Ministry of Gender Equality and Family

UN WOMEN

online violence against women in Asia

A MULTICOUNTRY STUDY

ONLINE VIOLENCE AGAINST WOMEN IN ASIA: A MULTICOUNTRY STUDY

UN WOMEN
November 2020

Research by: Zarizana Abdul Aziz
Editing by: Gihan Hassanein
Copy editing by: Gretchen Luschsinger

TABLE OF CONTENTS

ACKNOWLEDGEMENTS

The authors would like to thank in particular Melissa Alvarado, Marie Palitzyne, Younghwa Choi and Lou Eve, UN Women Regional Office for Asia and the Pacific; Anju Pandey and Ishita Kaul, UN Women, India; and Charise Jordan and Jessa Colobong, UN Women, Philippines.

We also acknowledge Noraida Endut, Centre for Research on Women and Gender, Universiti Sains Malaysia; Jelen Paclarin, Women's Legal and Human Rights Bureau, the Philippines Commission on Human Rights; Nighat Dad and Shmyla Khan, Digital Rights Foundation, Pakistan; and Serene Lim, KRYSS Network, Malaysia.

We appreciate the inputs of Lyndsay McLean, Senior Associate, The Prevention Collaborative; Dina Deligiorgis, UN Women Headquarters; and Mary Ellsberg, Global Women's Institute, George Washington University.

We thank the Government of the Republic of Korea for its generous support, and all those who agreed to participate in this research, including respondents to the questionnaire; participants from civil society, academia and national human rights institutes in focus group discussions and key informant interviews in India, Malaysia, Pakistan, the Philippines and the Republic of Korea; and government officials and representatives from Internet intermediaries who agreed to be interviewed in person and online.

KEY TERMINOLOGY

ICT means "information and communication technology" and includes all forms of media, platforms and applications accessed by digital means, such as the Internet and digital telecommunications.

ICT VAWG refers to acts of violence against women and girls (VAWG) committed in part or fully through ICT. These acts include, among others, cyberstalking; bullying; online harassment; multiple platform harassment; dog-piling (the vicious mob attack of a person over comments); accessing, uploading or disseminating intimate photos, videos, or audio clips without consent; accessing or disseminating private data without consent; doxing (searching and publicizing someone's personal data) and sextortion. ICT VAWG is popularly referred to as "online VAWG".

ICT intermediaries bring together or facilitate transactions among third parties on the Internet and digital media. They provide access to, host, transmit and index content, products and services originating from third parties on a digital medium, and provide ICT-based services to third parties.

Secondary perpetrators refer to individuals who actively participate in ICT-related VAWG by downloading, forwarding and sharing VAWG content by third parties (principal perpetrators), recklessly disregarding or ignorant of the fact that the content is violent or was disseminated without the consent of the subject.

PHOTO: UN Women/Shaista Chishty

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

Freedom of expression and access to information are fundamental to a range of human rights. In today's digital age, the Internet is enabling new online social spaces and transforming how individuals communicate and interact. It is reshaping society. Yet the potential of the Internet and digital technology is undermined by high levels of information communication technology (ICT)-related violence against women and girls (VAWG).

Eliminating ICT VAWG is critical to empower women and ensure their equal access to ICT. Removing violence against women from digital and online platforms also has the net effect of promoting and strengthening freedom of information because it creates an environment that allows more individuals, especially those who face discrimination in other public spaces, to participate and make their voice heard.

This study on ICT VAWG was conducted from July to December 2019 in five Asian countries: India, Malaysia, Pakistan, the Philippines and the Republic of Korea. In each country, the research looked at the manifestations of ICT VAWG, the measures (legislation, policies and programmes) taken by States and ICT intermediaries to both prevent and respond to it, and perceptions of civil society organizations (CSOs).

Although this report is based on research conducted prior to the COVID-19 pandemic, it assumes greater relevance given how critical ICT has become in rethinking ways of communicating, working, conducting business, managing family life, and accessing services, facilities and justice. On the positive side, social distancing, movement restrictions and lockdowns imposed across the globe have led to opportunities for flexible work hours and work from home, and increased time with children, all of which have been part of women's demands for decades.

Not surprisingly, however, users with limited digital skills, predominantly women and girls, are more at risk of ICT VAWG. Schoolchildren who spend more time online may also be at risk, including from online sexual exploitation.

This report is not a comprehensive analysis of all data gathered from the research that was conducted. It focuses on the most pertinent information to answer the following questions:

- How does ICT VAWG manifest?
- What measures (legislation, policies and programmes) do States take to both prevent and respond to ICT VAWG?
- How do CSOs on the frontlines of combatting VAWG and ICT VAWG perceive state actions in the prevention, protection, prosecution, punishment and provision of redress for ICT VAWG?
- How do ICT intermediaries prevent and respond to ICT VAWG?

The objectives of the research are to:

- Study state efforts to date in dealing with ICT VAWG;
- Investigate civil society perspectives on state efforts, achievements and challenges in preventing violence against women, protecting survivors, prosecuting cases, punishing perpetrators and providing redress for survivors;
- Identify promising practices and make recommendations to eliminate ICT VAWG;
- Consider ICT intermediaries' efforts to date in addressing ICT VAWG; and
- Develop a knowledge and advocacy product that provides different stakeholders with an overview of ICT VAWG in Asia along with recommendations to address it

This report is based on a mixed methods approach, using both the review of secondary materials and primary data collection. The first part consists of desk research based on secondary data and reports on state practices. The second part involves a standardized questionnaire administered to CSOs to probe their perceptions of state actions to prevent and respond to ICT VAWG. The third part comprises focus group discussions with both civil society experts and government officials (where possible), and key informant interviews. The objective of these discussions and interviews was to obtain insights on systemic national patterns or issues as well as perceptions and opinions of in-country experts on state and Internet intermediary actions in preventing and responding to ICT VAWG.

The main findings are grouped under the following subheadings:

- ICT VAWG risk factors
- Manifestations of ICT VAWG
- Where ICT VAWG happens
- State obligations to respond
- ICT intermediary measures to prevent and respond

FINDING: ICT VAWG is common in all five countries.

The findings indicate that ICT VAWG is common in all five countries. Sexist and misogynist comments or gender hate speech were rated the most common form of ICT VAWG. Manifestations include *digital voyeurism* (the illicit filming, watching and sharing online of films of women's bodies, through live or recorded streaming of the footage), *morphing* of women's images into a composite image called *ahegao, online harassment* of women over dress and behaviour deemed "inappropriate" by those intent on moral policing of women's bodies and actions, the *dissemination of rape footage* in video clips uploaded or traded, and *live-streaming of child sexual abuse*.

Women with intersecting identities are regularly targeted online. Those in public and political life (human rights defenders, journalists and political figures) face ICT VAWG used to silence them and "put them in their place".

FINDING: CSOs and advocates agreed on several important factors that increase the risk of ICT VAWG, including gender inequality, misogyny and negative cultural perceptions of women.

When asked to rate their perception of nine factors that increase the risk of ICT VAWG, CSOs surveyed in the five countries considered several very or extremely important. These encompassed gender inequality, negative perceptions of women, misogyny, impunity, anonymity, ease of

transmission, dissemination of false information, disinhibition of perpetrators, lack of media literacy and online behavior and etiquette. Exceptions were India where media literacy was less of an issue, along with the Philippines in terms of media literacy and the disinhibition of perpetrators, and Pakistan in terms of the disinhibition of perpetrators, impunity and ease of transmission. CSO advocates maintained that online behaviour and etiquette must be addressed in order to stop ICT VAWG.

FINDING: When prevention programmes exist, for example, in schools, they tend to focus on cyberbullying and safe Internet use.

Civil society advocates indicated that state programmes tend to focus on Internet safety and cyberbullying. Awareness programmes for the general public often emphasize the dissemination of disinformation and misinformation, and do not typically include ICT VAWG. Advocates also considered a top-down approach to prevention as ill-suited, particularly for youth, who need interesting programmes they can relate to. They stressed that existing state programmes have not been particularly successful with this approach.

FINDING: Scarcity of programmes on Internet etiquette and culture.

The Internet has the effect of disinhibiting users. Many tend to disclose more, lulled by the fact that they are communicating via a screen rather than with a live audience. The reduction of non-verbal cues in computer-mediated and digital communication has challenged social mores learned from face-to-face interaction.

State prevention programmes tend to inform girls about online safety. Few programmes discuss Internet etiquette and culture, toxic online behaviour and the prohibition of ICT VAWG.

FINDING: CSOs and advocates indicate that victims/survivors rarely or never report ICT VAWG to the authorities.

CSO respondents suggested that victims/survivors prefer to confide in friends, work colleagues and civil society organizations instead of reporting ICT VAWG to the authorities. If a report is lodged, it is more likely to be with the relevant ICT intermediaries than with state authorities. According to CSOs, seeking the intervention of authorities or even ICT intermediaries is often the last resort. Fear of reprisals from perpetrators, lack of confidence in the police, the high cost of civil legal action and a lack of confidence in the judicial process are significant barriers to complaining to authorities. CSOs indicated that ICT VAWG is a low priority for the police and prosecutors, and there is an unhealthy level of victim blaming.

FINDING: State measures mainly focus on legislation that criminalizes ICT VAWG, carrying sentences of imprisonment and fines, sometimes with specialized law enforcement personnel, prosecutors and courts.

All five countries have undertaken legal reforms in response to ICT VAWG. Legislation criminalizing ICT VAWG is sometimes accompanied by specialized law enforcement personnel, prosecutors and courts.

The specificities of ICT VAWG, such as its easy and rapid dissemination across multiple platforms and networks, and the participation of bystanders (who may wittingly or unwittingly join in perpetrating it, such as by retransmitting content), are precisely what make the harm egregious. Experience dictates that specific legal provisions are required to address gender-based offences, including specialized courts. Similarly, specific legal provisions are required to address and respond to ICT VAWG. Although States have established courts and trained investigators and prosecutors for ICT-related offences, none are specialized in ICT VAWG.

ICT VAWG requires a fresh lens to view issues such as secondary perpetration, namely by bystanders actively perpetuating violence by downloading, forwarding and sharing content by third parties (principal perpetrators), while recklessly disregarding or ignorant of the fact that the content is violent or was disseminated without the consent of the subject.

FINDING: CSO respondents favoured expanding possible sanctions to include ordering perpetrators to have content removed and delinked from searches as well as fines and restitution (where possible).

The most effective way of punishing ICT VAWG has not been determined. Incarceration is considered a possible sanction for some forms. All civil society advocates agreed that ordering perpetrators to take down harmful content (or where the content has been disseminated by bystanders or secondary perpetrators, cause it to be taken down) should be part of the punishment regime. Other sanctions include apology, restitution, compensation and ways to assist victims/survivors to rebuild their lives and online presence. Such punishments should aim also to prevent recidivism, deter others and rehabilitate the perpetrator. Sanctions implemented by ICT intermediaries must reflect the harm and gravity of ICT VAWG, and can include apology, suspension and banning from the platform.

