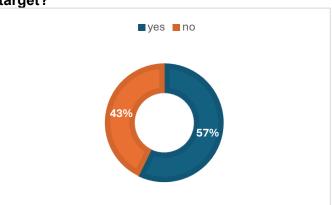




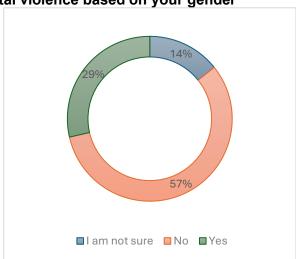
% of respondents who have experienced any type of digital violence in the last year



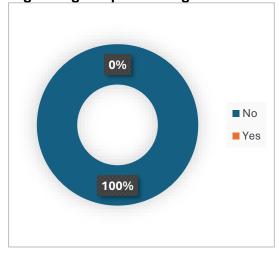
As a result of your work or lending your voice to certain campaigns, have you ever been the target?



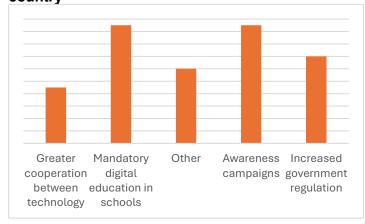
% of respondents have experienced any form of digital violence based on your gender



% of respondents who think their government is doing enough to prevent digital violence



Actions that could be taken to improve online safety and security in your community or in your country





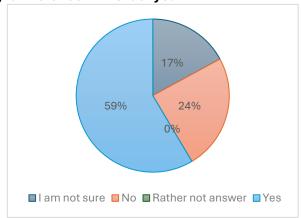




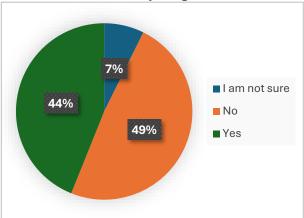


Kenya

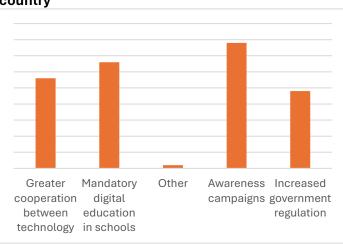
% of respondents who have experienced any type of digital violence in the last year



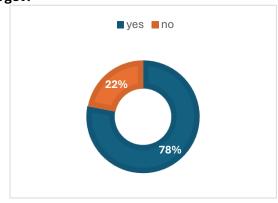
% of respondents have experienced any form of digital violence based on your gender



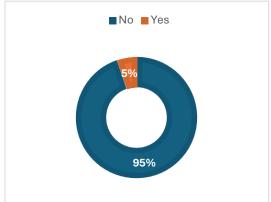
Actions that could be taken to improve online safety and security in your community or in your country

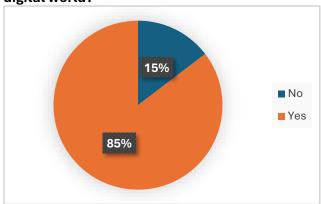


As a result of your work or lending your voice to certain campaigns, have you ever been the target?



% of respondents who think their government is doing enough to prevent digital violence





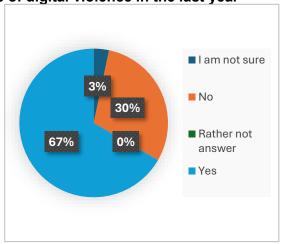




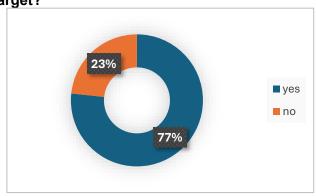


Bolivia

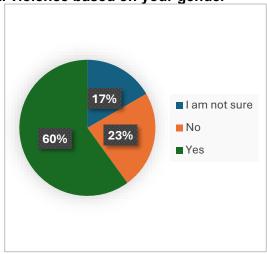
% of respondents who have experienced any type of digital violence in the last year



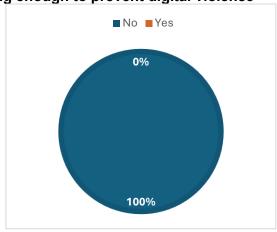
As a result of your work or lending your voice to certain campaigns, have you ever been the target?



