RECIPE
Recentering The Civic Internet Through Partner Engagement

OXFAM Ireland

Co-funded by the European Union

SUMMARY ASSESSMENT REPORT:

THE DIGITAL LANDSCAPE, THREATS, AND OPPORTUNITIES.

This is a summary of an extensive report on research conducted as part of the ReCIPE (Recentering the Civic Internet through Partner Engagement) project, led by Oxfam Ireland, to find out more about the current digital context, the issues people are facing and how these might be addressed from the perspective of civil society organisations (CSOs), activists and community members in the Global South.

MAIN DATA ON DEMOGRAPHICS:

1030
RESPONDENTS

9
COUNTRIES
BOLIVIA CAMBODIA EL SALVADOR KENYA OCCUPIED PALESTINIAN TERRITORY SOMALIA TUNISIA UGANDA VIETNAM

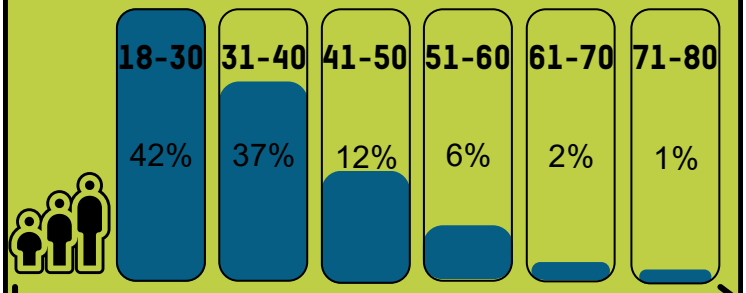
87
QUESTIONS
Not all questions were addressed to all respondents; depending on their profile, they answered the components of the survey relevant to them.

94%
HAVE REGULAR ACCESS TO THE INTERNET.

BY GENDER:

48.2%	45.8%	5.4%	0.6%
Women	Men	Preferred not to answer	Non-Binary

BY AGE:



WOMEN'S MAIN OCCUPATIONS:

- Business
- Social and health
- Housewife
- Teaching
- Other areas of work

MEN'S MAIN OCCUPATIONS:

- Business
- Social and health
- Agriculture/ livestock
- Transport
- Other areas of work

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

76% do not have professional experience related to digital rights

77% of those working or involved in the digital rights sector are members of an NGO.

12% are members of a feminist collective.

RESULTS AND KEY FINDINGS

Internet access

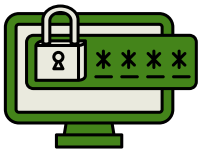
94% of respondents have regular access to the internet. But even when the internet is accessible, those on lower incomes or who live in rural or remote areas face challenges. **The cost of connecting to the internet** is considered expensive or very expensive by more than **60%** of respondents. **68%** of respondents consider the **quality of connectivity** in their country to be fair or poor.

The amount of people without internet access increases with age:

- **28% of those aged 51 and up** do not have access to the internet.
- **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 based on gender.

Digital security



- Around **50%** of respondents claim to have experienced various types of digital security problems such as information theft, website attacks, phishing or financial crime.
- Only **28%** of respondents have sought support or help from CSOs while facing digital security problems.
- **29%** reported these problems to an official authority.
- **62%** of respondents do something to protect themselves, and **38%** of people currently do not take any measures to protect themselves from external attacks.

Knowledge and experiences of digital violence and safety

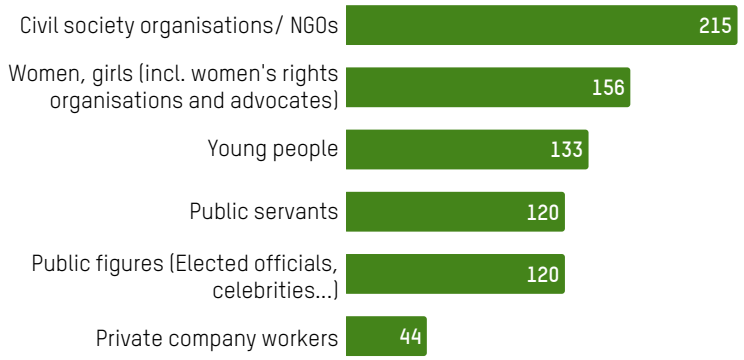
35% of respondents were victims of digital violence in the last year. This is a relevant number given the percentage of people with internet access. **44% of people also report having experienced digital violence as a result of lending their voice to certain campaigns on social media**. Depending on the country, this figure increases significantly.

When it comes to digital violence, survey responses suggest that awareness of the concept is still limited. A number of respondents say they are not sure if they have been victims of digital violence; in response to the question 'What do you understand by digital violence?', **20%** of respondents are not sure and **19%** prefer not to answer.

The most common forms of digital violence experienced by respondents:

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%**

Victims of digital violence:



From the interviews, the most common victims of digital violence are women and girls, members of CSOs/NGOs, and young people, as shown in the above table. These findings are consistent with the other figures mentioned relating to digital violence.