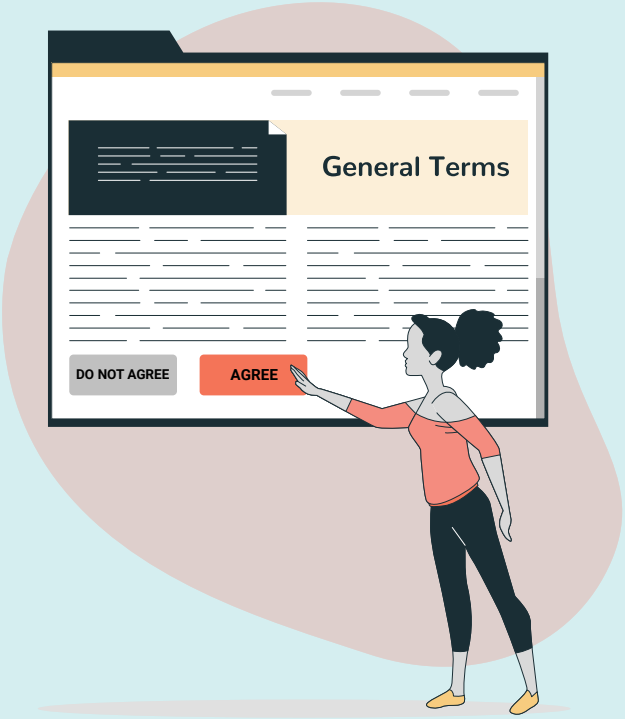
FINDING: States and ICT intermediaries need clarity in defining ICT VAWG

There is a need for clarity and consensus among States, ICT intermediaries and civil society on what constitutes online violence against women. States tend to view violence as a criminal offence, placing greater priority on grievous physical and sexual harm, and trivializing non-grievous harm, including violence occurring in online spaces. Industry representatives noted that identifying ICT VAWG was sometimes challenging

and requested clearer definitions. Complicating this is the fact that what constitutes ICT VAWG is often coloured by a given culture and society. Further, ICT VAWG (e.g., nonconsensual sharing of intimate images) should not be framed under obscenity laws because the focus of the violence reported is the lack of consent to its dissemination.

FINDING: Lengthy online community rules are frequently not read by users

Lengthy online community rules are not effective because they are frequently not read by users. Despite being sufficiently tech savvy to use platforms and applications, users may not be conversant in the convoluted legal jargon of community rules. Since users just want to start using applications and platforms, they click on "agree" without reading the rules. For ICT intermediaries to continue relying on these terms is ineffective, even though it is legally sound.



WHAT DO **THE FINDINGS** MEAN?

The study shows that much of the violence women experience offline is replicated online. So are the risk factors. It is critical to conceptualize the issues that inform and underpin violence against women, such as male entitlement to power, women's bodies, decision-making, etc. While safety measures are important, there is a critical need to address misogyny and gender equality, which drive violence against women, as well as hate and the toxic use of digital media. Preventing ICT VAWG requires reaching out not only to girls but to all digital media users, including boys and men, to address online behaviour and Internet culture.

The acceptance or rejection of ICT VAWG is shaped by the actions of States and ICT intermediaries. They are both in a position to create an online culture free from ICT VAWG. They can remove – or at least reduce – toxic behaviour on the Internet, and take appropriate and transparent measures to sanction perpetrators of ICT VAWG. It is critical to restore confidence in the legal process so that women and girls may access justice. Women withdrawing from digital spaces due to ICT VAWG is not a solution and should not be tolerated.

PHOTO: UN Women/Ali Najam and Asif Ali

I. INTRODUCTION

I. INTRODUCTION

Information and communication technology (ICT) and the Internet have radically transformed how people interact. In many instances, these technologies have become the main form of communication in commercial dealings as well as in personal, political and social interaction. "This development is especially critical for new generations of girls and boys, who are starting their lives extensively using new technologies to mediate their relationships, affecting all aspects of their lives."[1]

Freedom of expression and access to information are fundamental rights that enable a range of other human rights. The transformative potential of the Internet and digital technology is under threat, however, due to high levels of ICT-related violence against women and girls (VAWG). Although this report is based on research conducted prior to the COVID-19 pandemic, it assumes even greater relevance given how critical access to ICT has become during the pandemic. Social distancing, movement restrictions and lockdowns imposed by States across the globe have led to a sharp rise in the use of ICT as the primary means of maintaining social relationships, receiving information, working, getting an education and conducting business.

Not surprisingly, users with limited digital skills, predominantly women and girls, are more at risk of ICT VAWG.[2] Schoolchildren who spend more time online may also be at risk, including through online sexual exploitation. Apart from a few media reports, law enforcement statistics and anecdotal evidence, rigorous studies have yet to estimate the increased incidence of ICT VAWG during the pandemic, including zoom-bombing (a form of video hijacking where hackers infiltrate video meetings, often shouting racial or misogynistic slurs, making threats or cyberflashing).[3]

Although States have adopted various strategies to end it, ICT VAWG continues to be a universal phenomenon. Some laws, policies, processes and procedures for offline VAWG may be equally applicable to ICT VAWG, given a continuum of violence offline and online. ICT VAWG is highly specific in many ways, however, and requires measures adapted to it. These must tackle, among others, the ease and speed of transmission, and in some instances, a "fertile landscape in which predators can roam".[4]

1 Dubravka Šimonović, 2018, Report of the Special Rapporteur on violence against women, its causes and consequences on online violence against women and girls from a human rights perspective, A/HRC/38/47, United Nations.

2 See UN Women, 2020, "Online and ICT Facilitated Violence against Women and Girls during COVID-19," https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2020/brief-online-and-ict-facilitated-violence-against-women-and-girls-during-covid-19-en.pdf?la=en&vs=2519.

3 Zoom bombing is the disruption of a zoom meeting by the sudden appearance of uninvited participants who view, shout slurs at or cyberflash participants. Kari Paul, 2020, "Zoom is malware: why experts worry about the video conferencing platform," The Guardian, 2 April, https://www.theguardian.com/technology/2020/apr/02/zoom-technology-security-coronavirus-video-conferencing. See also Lizle Loots, Elizabeth Dartnell and Jocelyn Kelly, 2020, Online safety in a changing world – COVID-19 and cyber violence, SEXUAL VIOLENCE RESEARCH INITIATIVE, 16 APRIL, https://svri.org/blog/online-safety-changing-world-%E2%80%93-covid-19-and-cyber-violence. Offline VAWG during pandemics and other crises is better understood. See United Nations, 2020, "Policy Brief: The Impact of COVID-19 on Women," 9 April, https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2020/policy-brief-the-impact-of-covid-19-on-women-en.pdf?la=en&vs=1406. See also Amber Peterson and others, 2020, "Pandemics and violence against women and children," CENTRE FOR GLOBAL DEVELOPMENT, April, https://cisp.cachefly.net/assets/articles/attachments/82017_pandemics-and-vawg.pdf.

4 Katherine Gregory, 2020, "A predator kept targeting victims on Tinder for years. Why wasn't he stopped sooner?" ABC NEWS, 6 February, https://www.abc.net.au/news/2020-02-07/dating-app-sexual-assault-predator-was-using-dating-profiles/11931586.

The increased prevalence of ICT VAWG, the lack of effective measures to prevent and contain it, and ensuing impunity must all be addressed as part of the struggle to eliminate all forms of gender-based violence.

In this, it is crucial to not only investigate the obligation of States to eliminate ICT VAWG, but also to look at the roles and responsibilities of ICT intermediaries. While the Internet is regarded as a public forum, this space cannot usually be accessed directly by the public. It is mostly reached via private actors serving as intermediaries, typically, transnational corporations. ICT intermediaries provide hosting facilities and telecommunications services. They control online platforms and networks, including social media platforms such as Facebook and Twitter, and video-sharing apps such as Tik Tok. ICT intermediaries have a responsibility to balance their business imperative to encourage traffic on and to their platforms while protecting freedom of speech, and removing violent, inappropriate and harmful content. This often creates tensions.

This report refers both to "ICT VAWG" and the more user-friendly expression "online VAWG". Both terms are used by Dubravka Šimonovic, the United Nations Special Rapporteur on Violence Against Women, its Causes and its Consequences in her report about this topic.[5]

The report presents new knowledge on ICT VAWG in five countries in Asia: India, Malaysia, Pakistan, the Philippines and the Republic of Korea. While it is not a comprehensive analysis of all data gathered from research, it focuses on the most pertinent information in an attempt to answer the following questions:

- How does ICT VAWG manifest?
- What measures (legislation, policies and programmes) do States take to both prevent and respond to ICT VAWG?
- How do CSOs on the frontlines of combatting VAWG and ICT VAWG perceive state actions in the prevention, protection, prosecution, punishment and provision of redress for ICT VAWG?
- How do ICT intermediaries prevent and respond to ICT VAWG?

The objectives of the research are to:

- Study state efforts to date in dealing with ICT VAWG;
- Investigate civil society perspectives on state efforts, achievements and challenges in preventing violence against women, protecting survivors, prosecuting cases, punishing perpetrators and providing redress for survivors;
- Identify promising practices and make recommendations to eliminate ICT VAWG;
- Consider ICT intermediaries' efforts to date in addressing ICT VAWG; and
- Develop a knowledge and advocacy product that provides different stakeholders with an overview of ICT VAWG in Asia along with recommendations to address it.

The paper outlines the research methodology and the framework for ICT VAWG, and presents findings. It also analyses the issues raised and makes recommendations to address ICT VAWG.[6]

5 The 2030 Agenda for Sustainable Development emphasizes the general and inclusive term "information and communications technology", but other reports use "online violence", "digital violence" or "cyberviolence".

6 Refers to work by the Due Diligence Project since 2014.

PHOTO: UN Women/Joser Dumbrique

II. RESEARCH METHODOLOGY

II. RESEARCH METHODOLOGY

The choice of the five countries selected for this research – India, Malaysia, Pakistan, the Philippines and the Republic of Korea – was based on the following criteria:

- The State has initiated several measures to address ICT VAWG (e.g., related laws, policies and mechanisms);
- Independent and vibrant civil society organizations and individual experts are present;[7]
- Diversity in terms of language and socio-political and economic situations;
- At least one country from each subregion of Asia (East Asia, South-East Asia and South Asia); and
- The viability of collecting primary data.

The research employed a mixed methods approach with a review of secondary materials and primary data collection. It included:

1. DESK RESEARCH

The first part of the research consisted of desk research based on secondary data and reports on state practices, namely laws, policies, programmes and mechanisms to prevent and respond to ICT VAWG. It also covered policies and measures put in place by ICT intermediaries to prevent, address and remedy ICT VAWG.

2. Questionnaire for civil society organizations

The second part of the research involved a questionnaire administered to CSOs to probe their perceptions of state actions in preventing and responding to ICT VAWG, given their unique knowledge as practitioners and advocates.

Developed in collaboration with academics and civil society, and based on prior roundtable discussions and expert group meetings,[8] the questionnaire was completed electronically by 39 CSOs – 10 in India, 9 in Malaysia, 6 in Pakistan, 9 in the Philippines and 4 in the Republic of Korea.[9] Their responses should be considered an indication of trends at the time

7 "[S]trong autonomous feminist movements is both substantively and statistically significant as a predictor of government action to redress violence against women." Mala Htun and S. Laurel Weldon, 2012, "The civil origins of progressive social change: Combatting violence against women in global perspective, 1975-2005," American Political Science Review 548.

8 Two expert group meetings were convened by the Due Diligence Project, in 2015 in Florence, Italy and in 2019 in Washington, DC. Participants included former United Nations mandate holders on freedom of expression and on violence against women, government officials, academics, and experts/advocates on ICT and/or violence against women.

9 The questionnaire was 20 pages long and asked CSOs about their perceptions of manifestations of ICT VAWG, prevention strategies and responses including sanctions and remedies. The questionnaire administered in the Republic of Korea was translated into Korean.

they were provided rather than as proof positive evidence.

CSOs were approached because they are often the first level of support for victims/survivors. They frequently facilitate or mediate access to state facilities and remedies. For their responses, CSOs drew from their institutional memory and wealth of experience in working with victims/survivors; undertaking outreach and educational programmes, either in partnership with the State or otherwise; and engaging with Internet intermediaries.

CSOs were selected after a consultative process with regional and national experts. Those invited to participate in the research are well known in their countries, with a history of credible activities at the national, regional and international levels, and gender equality/rights-based approaches. They all undertake VAWG-related activities or have missions or objectives that include ending hate and violence in the digital space as well as promoting Internet freedom of expression and equal access to ICT for all.

Social movements have long been catalysts for change. Scholars point out that VAWG has rarely been raised as an issue without pressure from social movements, and in particular organizations focused on women.[10] Furthermore, their responses often predate government action.[11] Engaging with civil society organizations and advocates, both important pillars of social movements, helps research identify issues and shape optimal responses to eliminate ICT VAWG.