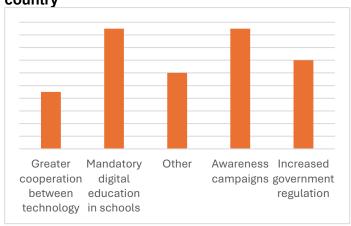
% of respondents have experienced any form of digital violence based on your gender

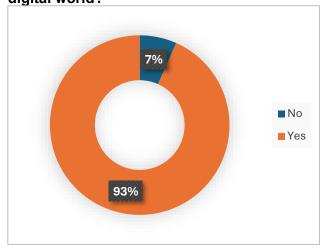


% of respondents who think their government is doing enough to prevent digital violence



Actions that could be taken to improve online safety and security in your community or in your country





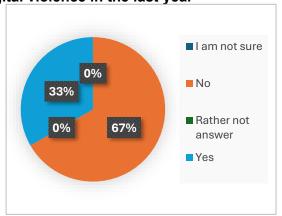




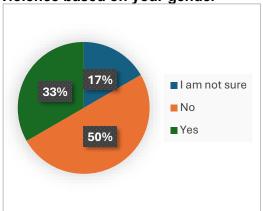


Uganda

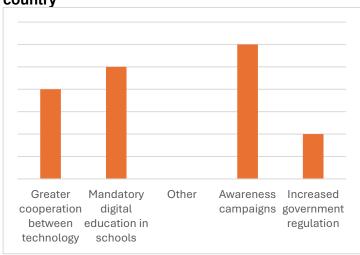
% of respondents who have experienced any type of digital violence in the last year



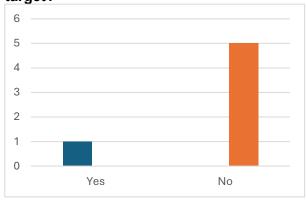
% of respondents have experienced any form of digital violence based on your gender



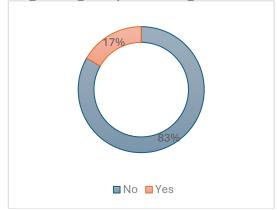
Actions that could be taken to improve online safety and security in your community or in your country

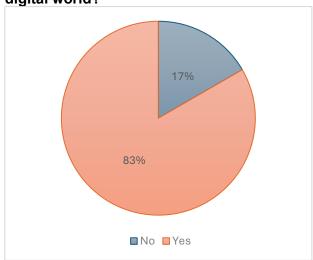


As a result of your work or lending your voice to certain campaigns, have you ever been the target?



% of respondents who think their government is doing enough to prevent digital violence





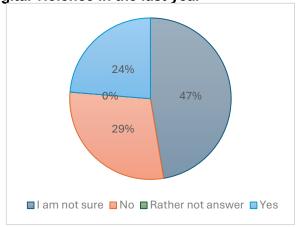




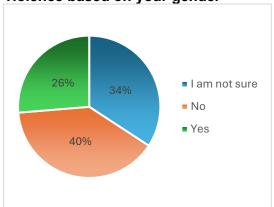


Cambodia

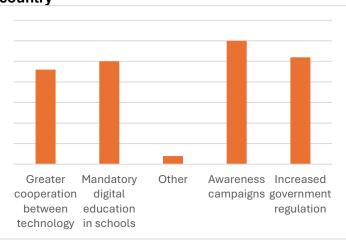
% of respondents who have experienced any type of digital violence in the last year



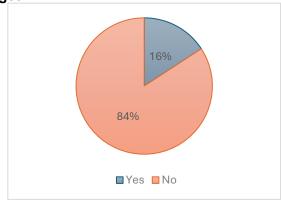
% of respondents have experienced any form of digital violence based on your gender



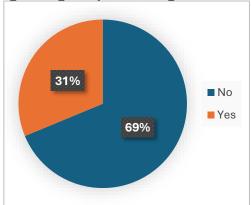
Actions that could be taken to improve online safety and security in your community or in your country

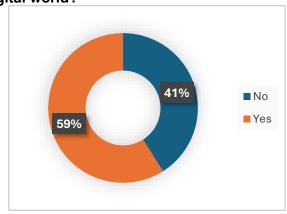


As a result of your work or lending your voice to certain campaigns, have you ever been the target?