50% of those surveyed report having experienced digital security issues (e.g. account theft, social networking, etc.), rising to 64% of those aged over 40.

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. Around 50% of women say they have experienced **gender-based digital violence**; around 15% are not sure. 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.
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 more likely to be victims of digital violence in general and gender-based violence in particular. In addition, as people get older, the risks associated with using the internet may increase.

Current measures to prevent digital violence

of respondents believe that governments are not doing enough to prevent and combat digital violence and protect people. In some countries, this is much higher.

RECIPE Recentering The Civic Internet Through Partner Engagement
OXFAM Ireland
Co-funded by the European Union

RESULTS AND KEY FINDINGS

48%

of respondents believe that the current implementation of policies and regulations in their country is not effective.

35%

are not sure.

Respondents believe that governments are not doing enough to prevent and combat digital violence and protect people, and the main reasons are:

- Lack of specific policies or inadequate legislation.
- Lack of enforcement of existing laws.
- Governments and institutions' limited resources or capacity.
- Impunity and need for more sanctions.
- Lack of awareness leads to under-reporting.
- Lack of cooperation and coordination.
- Digital violence used against citizens by some governments.

Capacities and resources of CSOs

Responses to the survey indicated that there is a need for CSOs to deepen their knowledge of data protection and digital rights issues, protection and prevention of gender-based digital violence and external threats.

Around 28% of respondents report having received training on digital rights and/or digital security.

Some suggested areas for improvement in training are:

- Improving the contextual factors of such training to make them more relevant.
- Allocating sufficient time for practice, with a clear learning plan and objectives, not just a technical focus.
- Broadening the knowledge to include protection and human rights and targeting minority groups.
- Staying updated on emerging trends: AI, Chat GPT...

Proposals to prevent threats to digital rights

By civil society actors:

- Identify the most vulnerable population.
- Bring together organisations in a network to share information on digital rights and violence and to strengthen organisations.
- Focus on prevention though awareness strategies for citizens.
- Develop advocacy strategies and identify existing public policies.

By activists:

- Advocate for laws that criminalise all forms of digital violence and influence digital rights policy.
- 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.
- Educate the community and run workshops to build citizens' capacity on the issue.

By social and/or educational actors:

- Set up victim support programmes and focus on psychological support.
- Systematise support, complaints procedures, reporting channels and communication formats.
- Enhance and disseminate digital educational content.
- Make digital literacy compulsory in schools.

By the media and social networks:

- Identify the most vulnerable populations and carry out social media campaigns to identify, detect and report digital violence.
- Make information on social media more accessible, reliable and factual.
- Share general data on digital threats and violence to generate a public and media agenda.

By governments or local authorities:

- Carry out a diagnosis of the state of the country in terms of digital violence.
- Develop digital violence legal frameworks and specific protocols.
- Increase sanctions and penal reform, and increase resources for protection and justice.
- Strengthen data protection legislation.

By technology companies:

- Improve internet governance policies.
- Take responsibility for investing in prevention and support and train staff, including outsourced staff.
- Establish agile response mechanisms for cases of digital violence.
- Tackle the digital and security divide and educate technology users on how to protect themselves.

By all actors to be people-centred:

- Prevent revictimisation and address the root causes of digital violence.

RESULTS AND KEY FINDINGS

Specific proposals to protect vulnerable people against threats of digital violence, particularly for women, girls, non-binary people or other minorities

- Facilitate access to information, prevention and support for vulnerable populations, paying particular attention to rural areas, indigenous peoples, women and non-binary groups, who very often feel neglected and underrepresented.
- Ensure that online content does not reproduce violence, misogyny, machismo or other forms of discrimination.
- Develop specific legislation on digital violence with an intersectional feminist and human rights approach, and establish clear criteria for content policing.
- Strengthen the justice system by working with prosecutors, judges and police.
- CSOs and feminist collectives should have a better understanding of what digital violence is and should organise themselves collectively to respond to it.
- Work on gender bias in companies.

RECCOMMENDATIONS SUMMARY

This section provides a summary of the main suggestions made by respondents; 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 the project.

Awareness-raising and training with information about digital risks and how to deal with them.

Create a network of digital rights defenders with a collaborative and cross-sectoral approach.

Put the issue of digital rights and safety on the international agenda.

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.

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.

Improve coordination between government ministries, the media and civil society.

Identify the most vulnerable groups and develop specific instruments to protect them.

Strengthen support and assistance mechanisms for victims of digital violence, abuse or any kind of threat on social networks.

Support CSOs and/or activists with more information and resources.

Enhance the ability to anticipate risks associated with emerging technologies.

Bridge the digital divide:

1. Advocate for policies that promote affordable and accessible internet access;
2. Improve infrastructure to expand access;

For more information, visit:

WWW.OXFAMRECIPE.EU

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

RECIPE
Recentering The Civic Internet Through Partner Engagement

OXFAM Ireland

Co-funded by the European Union