3. Focus group discussions and key informant interviews

The third part of the research consisted of focus group discussions with both civil society experts and government officials (where possible) or key informant interviews. The latter were set up with government officials (who usually prefer individual interviews) or when experts were unable to attend group discussions. The objective of both formats was to obtain insights on systemic national patterns or issues as well as perceptions and opinions of in-country experts on States' and Internet intermediaries' actions in preventing and responding to ICT VAWG.

(i) Focus group discussions were held with 10 organizations in India, 6 in Malaysia, 9 in the Philippines, 6 in Pakistan and 2 in the Republic of Korea.[12] A focus group discussion was also conducted with government officials and the National Human Rights Institute in the Philippines.

(ii) Key informant interviews with officials from relevant government agencies and mechanisms included representatives from law enforcement agencies (police, departments of justice and prosecutors), relevant line ministries (in charge of women/gender equality, local government, interior/home affairs, education, labour and children), human rights commissions, and relevant agencies in charge of ICT and cybersecurity.

(iii) Key informant interviews with ICT intermediaries sought a deeper understanding of policies they have adopted.

4. Triangulation

The triangulation of findings gathered through multiple forms of enquiry provided more depth and certainty to conclusions drawn from the data.[13] It also provided opportunities to collect additional information and explore complex issues that are not easy to quantify.

Findings were analysed to identify measures by States and ICT intermediaries that can be considered good or promising practices.

10 Htun and Weldon, "The civil origins of progressive social change."

11 Ibid.

12 In Malaysia, Pakistan, and the Republic of Korea, a majority of CSO respondents were from established women's organizations working on VAWG/ICT VAWG.

13 The focus groups discussions and interviews were taped, where possible. Otherwise, notes of interviews were taken. The themes were then identified, organized and analysed.

PHOTO: UN Women/David Pellman

III. UNDERSTANDING ICT VAWG

III. UNDERSTANDING **ICT VAWG**

UNDERSTANDING **VAWG**

VAWG is one of the most serious, life-threatening and widespread violations of human rights worldwide. It occurs at home, in workplaces, in public spaces and online, and can culminate in femicide, or the deliberate murder of women and girls. It devastates lives, and fractures families and communities.

The 1993 United Nations Declaration on the Elimination of Violence against Women defines it as an act of gender-based violence (GBV) that results in, or is likely to result in, physical, sexual, psychological or economic harm or suffering to women, including threats of such acts, and coercion or arbitrary deprivation of liberty, whether occurring in public or private life.[14]

VAWG is a form of discrimination against women and girls and a violation of their human rights, including their right to live free from violence. The prohibition of VAWG has been affirmed in international and regional human rights instruments, and is accepted as a principle of international law applicable across all nations.[15]

PHOTO: UN Women/Henriette Bjoerge

The underlying causes of VAWG are complex. Research points to gender inequality and power imbalances between men and women, reinforced by discriminatory and gender-biased attitudes, norms and practice. Key risk factors include inequitable cultural and social norms that support male authority over women, condone or trivialize VAWG, and stigmatize victims/survivors. Deeply ingrained societal norms and institutions place a lower value on women and girls and contribute to

14 Violence against women has been defined and elaborated in many human rights and feminist instruments and discourses, including CEDAW. The following forms of violence share similarities to online violence against women: intimate partner violence, domestic violence, sexual harassment, harassment based on gender, stalking and inciting others to commit violence against women. ICT VAWG in this report includes ICT-related gender-based violence committed against lesbians, bisexual, transgender and any others persons who do not conform with being gender binary.

15 United Nations Committee on the Elimination of Discrimination against Women, General Recommendation No. 35 on gender-based violence against women, updating General Recommendation No. 19, CEDAW/C/GC/35, 14 July 2017.

high levels of acceptance of VAWG by both men and women. Widespread cultural acceptance of VAWG often operates alongside rampant impunity for perpetrating it.

VAWG impedes human development, women's empowerment and gender equality. It has serious immediate and long-term physical, sexual, psychological and economic consequences that often prevent women and girls from fully participating in society. For instance, VAWG significantly undermines women's educational and employment opportunities, income-earning capability and advancement in the workplace, all of which limit their economic development.

UNDERSTANDING ICT VAWG

The global Sustainable Development Goals include targets for ending discrimination against women and girls, and enhancing the use of technology advancing their empowerment.[16] Yet while ICT VAWG impedes these objectives and violates women's human rights, research on online violence, especially directed at women, is scarce.[17] There are few studies on ICT VAWG countermeasures.

Freedom of expression is not an absolute right. For example, it does not enable someone to harass women, stalk them, or threaten to rape or kill them. Removing VAWG from digital platforms promotes and strengthens freedom of information by creating an environment that allows more individuals, especially those who face discrimination in other public spaces, to participate.[18] Achieving universal access to the Internet requires that women and girls can fully exercise their rights.

An intersectional perspective should be applied to ICT VAWG, as it is for offline VAWG. Diverse groups of women suffer from multiple and intersecting forms of discrimination and inequalities, making them especially vulnerable to violence. Factors of vulnerability include age, ethnicity, poverty, class, sexual orientation, gender identity, disability, religion, indigeneity, nationality, immigration status, and urban and rural locations, among others.

Women with intersecting identities are easily targeted online, which may result in more severe consequences. Some groups, such as women human rights defenders; women in politics; journalists; women with disabilities; lesbian, bisexual or transgender women; and women from marginalized groups are frequent targets of online VAWG,[19] which is used to silence them and "put them in their place".

16 United Nations General Assembly, 2015, Transforming our world: the 2030 Agenda for Sustainable Development, A/RES/70/1.

17 Nicola Henry and Anastasia Powell, 2018, "Technology-Facilitated Sexual Violence: A Literature Review of Empirical Research," Trauma, Violence & Abuse 195 (April).

18 Zarizana Abdul Aziz, 2017, *Due Diligence and Accountability for Online Violence Against Women*, DUE DILIGENCE PROJECT, July, http://duediligenceproject.org/wp-content/uploads/2019/05/Paper-on-Due-Diligence-and-Accountability-for-Online-Violence-against-Women-make-this-active-link.pdf.

19 Šimonović, Report of the Special Rapporteur, note 4, p. 8.

PHOTO: UN Women/Joser Dumbrique

IV. RESEARCH FINDINGS:

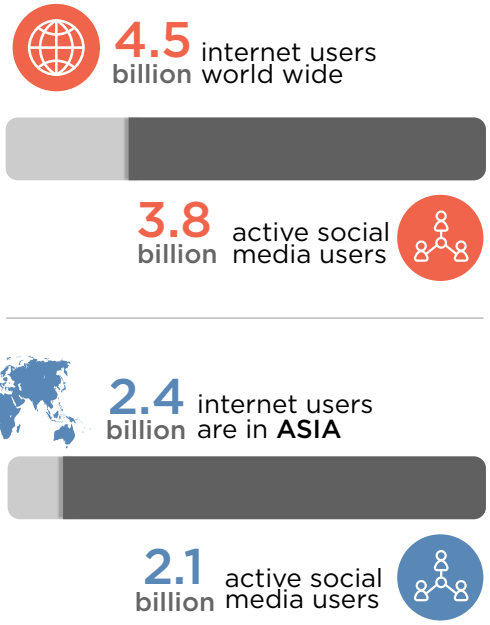
ICT VAWG IN INDIA, MALAYSIA, PAKISTAN, THE PHILIPPINES AND THE REPUBLIC OF KOREA

IV. **RESEARCH FINDINGS:** ICT VAWG IN INDIA, MALAYSIA, PAKISTAN, THE PHILIPPINES AND THE REPUBLIC OF KOREA

(A) BACKGROUND

Access to ICT has grown exponentially. Telecommunications service providers are bringing connectivity to increasingly larger swaths of the population, in urban and rural communities, resulting in an expanded mobile share of web traffic. As of January 2020, an estimated 4.5 billion people were using the Internet globally – over half of the world's population. There are 3.8 billion active social media users.[20]

As of December 2019, 50.1 per cent of web traffic was on mobile phones.[21] Women are 26 per cent less likely than men to have access to mobile phones, however.[22] Globally, women from developing nations make up the majority of the offline population.[23]



20 INTERNET WORLD STATS – USAGE AND POPULATION STATISTICS, https://www.internetworldstats.com/stats3.htm, last visited 26 April 2020.

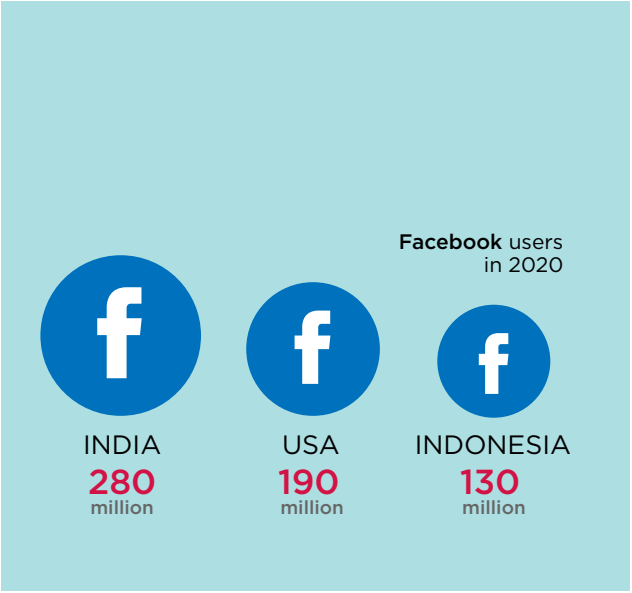
21 Simon Kemp, 2020, "Digital in 2020: 3.8 Billion People Use Social Media," We are Social, 30 January, https://wearesocial.com/blog/2020/01/digital-2020-3-8-billion-people-use-social-media.

22 GSMA ASSOCIATION, 2018, GSMA CONNECTED WOMEN PROGRAMME, A TOOLKIT FOR RESEARCHING WOMEN'S INTERNET ACCESS AND USE, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2018/05/GSMA-Women-and-Internet-Research-Toolkit_WEB.pdf.

23 Carlos Iglesias, 2020, "The gender gap in internet access: using a women-centred method," WORLD WIDE WEB FOUNDATION, 10 March, https://webfoundation.org/2020/03/the-gender-gap-in-internet-access-using-a-women-centred-method/.