% of respondents who think their government is doing enough to prevent digital violence





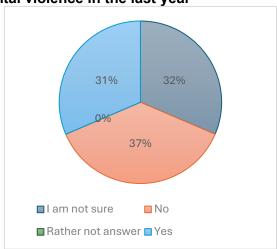




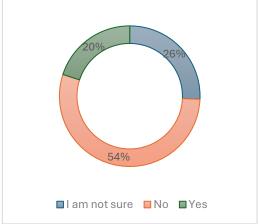


Vietnam

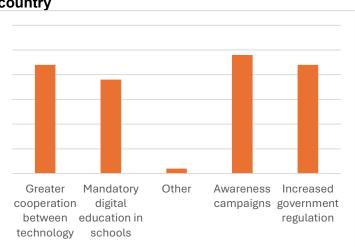
% of respondents who have experienced any type of digital violence in the last year



% of respondents have experienced any form of digital violence based on your gender

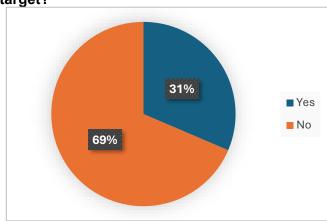


Actions that could be taken to improve online safety and security in your community or in your country



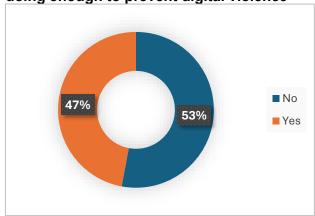
As a result of your work or lending your voice to certain campaigns, have you ever been the

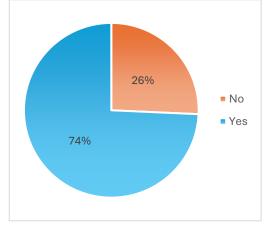




% of respondents who think their government is







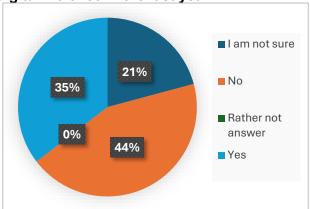




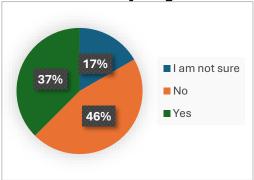


Somalia

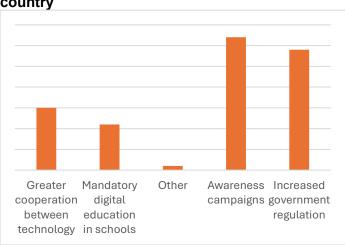
% of respondents who have experienced any type of digital violence in the last year



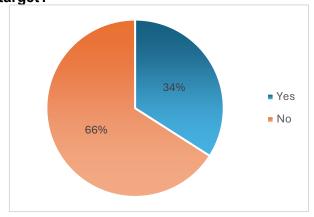
% of respondents have experienced any form of digital violence based on your gender



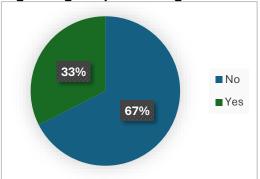
Actions that could be taken to improve online safety and security in your community or in your country

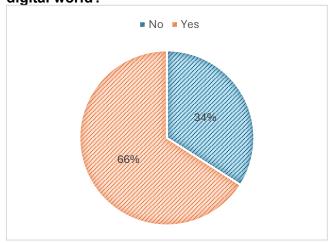


As a result of your work or lending your voice to certain campaigns, have you ever been the target?



% of respondents who think their government is doing enough to prevent digital violence











"This publication was co-funded by the European Union. Its contents are the sole responsibility of authors and implementing partners and do not necessarily reflect the views of the European Union"



Dublin Office

Oxfam Ireland, Portview House, Thorncastle Street, Ringsend, Dublin 4 D04V9Y9

Find us on map

- 2 Call +353 (0) 1 672 7662 (ROI)
- Email IRL-info@oxfam.org

Belfast Office

Oxfam Ireland, 42 The Cuts The Cutts, Dunmurry, BELFAST BT17 9HN, Northern Ireland

Find us on map

- 2 Call +44 (0) 28 9023 0220 (NI)
- Email IRL-info@oxfam.org