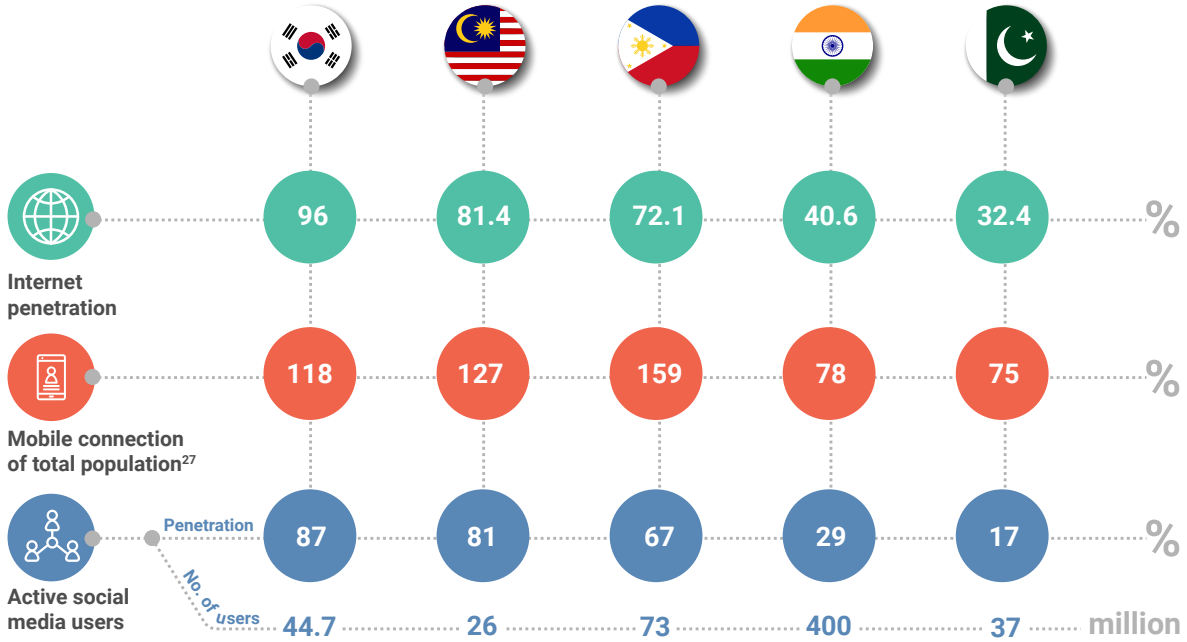
Asia as a region has some of the fastest average mobile Internet speeds. Internet penetration hovers around 56 per cent with almost 2.42 billion users and 2.14 billion active social media users. The region accounts for nearly half of the world's Internet users and over 60 per cent of all social media users.[24]

Asia represents a lucrative market for telecommunications companies and Internet intermediaries. In 2020, the country with the highest number of Facebook users is India with 280 million users. It is followed by the United States with 190 million users and Indonesia with 130 million users.[25] The number of potential Internet users in Asia (not including Western and Central Asia) is 1.87 billion with 1.12 billion in South Asia, 625 million in East Asia and 229 million in South-East Asia.[26]



Internet penetration in the five countries in this study varied greatly, from 35 per cent to 96 per cent. Social media penetration varied too, from 17 per cent to 87 per cent (Table 1).

Table 1: Internet and social media penetration in the five countries



24 Kemp, "Digital in 2020."

25 STATISTA, https://www.statista.com/statistics/268136/top-15-countries-based-on-number-of-facebook-users/, last visited 12 May 2020.

26 Kemp, "Digital in 2020."

27 Where the percentage is more than 100 per cent, it indicates that individuals have multiple forms of mobile connectivity. In fact, it is estimated that there are more mobile devices in the world than people. RADICATI GROUP, 2020, Mobile Statistics Report, 2020-2024, https://www.radicati.com/wp/wp-content/uploads/2020/01/Mobile_Statistics_Report,_2020-2024_Executive_Summary.pdf.

(B) ICT VAWG RISK FACTORS

The 39 CSOs surveyed for this study were asked to rate their perception of nine factors that increase the risk of ICT VAWG:

- Gender inequality
- Negative perception of women
- Misogyny
- Impunity
- Anonymity
- Ease of transmission
- Dissemination of false information
- Disinhibition of the perpetrator
- Lack of media literacy

With a few exceptions, respondents considered all nine factors very or extremely important.[28] They stated that it is critical to address online behaviour and etiquette.[29] Perceived anonymity in online communication can result in individuals becoming more disinhibited. Many online users tend to disclose more, lulled by the fact that they are communicating via a screen rather than with a live audience. The reduction of non-verbal cues in digital communication challenges social mores learned from face-to-face interaction. All of these elements lead many users to act with less restraint, resulting in more frequent and intense ICT VAWG.

In the Republic of Korea, activists perceived misogyny and misogynistic hate speech as critical issues in combatting ICT VAWG. They encouraged the National Human Rights Commission of Korea to undertake a fact-finding study and the legislative assembly to explore legal reform.[30] The Commission recommended that the State legally prohibit gender hate speech and "take various and aggressive national measures, including the reinforcement of equality education and anti-hatred campaigns".[31]

The nine drivers were also shared in focus group discussions and key informant interviews. Participants stressed that understanding the negative or toxic use of the Internet and the causes behind it is important, including in formulating strategies to address it. They pointed to gender inequality, misogyny and negative perceptions of women as some of the underlying causes. Furthermore, women are more at risk where perpetrators enjoy impunity.

State prevention programmes tend to inform girls about online safety rather than address the issues identified above. Few discuss toxic online behaviour, Internet etiquette and culture, and the prohibition of online harassment and cyberbullying.

(C) MANIFESTATIONS OF ICT VAWG

CSOs rated sexist and misogynist comments or gender hate speech as the most common form of ICT VAWG (Figure 1). Online harassment, stalking, discrimination and threats of violence (sexual and non-sexual) were also seen as very common.[32]

Digital voyeurism

Digital voyeurism is the illicit filming, watching and sharing online of films of women's bodies, through live or recorded streaming of the footage. According to CSOs and government representatives, digital voyeurism is common in the Republic of Korea.

Non-consensual filming occurs through hidden cameras in everyday items such as car keys, lighters, hats, buttons and hair dryers. It can also happen when a woman uploads her photograph, no matter how briefly. Her image can then be "stolen" and disseminated without her consent. Women's faces can also be "deep-faked" onto online images.

28 In a few instances, these factors are considered "somewhat important".

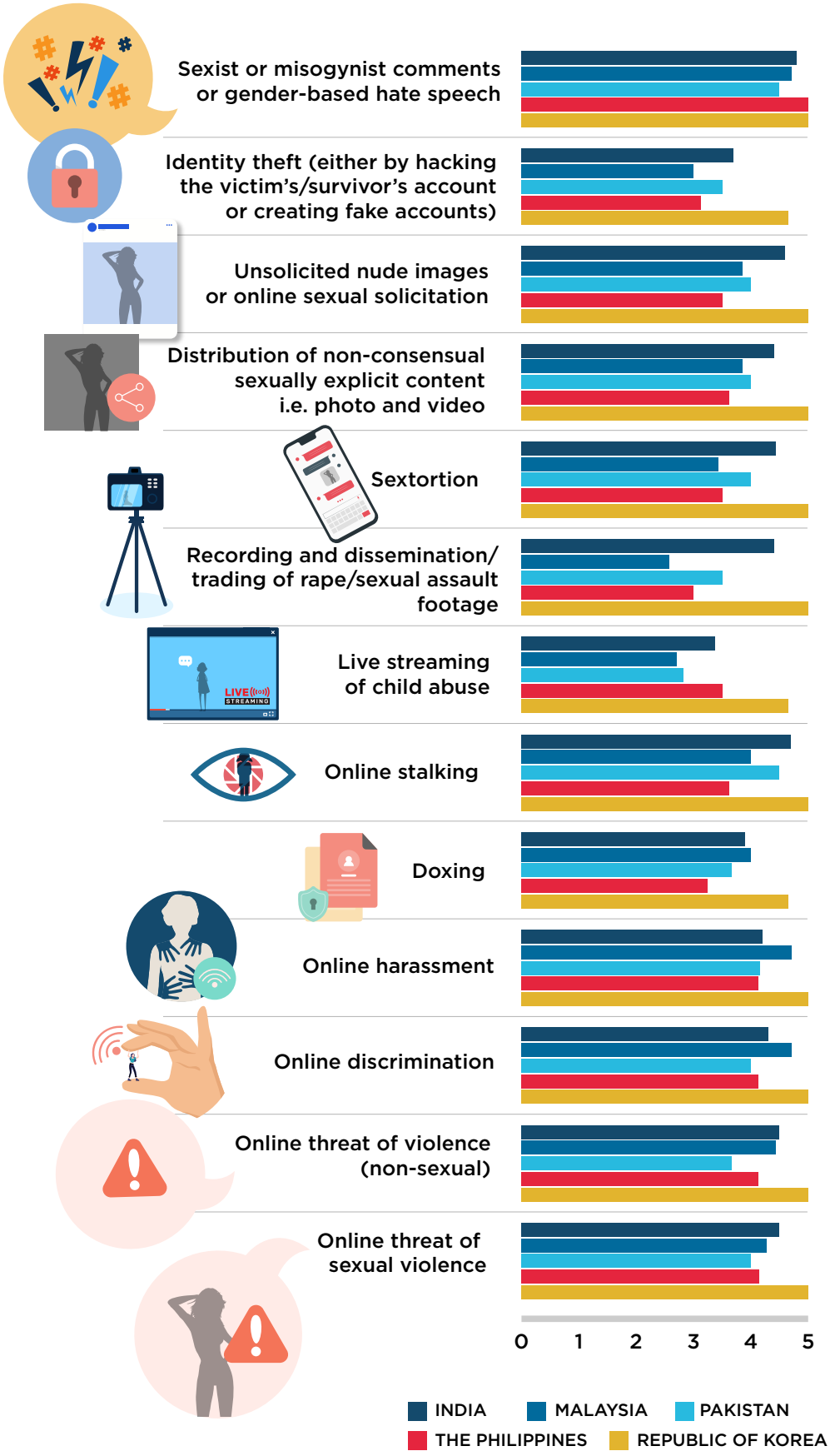
29 Discussions with advocates in India and the Philippines.

30 Report of the National Human Rights Commission of Korea submitted to the UN CEDAW pre-sessional working group on the list of issues in relation to the 8th review of the Republic of Korea, https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/KOR/INT_CEDAW_IFN_KOR_28039_E.pdf, last visited 18 November 2019.

31 Ibid.

32 Each term is explained in more detail below.

Figure 1: CSO perceptions of commonly occurring forms of ICT VAWG



Note: n= 37. 1= never, 2=rarely, 3=occasionally, 4=a great amount and 5=a great deal.

In the Republic of Korea, the problem of digital voyeurism has been corroborated by media coverage. In 2017, over 7,000 women there found compromising videos of themselves on adult websites, a sevenfold increase in four years. Many have been unknowingly filmed in changing rooms and restrooms by a growing army of voyeurs or by their former intimate partners.[33]

In March 2019, the police arrested two men for setting up mini-cameras with 1-millimetre lenses in digital boxes, hair dryer holders and wall sockets in 42 rooms in 30 hotels across the Republic of Korea, and streaming the footage live online. At the time of the arrest, the suspects had filmed 1,600 guests, set up a website and gathered 97 monthly subscribers.[34] K-Pop celebrities have also been arrested for filming themselves having sex with women, uploading the videos to Internet chat rooms and allegedly operating prostitution rings.[35]

Hidden cameras were reportedly found installed in different blocks of a university in Pakistan in 2019. The footage was used to harass, extort and blackmail students.[36] The scandal strained the already critical struggle to educate girls and women, and reportedly resulted in parents pulling their daughters out of higher educational institutions in a province with an already low schooling rate for women and girls.[37]

Online harassment

Online sexual harassment that takes place through phone calls, text messaging, mobile phone apps and the Internet. According to a 2018 survey by the Malaysian Centre for Constitutionalism and Human Rights, 50.4 per cent of respondents had experienced one form of online harassment at least once in their life, with women experiencing online sexual harassment at least twice as often as men.[38]

According to Malaysian CSOs, Muslim women's advocates, in particular, are harassed online over dress and behaviour deemed "inappropriate" by those intent on moral policing of women's bodies

33 CNA Insider, 2018, "South Korea's Digital Sex Crime Wave," YOUTUBE, 24 February, https://www.youtube.com/watch?v=n8EVv1FFl5I. See also Derrick A Paulo, 2018, "In South Korea, a society faces up to an epidemic of sexual harassment," CNA, 24 February, https://www.channelnewsasia.com/news/cnainsider/south-korea-sexual-harassment-revenge-porn-abuse-get-real-9987316.

34 Justin McCurry, 2019, "Arrests over hotel spycam porn ring that filmed 1,600 guests across South Korea," *The GUARDIAN*, 20 March, https://www.theguardian.com/world/2019/mar/21/arrests-over-hotel-spycam-porn-ring-that-filmed-1600-guests-across-south-korea. See also Justin McCurry, 2019, "Spycams, sex abuse and scandals: #MeToo reaches Korean pop," *The GUARDIAN*, 22 March, https://www.theguardian.com/music/2019/mar/22/metoo-k-pop-music-industry-sexaul-assault-scandals-korean-cultural-life.

35 Justin McCurry, 2019, "'K-Pop's Great Gatsby': Seungri charged over prostitution ring," *The GUARDIAN*, 12 March, https://www.theguardian.com/world/2019/mar/12/k-pop-scandal-big-bang-seungri-south-korea-charged-over-illegal-prostitution-ring.

36 Bilal Raza, 2019, "Blackmailing, harassment of students exposed in Balochistan University," SIASAT, 14 October, https://www.siasat.pk/forums/threads/blackmailing-harassment-of-students-exposed-in-balochistan-university.719888/.

37 Imam Sultan, 2020, "How blackmail, harassment forced Pakistani women from university," AL JAZEERA, 9 January, https://www.aljazeera.com/indepth/features/blackmail-harassment-forced-pakistani-women-university-200107095706289.html. Statistics as quoted by Imam Sultan from the Pakistan Bureau of Statistics.

38 LB Systems, 2018, "Cyber harassment in Malaysia – What do we see happening?" Malaysian Centre for Constitutionalism and Human Rights, 31 January, https://mcchr.org/2018/01/31/cyberharassment-in-malaysia-what-do-we-see-happening.

and actions. For example, a notable female politician and a celebrity were both publicly harassed for not wearing hijabs "properly". A young woman was bullied online after posting a photo of her night out with friends. Another female politician was harassed online for not putting on make-up, and for supporting a civil society organization deemed "deviant" by her attackers due to its work on the rights of Muslim women.

In a 2016 survey on ICT VAWG in India, 58 per cent of respondents "had faced some kind of online aggression in the form of trolling, bullying, abuse or harassment".[39]

Online harassment in Pakistan has resulted in women and girls being unable to maintain their own accounts on social media.[40] A CSO respondent said that data from programmes with girls suggest that only 17 per cent of girls had social media accounts in their own names. The others either maintained accounts anonymously (for example, under the name of a male relative) or cancelled their social media accounts altogether due to hacking and online harassment.[41] Families mostly do not want to disclose that their female members are being harassed; they would rather report a gender-neutral crime. This leads to underreporting of harassment cases and widespread impunity.

In the Philippines, 80.5 per cent of CSO survey respondents said that perpetrators were typically friends or acquaintances of victims/survivors, a pattern also reported by 65.7 per cent of respondents in Malaysia and 70 per cent in Pakistan.

In the focus group discussions, CSOs highlighted how some female journalists had stopped writing on "sensitive" political issues due to intolerable harassment and gender hate speech (see Box 1).[42] The harassment targeting female journalists was more sexualized and intense than that aimed at male journalists.

BOX 1:

A DIRECT ATTACK ON PARTICIPATION AND HUMAN RIGHTS

ICT VAWG against women's rights ADVOCATES, journalists and politicians is a direct attack on women's visibility and full participation in public life.[43] Yet, as with other forms of non-physical harassment, victims are often told to "just ignore it". This response fails to acknowledge the fact that, in an increasingly digitalized world, the victim/survivor often does not have the luxury of turning off her computer to ignore the harassment. Further, harassment can occur across different online or digital media. Given the importance of digital interactions, the prospect of disconnecting altogether can make ICT VAWG a profoundly isolating experience for the victim/survivor.

The UN Special Rapporteur on Violence Against Women, its Causes and Consequences concluded in her report on violence against women in politics that "the aim of violence against women in politics is to preserve traditional gender roles and stereotypes and maintain structural and gender-based inequalities… Ultimately, online violence against women in politics is a direct attack on the full participation by women in political and public life and their enjoyment of their human rights".[44]

39 From a survey with 500 respondents (97 per cent women and 3 per cent transgender) from major Indian cities such as Delhi, Mumbai, Bangalore, Chennai, Hyderabad and Kolkata. Japleen Pasricha, 2016, *Violence online in India: Cyber crimes against women and minorities on social media, Feminism in India*, https://feminisminindia.com/wp-content/uploads/2016/05/FII_cyberbullying_report_website.pdf. See also Shreya Kalya, 2016, "Survey Finds Nearly 50% of Women In Indian Cities Face Online Abuse, Fewer Report Them," *INDIA TIMES*, 6 December, https://www.indiatimes.com/news/world/survey-finds-nearly-50-of-women-in-indian-cities-face-online-abuse-fewer-report-them-266051.html.

40 DIGITAL RIGHTS FOUNDATION, 2017, Measuring Pakistani Women's Experiences of Online, Violence: A Quantitative Research Study on Online Gender-Based Harassment in Pakistan, https://digitalrightsfoundation.pk/wp-content/uploads/2017/05/Hamara-Internet-Online-Harassment-Report.pdf.

41 Focus group discussion with CSOs in Pakistan, July 2019.

42 Focus group discussion with CSOs in Pakistan, July 2019.

43 Centre for Social Research, 2014, *Violence against women in politics: A study conducted in India, Nepal and Pakistan*, https://www.unwomen.org/en/digital-library/publications/2014/6/violence-against-women-in-politics#:~:text=The%20study%20also%20finds%20that,their%20resolve%20to%20join%20politics.

44 Šimonović, Report of the Special Rapporteur. See also Dubravka Šimonović, 2018, Violence against women in politics, A/73/301, 6 August, https://undocs.org/en/A/73/301.

Gender hate speech, cyberbullying and mob attacks

Gender hate speech includes hateful, insulting, demeaning, shaming and vitriolic comments and other forms of expression, based on a person's gender, often inferring that the person should either harm herself or that the person should be harassed or harmed (psychologically or physically). Gender hate speech can lead to cyberbullying.

In interviews in the Republic of Korea, key informants referred to the cyberbullying of Sulli, a female celebrity who committed suicide as a result of the viciousness of the attacks she experienced.[45] When joined by mobs of people, vicious cyberattacks are also known as dog-piling. Sulli defied conservative social expectations towards women and engaged in social issues such as women's reproductive rights. She also spoke out against the toxicity of the online abuse she endured.

According to a 2016 survey by the Korean National Human Rights Commission, 85 per cent of women experienced hate speech online.[46] The study found that women may even conceal their identities for fear of hate crimes. More than half of the respondents said that they did not know how to deal with online and offline misogyny and hate crimes.

In Malaysia, in the case of a man who threatened and slandered his wife in blog postings, comparing her to a prostitute and swindler, the court ruled that these posts had caused suffering and continuous exceptional hardship, mental stress, deep humiliation, untold embarrassment and misery for the victim/survivor.[47]

45 Interview with CSOs and government stakeholders in the Republic of Korea. See also Reuters, 2019, "After death of K-pop's Sulli, calls to strip cyber bullies of anonymity – from fellow singer and victim Solbi, music industry and fans," *SOUTH CHINA MORNING POST*, 18 October, https://www.scmp.com/lifestyle/entertainment/article/3033397/after-death-k-pops-sulli-calls-strip-cyberbullies-anonymity, last visited 14 May 2020.

46 Sung Soo Hong and others, 2017, *The situation of hate speech and regulatory measures to combat hate speech*, National Human Rights Commission of Korea.

47 LB Systems, 2018, "Cyber harassment in Malaysia – What do we see happening?" Malaysian Centre for Constitutionalism and Human Rights, 31 January.

CSOs in Malaysia as well as Pakistan said that they were frequently attacked because of their work and political stances, including after annual International Women's Day marches. They claimed that, at times, the conservative media instigates these attacks by emphasizing that CSOs champion a liberal agenda such as LGBTIQ+ issues.

Mass media reports confirmed that organizers of the 2019 International Women's Day marches in both countries were harassed, and subjected to hate speech and documented body-shaming, as well as death and rape threats on social media.[48] Photos of participants in the marches were shared on social media without consent, followed by hateful and degrading comments.[49] The organizers also complained that "[t]he media played a massively

48 Saad Sayeed, 2019, "The International Women's Day march in Pakistan has led to death and rape threats on social media," *REUTERS NEWS*, 16 March, http://news.trust.org/item/20190316132548-xy3gv. See also Bina Shah, 2019, "The Real Enemy of Pakistani Women Is Not Men – It is society's acceptance of patriarchy," *The New York Times*, 17 April, https://www.nytimes.com/2019/04/14/opinion/pakistan-womens-march.html. Danial Dzulkifly, 2018, "After Women's March, participants harassed online and offline," *MALAY MAIL*, 10 March, https://www.malaymail.com/news/malaysia/2018/03/10/after-womens-march-participants-harassed-online-and-offline/1595223.

49 Netizen Report, 2019, Activists in Pakistan and Malaysia confront online backlash after International Women's Day events, *GLOBAL VOICES AD VOX*, 28 March, https://advox.globalvoices.org/2019/03/29/netizen-report-activists-in-pakistan-and-malaysia-confront-online-backlash-after-international-womens-day-events/.

negative role in this campaign ... they just looked at what trolls were saying online and picked up (on) a few placards that were provocative to try and sell their content".[50]

In the Philippines, advocates described how LGBTIQ+ advocates promoting the Sexual Orientation and Gender Identity Expression Equality Bill were subjected to cyberattacks, including through the use of culture and religion to incite hatred, and threats of physical violence.[51]

A 2020 Indian survey of 630 school-going adolescents in Delhi found that 9.2 per cent had experience cyberbullying. Only half had reported their experiences to teachers, guardians or Internet intermediaries. Vulnerability to cyberbullying increased with Internet use: 22.4 per cent of respondents (aged 13-18 years) who used the Internet for more than three hours a day were exposed to online bullying, while up to 28 per cent of respondents who used the Internet for more than four hours a day faced cyberbullying.[52] The correlation between cyberbullying and Internet use is more alarming now given that children and adolescents spend up to seven hours online each school day due to the COVID-19 pandemic.

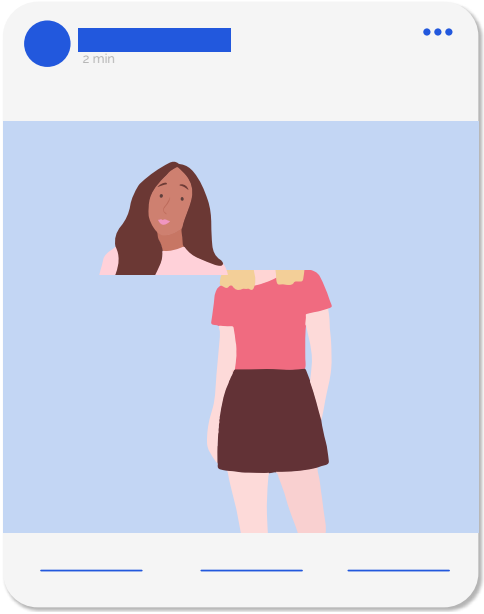
Morphing/transmogrification

A very specific form of digital sexual violence is **morphing, transmogrifying or splicing photos or videos** (for example, using "deep fake" applications to morph the head of a victim/survivor onto another image), and uploading them, including onto pornographic websites. In the Republic of Korea, key informants said that perpetrators would derogatorily "sexualize" images of female celebrities or women whom they know by morphing them into a composite image called *ahegao* (originating from Japan) or "slut-reporting".

50 Sayeed, "The International Women's Day march," quoting an interview with Nighat Dad. Similar sentiments were shared by advocates during focus group discussions in Pakistan and Malaysia in July and August 2019, respectively.

51 Discussion with Filipino advocates in October 2019.

52 Childright and You, 2020, *Online safety and internet addiction: A study conducted amongst adolescents in Delhi-NCR*, https://www.cry.org/wp-content/uploads/2020/02/Online-Safety-and-Internet-Addiction-p.pdf.



Cyberflashing

Cyberflashing is the practice of sending women unsolicited images of male genitalia, often with the intent of silencing women. One advocate related that she started receiving numerous Skype and WhatsApp calls with the flashing of private parts. "It was one way to harass and silence women. Pictures of male genitals were sent. These pictures were unsolicited. I experienced psychological trauma. There were also direct threats sent via messaging to my number." Other advocates shared that they immediately deleted these images for fear that their husbands and male relatives would discover them. Although they are prepared for online harassment for their political work, they intimated that ICT VAWG still affects them and causes them to pause, even as they continue their advocacy.

Online threats and blackmail

Advocates noted that online threats or blackmail are more challenging to investigate and more likely to be trivialized by the police. Blackmail is

very common and deters women from coming forward. Women who have pursued cases against these practices have been intimidated and forced to recant through further blackmail, such as threats to release material or compromising images (whether genuine or fake) online.

An advocate also shared that in one case, a male subordinate blackmailed his female boss after she innocently handed him her phone to download a document. "He was her subordinate but was harassing his boss. Power dynamics related to supervisor-subordinate in this case did not matter as male privilege was more important."

Media reports underline the extent to which blackmail is perpetrated. In 2016, Pakistan woke to news of online violence against students at a college. An 18-year-old opened an email to see a picture of her face digitally combined with the naked body of another person.[53] The perpetrators, going by the pseudonym Gandageer Khan, had harassed and blackmailed 50 young women for four years before they were arrested. The perpetrators hacked into women's Facebook accounts to steal their photos.[54]

Identity theft and fake profiles

Identity theft and fake profiles involve perpetrators posing as the victim/survivor and acting in their name, often in a humiliating or harmful manner. For example, a perpetrator may pretend to be their female target, advertise sexual services online, and provide an address and other contact information.

In the example above of the Pakistani college, perpetrators doctored several images of a female student who refused to be blackmailed and uploaded them onto a page they created on Facebook. They also doxed the student (i.e., searched and maliciously publicized her personal data). Each picture included the student's name, her phone number and a lewd message: "I am available for sex. Call me for a quickie."[55]

Non-consensual dissemination of intimate photos/videos

Accessing and/or uploading and disseminating intimate photos, videos or audio clips without consent is a critical concern. During focus group discussions with CSOs and the National Human Rights Institute in the Philippines, one predominant issue that surfaced was the pervasiveness of the non-consensual distribution of sexually explicit photos/videos of women. Participants noted that they received complaints mainly from women who were not able to leave an intimate relationship because of threats of having their sexually explicit photos disseminated online, and women whose former intimate partners disseminated their photos online as a revenge tactic.

As in the case of the Pakistani college, images are often obtained through the hacking of women's social media or cloud accounts. In *Yasir Lateef v. the State*, in Pakistan, the accused hacked the victim's Facebook account and uploaded her personal pictures online without her consent. The court condemned the actions as "obnoxious and filthy in nature".[56]

In this instance, consent refers to the uploading and dissemination of photos, and video and audio clips, not to the act of photographing or recording. When the perpetrators are intimate partners or former intimate partners of the victims/survivors, the non-consensual dissemination of photos is

53 Simon Parkin, 2016, "Pakistan's troll problem," *THE NEW YORKER*, 28 June, https://www.newyorker.com/tech/annals-of-technology/pakistans-troll-problem.

54 Ibid.

55 Ibid.

56 2016 P Cr. LJ 1916.

sometimes referred to as "revenge porn", although the expression is a misnomer. The term pornography indicates that all parties involved are aware that their acts are being recorded or photographed, and that they have consented to the acts, as well as to their publication, dissemination or broadcast. If any of these essential elements are missing, the resulting recordings cannot be deemed pornography.

Filipino advocates pointed out that in early 2019, a Google drive containing lewd photos and videos of female students from one high school was shared. Boys who wanted access to the drive had to contribute a photo or video of a young girl that was perceived to be sexual in nature. The photos and/or videos were shared without the girls' consent, and the names of some were identified on the drive. Another advocate said that a similar incident occurred in her university, but no disciplinary action was taken against the offenders, and the drive was eventually deleted.[57]

Reports of similar cases have appeared in the media. A group on Facebook disguised themselves as the "Pastor Hokage Bible Study". To gain access to the group, one had to contribute a lewd photo. Members would make sexual and insulting comments, and exchange the names of women whose images were shared.[58] Once exposed, the members would regroup under a different name.

Another alarming twist in the non-consensual sharing of videos and images pertains to the dissemination of rape footage. Several media articles have reported on incidents of rape and gang rape in India and Pakistan where video clips were uploaded or traded.[59] These videos would initially be used to blackmail victims/survivors into not reporting the crime to the police, but subsequently, the footage would be "stolen" and sold. The link between suicide and sexual abuse have been the subject of several studies.[60] "One can only wonder what would have happened to these victims whose videos are being sold in the market. I don't doubt that many of them might have resorted to committing suicide", said a rape survivor of the trade in rape footage.[61]

Doxing

Doxing is the disclosure online of personal data (for example, mobile phone numbers), frequently accompanied by malicious suggestions from the perpetrator for others to contact the victim/survivor. Even if such data can be searched and obtained in the public domain, they should still be considered personal.

Doxing constitutes ICT VAWG. It is sometimes more egregious, however, when the disclosure is accompanied by images of the victim/survivor. For example, some sites post photos of "beautiful women" taken in public places together with their names.[62] This is problematic in societies where women and girls can be subjected to VAWG for having their photos and videos posted online, even if not by them.

Sextortion

Sextortion is extorting sex or sexual favours by threatening to disseminate intimate images and rape footage. Online, women and girls are susceptible to unsolicited sexual advances through social media. Filipino advocates described how a 16-year-old girl received random Facebook requests from foreign men, asking her to show them her body.[63] Once predators have obtained intimate photos of their targets, the latter are susceptible to sextortion.

57 Focus group discussion with CSO advocates in the Philippines in October 2019.

58 Margaret Claire Layug, 2017, "'Pastor Hokage' FB groups trading lewd photos of women exposed," *GMA NEWS ONLINE*, 3 July, https://www.gmanetwork.com/news/hashtag/content/616746/pastor-hokage-fb-groups-trading-lewd-photos-of-women-exposed/story/.

59 BBC News, 2015, "How a rape was filmed and shared in Pakistan," 26 February, https://www.bbc.com/news/world-asia-31313551. See also Asad Ashraf, 2016, "A dark trade: Rape videos for sale in India," *AL JAZEERA*, 31 October, https://www.aljazeera.com/indepth/features/2016/10/dark-trade-rape-videos-sale-india-161023124250022.html.

60 For example, Daniel L. Segal, 2009, *"Self-Reported History of Sexual Coercion and Rape Negatively Impacts Resilience to Suicide Among Women Students," Death Studies* 33: 848–855.

61 Ashraf, "A dark trade: Rape videos for sale."

62 Discussion with advocates in July and October 2019.

63 Focus group discussion, the Philippines, October 2019.

In the Nth Room Telegram ring dismantled by police in the Republic of Korea in early 2020, women and children were blackmailed into performing sexually explicit acts on camera, with thousands of users paying cryptocurrency to watch.[64]

Grooming, predation and exploitation of women and girls

The Philippines National Baseline Survey on Violence Against Children cited 7,000 reports of cybercrime per month, half of which were related to child sex abuse.[65] The survey also found that nearly one in two children aged 13 to 17 had experienced ICT violence.[66] Driven by poverty, the live-streaming of child sexual abuse has boomed in the Philippines because of the country's high level of English, good Internet access and well-established money transfer systems.[67] Complicating this is the fact that live-streaming may be conducted at home by family members, including parents, rather than crime syndicates.[68]

NEARLY
one in two
children aged 13 to 17 had **experienced ICT violence**

64 Kelly Kasulis, 2020, "New arrest amid nationwide anger over S Korea 'sextortion' case," *AL JAZEERA*, 11 May, https://www.aljazeera.com/news/2020/05/arrest-nationwide-anger-korea-sextortion-case-200511031427033.html.

65 Emma Batha, 2016, "Internet providers urged to tackle live streaming of child sex in the Philippines," *REUTERS*, 6 June, https://www.reuters.com/article/us-philippines-internet-child-sexcrimes-idUSKCN0YT04W. Council for the Welfare of Children, 2016, *National Baseline Study on Violence against Children: Philippines*, October, https://www.unicef.org/philippines/sites/unicef.org.philippines/files/2019-02/phl-nbsvac-resultssummary.pdf.

66 Council for the Welfare of Children, *National Baseline Study*.

67 Emma Batha, "Internet providers urged to tackle live streaming."

68 Oliver Holmes, 2016, "How child sexual abuse became a family business in the Philippines," *The GUARDIAN*, 30 May, https://www.theguardian.com/world/2016/may/31/live-streaming-child-sex-abuse-family-business-philippines.

The transnational nature of this crime, with victims and perpetrators living thousands of miles apart, requires close police cooperation and joint prosecution efforts with countries where the perpetrators originate, including Australia, the Netherlands, the United Kingdom and the United States of America.[69] One such case was prosecuted by the United States Attorney-General in 2017. In that case, a 69-year-old man paid people in the Philippines to sexually abuse children and send the images and videos to him.[70]

Despite close investigative cooperation, national police are often unable to identify the perpetrator, partially due to the use of unregistered and unidentifiable "burner" or temporary phones. They often have to resort to sting operations, setting up physical meetings with the assistance of the victims/survivors.

ICT has also expanded trafficking operations through cybersex dens.[71] In early 2020, police in the Republic of Korea uncovered online rooms on the encrypted messaging app Telegram, where users paid to see young girls perform demeaning sexual acts.[72] Sixteen minors and 74 women were blackmailed into uploading their images onto a chat group. They were lured by fake modelling jobs advertised online and blackmailed for more revealing pictures. Members

69 Mark Duell, 2019, "Paedophile ex-British Army lieutenant colonel, 70, who paid nearly £10,000 to watch Filipino mothers abuse their children on Skype from London home is jailed for three years," *DAILY MAIL*, 22 May, https://www.dailymail.co.uk/news/article-7057369/Paedophile-ex-British-Army-lieutenant-colonel-jailed.html.

70 United States Attorney's Office, 2017, "Camano Island Man [Joseph Vernon Grubbs] Sentenced to 9 Years in Prison for Paying for the Molestation of Children Viewed via the Internet," 5 October, https://www.justice.gov/usao-wdwa/pr/camano-island-man-sentenced-9-years-prison-paying-molestation-children-viewed-internet.

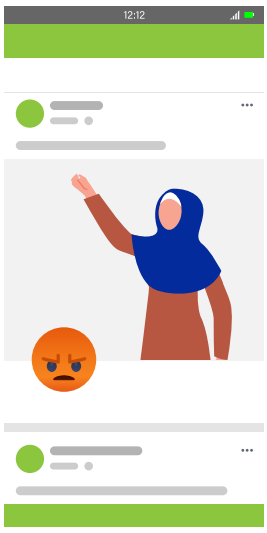
71 Lenlen Messina, *Violence Against Women (VAW) in the Digital World: Emerging Issues, Challenges and Opportunities – VAW in the Philippines*, ISIS INTERNATIONAL, https://www.isiswomen.org/index.php?option=com_content&view=article&id=1475&Itemid=346.

72 Yoonjong Seo, 2020, "Dozens of young women in South Korea were allegedly forced into sexual slavery on an encrypted messaging app," CNN, 28 March, https://www.cnn.com/2020/03/27/asia/south-korea-telegram-sex-rooms-intl-hnk/index.html. See also Kasulis, "New arrest amid nationwide anger."

would pay thousands of US dollars to enter the chat rooms; premium members could make increasing demands of the women and girls, who were referred to as slaves.

With schooling now moving online for children as young as 7, the risk of encountering predators online has increased. Sometimes, predators groom children before escalating the abuse to more explicit sexual acts. Women with disabilities are targeted too. The social isolation they experience means that they tend to rely on social media as a means of establishing and maintaining human connection. In some cases, perpetrators exploit their trust, which leads to acts of physical and sexual violence.[73]

Femicide and online activity



Whether offline or online, some women are targeted when they deviate from expected gender norms, behaviours, ideas, outlooks or attitudes. For example, women and girls may be subjected to VAWG for being active online or if their photos and videos are posted, even if not by them. In Pakistan, the first reported case of an ICT-related honour killing took place in Kohistan. Four women were killed after an online video showed them clapping and singing at a private wedding celebration. The whistleblower who exposed the killings and three of his brothers were also killed.[74]

In another case in Pakistan, model and activist Qandeel Baloch was killed by her brother, who stated it was because, "She was doing videos on Facebook and dishonouring the family name...."[75] In 2013, a group of men murdered two teenage girls and their mother after a video was posted that showed them dancing in the rain.[76]

Cyberstalking

Cyberstalking is the unwanted surveillance or monitoring of a person through ICT, namely the Internet or other electronic applications and platforms. It constitutes a pattern of behaviour that causes harm or distress.

In domestic violence cases, the perpetrator may harass and stalk the victim both on and offline. The use of geolocation and facial recognition applications by partners, former partners and rejected suitors to stalk victims/survivors is also an issue. Courts must be vigilant to ensure that restraining orders include cyberstalking and online harassment. For example, in Malaysia, the court interpreted its power to order a person "to refrain from approaching his spouse or former spouse" by applying it to the case of a husband who was ordered to stop stalking, harassing and attempting to stalk and/or harass his wife "whether in cyberspace or otherwise".[77]

LGBTIQ+-related ICT violence

During focus group discussions in Malaysia and Pakistan, advocates revealed that they were sometimes attacked either because of their political stance on LGBTIQ+ issues or because they were assumed to have supported LGBTIQ+ issues or be LGBTIQ+ themselves.

They described how during International Women's Day marches, the media would accentuate LGBTIQ+ issues and the involvement of LGBTIQ+ individuals and groups. In the clickbait culture, users race to elicit the highest emotional response. Videos of

73 Yoonjong Seo, "Dozens of young women in South Korea."

74 BBC, 2019, "Kohistan video murders: Three guilty in 'honour killing' blood feud," 5 September, https://www.bbc.com/news/world-asia-49592540.

75 John Boone, 2017, "'She feared no one': the life and death of Qandeel Baloch," *The GUARDIAN*, 22 September, https://www.theguardian.com/world/2017/sep/22/qandeel-baloch-feared-no-one-life-and-death.

76 Parkin, "Pakistan's troll problem."

77 Teh Bee Chin v Goh Swee Poh [2018] MLJU 192.

supporters chanting pro-LGBTIQ+ slogans went viral within six hours of posting and galvanized attacks against women's and LGBTIQ+ groups.[78]

LGBTIQ+ individuals on dating apps are especially vulnerable to rape and sexual exploitation. Rapes occurring via matchmaking through dating apps are not usually reported. Some dating apps place a disclaimer saying that sexual violence could happen, and that users should take the necessary precautions. Dating apps such as Tinder employ filters to check for problematic views.[79] These apps can detect offensive messages and ask the user whether they'd like to report them; it also has a panic button alerting law enforcement to provide emergency assistance. Photo verification is further intended to reduce "catfishing".[80, 81] Still, regular complaints that dating apps have not taken steps to remove or block known sex offenders have led the United States Government to investigate them.[82]

(D) WHERE DOES ICT VAWG HAPPEN?

CSO advocates indicated that high levels of ICT VAWG happen mostly on social media platforms and messaging apps as well as video-sharing platforms (Figure 2).

In the Republic of Korea, CSOs suggested that ICT VAWG is common on the messaging app Kakao Talk and the online platform Naver (both popular there) as well as Tumblr. In Malaysia, they indicated that it commonly occurs on WeChat, the Chinese language messaging and social media app.

Advocates suggested that ICT VAWG also happens on dating apps. ICT violence against LGBTIQ+ individuals is particularly common on dating apps such as Grindr and Tinder.

78 Discussion with advocates in August 2019.

79 On file with author.

80 "Catfishing" is luring someone into a relationship by means of a fictional online persona.

81 The Conversation, 2020, "Tinder's new safety features won't prevent all types of abuse," 9 February, https://theconversation.com/tinders-new-safety-features-wont-prevent-all-types-of-abuse-131375.

82 Gregory, "A predator kept targeting victims."

Figure 2: CSO perceptions of the occurrence of ICT VAWG on different platforms

Note: Respondents from India, Malaysia, Pakistan, the Philippines, the Republic of Korea. Percentage, n=38 (yes/no). Mobile phone refers to text messaging and calls. Google includes Google drive.

According to advocates, the harm caused by ICT VAWG varies depending on whether the platforms and applications are public or private. On some platforms, ICT VAWG is perpetrated openly through violent content that is shared and disseminated publicly. On other applications, such as WhatsApp and text messaging or mobile calls, ICT VAWG is communicated only to the victim/survivor or shared within a selected circle that may or may not include the victim. This also comprises "private" rings where, for example, high school or college students share intimate images of their former or current female partners.

(E) STATE OBLIGATIONS TO PREVENT AND RESPOND TO ICT VAWG

One of the objectives of the CSO questionnaire was to assess the existence and efficacy of government actions and measures against ICT VAWG. India, Malaysia, Pakistan, the Philippines and the Republic

of Korea are all signatories of the Convention on the Elimination of All Forms of Discrimination against Women (CEDAW). They have accepted obligations to pursue, by all appropriate means, the principle of equality of men and women, to adopt legislative and other measures, to eliminate discrimination against women, and to modify or abolish existing laws, regulations, customs and practices that constitute discrimination against women.[83] Comprising 23 experts who monitor the implementation of the Convention, the CEDAW Committee has reiterated that violence against women is a form of discrimination and a violation of women's human rights. Seventy Member States are obligated to eliminate it.

At the national level, these obligations are mirrored in each country's constitution. All five prohibit gender or sex discrimination, and uphold fundamental liberties, including gender equality, the right to life, freedom of expression, and the equal right to enjoy constitutional rights and freedoms. The Constitution of the Republic of Korea states that international treaty obligations are equal to domestic laws. The constitutions of both the Republic of Korea and the Philippines accept principles of international law as part of their domestic laws.

Although much of ICT VAWG is perpetrated by non-state actors, States are obligated to formulate and implement effective measures to prevent and respond to it, wherever it occurs, and by whomever is perpetrating it. This is the due diligence principle, which can be broken down into five obligations: to prevent violations, protect victims/survivors, prosecute and investigate violence, punish perpetrators, and provide redress and reparation for victims/survivors.[84]

As front-line advocates against ICT VAWG, CSOs were asked about their knowledge of existing state measures and their perceptions of implementation. The findings were indictive of whether governments had taken rigorous action to promote their programmes and policies among the public, civil society, first responders (for example, crisis intervention centres) and target communities.

Prevention

Prevention refers to stopping violence before it occurs, and involves transforming social norms, attitudes and behaviours. Secondary prevention – intervening early to stop abuse – will be covered under the discussion of protection.

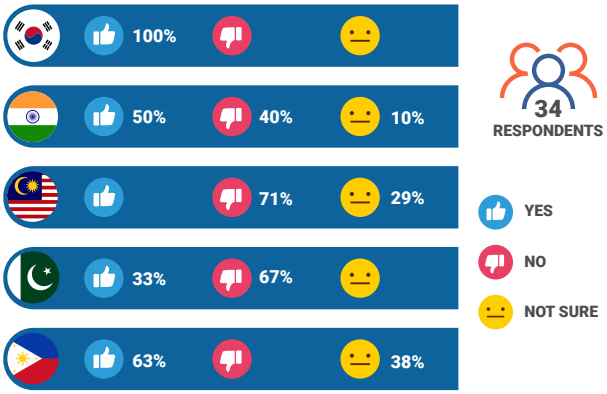
CSOs showed mixed awareness of state-supported efforts to prevent ICT VAWG (Figure 3). When asked whether the State implements ICT VAWG prevention programmes, most CSOs in India, Pakistan, the Philippines and the Republic of Korea answered yes, although only in the Republic of Korea were all respondents aware of programmes in their country. This indicates that some governments have had more success in publicizing their prevention programmes, which is critical in ensuring these programme achieve their intended impact.

Discussions with civil society advocates indicated that when government prevention programmes do exist, for example, in schools, they tend to focus on cyberbullying and safe Internet use for children. Programmes for the general public usually emphasize seditious and hate speech (based on race and religion, but not gender), or the dissemination of misinformation. These programmes do not typically include ICT VAWG.

83 Convention on the Elimination of All Forms of Discrimination against Women, Article 2, https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=IV-8&chapter=4&lang=en. See also General Recommendation 28 on the core obligations of States under CEDAW, https://documents-dds-ny.un.org/doc/UNDOC/GEN/G10/472/60/PDF/G1047260.pdf?OpenElement.

84 Zarizana Abdul Aziz and Janine Moussa, 2014, *Due Diligence Framework: State Accountability Framework for Eliminating Violence against Women*, International Human Rights Initiative, https://www.peacewomen.org/sites/default/files/Due%20Diligence%20Framework%20Report%20final.pdf.

Figure 3: CSO perceptions of state prevention programmes



When interviewed, state representatives confirmed that almost no programme aimed to prevent ICT VAWG. The only exceptions were programmes on preventing child sexual abuse as well as an initiative on matrimonial fraud conducted by the Indian police in collaboration with key stakeholders and matrimonial websites.[85]

Advocates pointed out that prevention should also employ an intersectional lens to reach underserved groups, such as persons with disabilities, racial and religious minorities, and LGBTIQ+ individuals who may experience violence differently due to their respective identities.

CSOs rated the effectiveness of state prevention programmes that they were aware of as "not at all effective" to "extremely effective" on a five-point scale. From their experience, a top-down approach to prevention is ill-suited, particularly with youth, who need interesting programmes they can engage with and relate to. Existing state programmes have not been particularly successful in employing approaches that take a more "human-centered design".

An example of a prevention programme is the Philippine National Police's Internet Child Protection programme, conducted in partnership with civil society and local governments. The programme includes online safety training sessions for schoolchildren (both elementary and high school), Internet service providers and community leaders on the inherent dangers of Internet use as well as advice on safety concerns.[86] The police also launched the Angel Net project to raise awareness and educate parents on safeguarding children from online crimes.[87] Furthermore, cybercafés have been urged to adopt a code of conduct and take measures to protect children from sexual exploitation.[88]

The Republic of Korea has initiated prevention efforts through education and awareness programmes that stress the wrongfulness of redistributing violent content, not just from a legal perspective but also from an ethical one. The Government collaborates with civil society on the programmes, which are widely available, and reach women and girls through posters in train stations, public toilets and buildings; public service announcements; and other materials on conventional and social media platforms. See also Box 2.

85 Discussions with key stakeholders and civil society advocates disclosed that online matrimonial fraud, where women seeking marriage partners on matrimonial websites are befriended by individuals with fake profiles and thereafter defrauded, is rife in India. See also the "Matrimonial Websites Fraud" prevention videos released by the Indian Police, https://www.youtube.com/watch?v=K4oNpUP340c, last visited 15 November 2019. See Summit Bhattacharjee, 2018, "Matrimonial frauds on the rise," *THE HINDU*, 16 June, https://www.thehindu.com/news/cities/Visakhapatnam/matrimonial-frauds-on-the-rise/article24176353.ece, last accessed 15 November 2019. These sites are known to also feature fake "candidates", for example, based on unsuspecting United States service members. See Jack Nicas, 2019, "Another victim in Facebook romance scams: A US congressman," *The New York Times*, 3 August, https://nytimes.com/2019/8/01/technology/facebook-military-romance-scam.html.

86 Ecpat International, 2011, *Global Monitoring: Status of action against commercial sexual exploitation of children – Philippines*, https://www.ecpat.org/wpcontent/uploads/2016/04/a4a_v2_eap_philippines.pdf.

87 Philippine National Police Anti-Cybercrime Group, 2016, "Online Child Pornography is Destroying Our Family," press release, 15 June, https://acg.pnp.gov.ph/main/press-releases/70-online-child-pornography-is-destroying-our-family.

88 Ecpat International, *Global Monitoring*.

BOX 2:

STEPS TO CONTROL DIGITAL SEX CRIMES IN THE REPUBLIC OF KOREA

In 2017, the Government of the Republic of Korea established the Digital Sex Crime Public-Private Consultative Body. Comprising government agencies, private online specialists, scholars and researchers, it has paid significant attention to online sexual harassment. A pan-Government meeting for ending sexual harassment, sexual violence and digital sex crimes was established to develop strategies and plans for a more integrated programme to stop ICT VAWG. The Ministry of Gender Equality and Family in 2018 created a separate Social Networking Service to implement digital sex crime policies, such as through posters and videos to raise awareness.

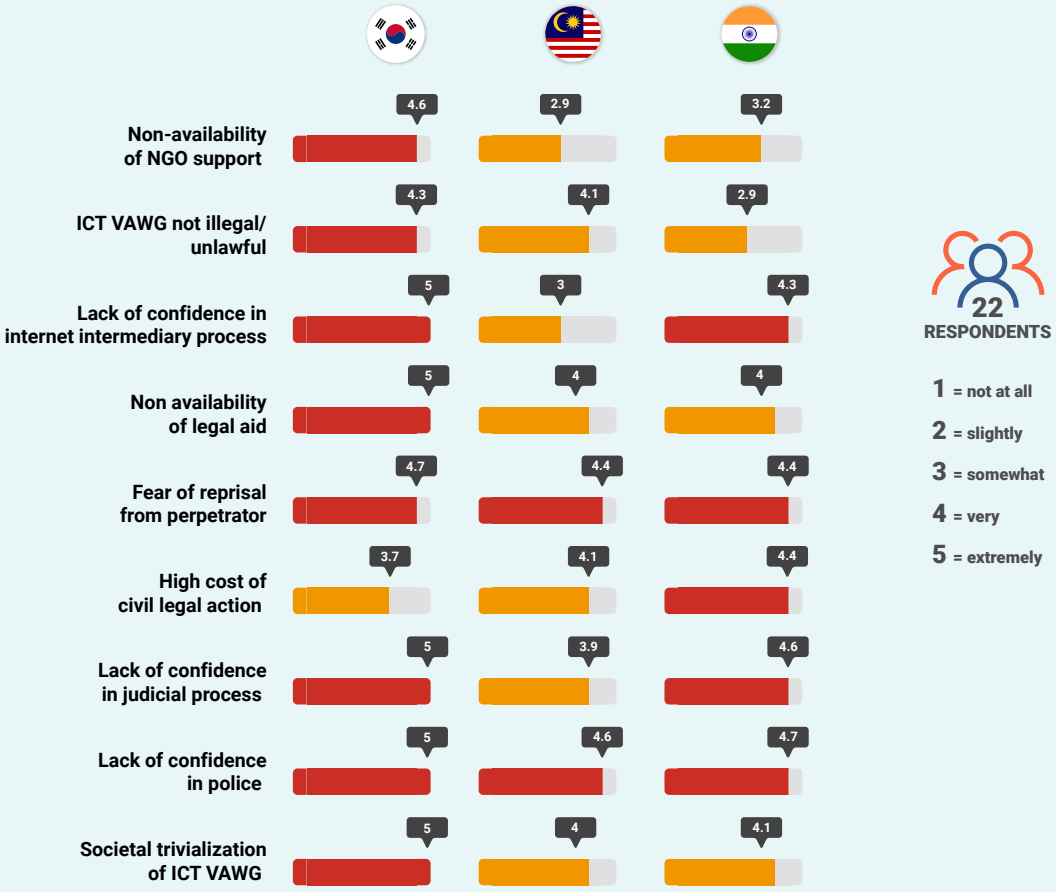
Protection of and services for victims/survivors

When asked to describe barriers to victims/survivors reporting ICT VAWG, most CSOs indicated the fear of reprisals from perpetrators, a lack of confidence in the police, the high cost of civil legal action and a lack of confidence in the judicial process (Figure 4). Societal trivialization of ICT VAWG as well as non-availability of legal aid are also problematic.

For the victim/survivor, taking action to report VAWG requires courage and confidence that the system will protect and provide services and facilities to support and see her through the process. Victims/survivors require timely services and some assurance of protection from reprisals, particularly if they know the perpetrator(s).

Measures taken by States appear to respond, to some extent, to some of these concerns (Box 3). Still, advocates suggested that services and facilities are insufficient to protect victims/survivors from further harm after an incident.[89]

Figure 4: CSO perceptions of barriers to victims/survivors reporting ICT VAWG



89 Focus group discussions with civil society advocates.

Prosecution and investigation

CSO respondents indicated that victims/survivors for the most part only sometimes, rarely or never report ICT VAWG to the authorities, preferring instead to confide in friends, work colleagues and civil society groups. If a report is lodged, it is more likely to be with the concerned ICT intermediary rather than with state authorities. Advocates also suggested that victims/survivors are more likely to report ICT VAWG if they do not know the perpetrator, given fear of retribution if they do know the person.

CSO respondents believed that ICT VAWG is a low priority for the police and prosecutors.[90] Some suggested that there is an unhealthy level of victim blaming by the police when cases are reported. Despite available data on cyber/digital crimes, advocates were uncertain whether law enforcement authorities collect gender-disaggregated data on ICT VAWG.[91]

State legislative responses

Good prevention strategies build on robust legislation and effective implementation, accompanied by programmes promoting gender equality and non-violence, and fostering a culture of intolerance for gender discrimination. It is particularly important for perpetrators to know that their actions will be punished.

Pakistan has promulgated specific laws on "electronic crimes", namely the Prevention of Electronic Crimes Act, 2019. It defines offences such as hate speech, cyberterrorism and its glorification, invasion of privacy, hacking, electronic fraud, unauthorized use of identity information, offences against the dignity of a person and offences against the modesty of a person. India passed the Information Technology Act 2008, which defines offences related to identity theft and violation of privacy.[92] Both laws are in addition to provisions in existing penal codes.

90 CSO questionnaires.

91 Focus group discussions with civil society advocates in July, August and October 2019.

92 Ministry of Electronics and Information Technology, Government of India, Information Technology Act 2008, https://meity.gov.in/content/information-technology-act.

BOX 3:

MEASURES TAKEN BY STATES TO PROTECT VICTIMS/SURVIVORS

The Philippines set up the Philippine National Police Anti-Cybercrime Group. From 2016 to March 2017, it recorded 522 cases of online libel, 226 online threats, 202 cases of photo and video voyeurism, 197 computer-related identity thefts and 127 cases of hacking. Thirty-five out of 38 victims/survivors have sought assistance from law enforcement.[93]

In the Republic of Korea, the Ministry of Gender Equality and Family has established the Digital Sexual Violence Victim Support Centre to provide support services such as counselling to victims/survivors[94] In 2017, the Republic of Korea adopted comprehensive measures to prevent digital gender-based violence. The initiative aimed to hold offenders accountable, to provide assistance to victims and to raise public awareness on digital gender-based violence.[95]

Discussions with advocates indicated that some provisions need to be reviewed and amended to ensure that they are applicable to ICT VAWG. For example, provisions on hate speech should stipulate hate speech *based on gender*. Where necessary, new provisions should be developed to address ICT VAWG, starting with, for instance, the

93 Christina Lopez, 2018, "Recognising and responding to online gender-based violence in the Philippines," Foundation for Media Alternatives, 10 November, https://www.fma.ph/2018/11/10/recognising-and-responding-online-gender-based-violence-in-the-philippines/. From experience with VAWG reporting rates, these numbers probably constitute a fraction of the actual incidences of ICT VAWG.

94 Ministry of Gender Equality and Family, 2018, "Launching comprehensive support services for digital sexual crime victims," *MOGEF News*, 24 May, http://www.mogef.go.kr/eng/pr/eng_pr_s101d.do?mid=eng001&bbtSn=705663.

95 United Nations, 2018, "Humand Rights Council Holds Interactive Dialogue with Special Rapporteurs on Violence against Women and on Migrants", GENEVA, 20 June, https://www.unog.ch/unog/website/news_media.nsf/(httpNewsByYear_en)/FF1329B93E092A03C12582B2005B00F5?OpenDocument.

non-consensual dissemination of intimate images, online sexual harassment, and stalking. The offence of sending false or offensive messages through communication services, which was repealed in India by the Supreme Court, should be replaced with a constitutionally compliant provision applicable to ICT VAWG.[96] Still, it can be difficult for States to predict the next form of ICT VAWG, which is why most legislation tends to be reactive. In general, a provision on general abuse should be in place, but not be so broad as to be unconstitutional.

The Philippines Anti-Photo and Video Voyeurism Act 2010 criminalizes the non-consensual taking, copying and reproducing of images showing a sexual act, or male and female genitalia or female breasts, as well as their publication on the Internet or in other digital media.[97] Other laws criminalize online child sexual abuse (Box 4).

At the same time, advocates advise caution in using the strong arm of criminal law. Laws such as the Communications and Multimedia Act 1998 (Malaysia) and the Information Technology Act 2000 (India), which seek to regulate ICT intermediaries and telecommunications companies, must have a narrow scope so that they cannot be used to violate freedom of expression protected by international human rights standards as well as national constitutions. They must abide by the three-tier test of suitability, necessity and proportionality.[98]

BOX 4:

LAWS FOCUSING ON CHILD SEXUAL ABUSE

The Philippines Anti-Child Pornography Act 2009 established a specialized Anti-Cybercrime Group and Cybercrime Prevention Act (R.A. 10175) 2012.[99] The Anti-Child Pornography Act obligates ICT intermediaries and service providers to notify the police of child sexual abuse material on their platforms.

The Republic of Korea has amended several laws in response to ICT VAWG, with an emphasis on child sexual abuse. These include the Act on the Prevention of Children and Juveniles from Sexual Abuse 2011, which punishes online service providers who fail to take necessary technological measures to immediately delete, prevent or block the transmission of indecent materials involving minors on the Internet, with the goal of halting the online circulation of illegal materials.[100]

Specialized courts

The Pakistan Prevention of Electronic Crimes Act 2019 provides for a specialized court and judges. Civil society advocates indicate, however, that courts and prosecutors appear to be underresourced and may benefit from (more) gender-sensitization training.[101] Malaysia too has set up specialized cybercrime courts, although they do not seem to address ICT VAWG.[102]

96 Shreya Singhal v. Union of India (2013) 12 SCC 73.

97 For a historical record of legislative reform in the Philippines, see Liza S. Garcia and Florence Y. Manikan, 2014, *Gender Violence on the Internet – the Philippine experience*, Foundation for Media Alternatives, https://www.fma.ph/wp-content/uploads/2017/09/monograph_finalz.pdf.

98 Focus group discussions with advocates in India, Malaysia, Pakistan and the Philippines. See also Malaysia: Communications and Multimedia Act, ARTICLE 19, 24 March 2017, https://www.article19.org/resources/malaysia-communictions-multimedia-act/.

99 United Nations Human Rights Council, 2017, National report submitted in accordance with paragraph 5 of the annex to Human Rights Council resolution 16/21: Philippines, A/HRC/WG.6/27/PHL/1, 1 May, https://www.refworld.org/docid/59197e344.html.

100 CEDAW Committee, 2015, Consideration of reports submitted by States parties under article 18 of the Convention, Eighth periodic report of States parties due in 2015, Republic of Korea, CEDAW/C/Kor/8, 5 October. In February 2012, further amendments expanded the range of sex crimes against minors to include indecent contact in public places, indecent conduct through ICT devices, and taking indecent photographs.

101 Focus group discussion with civil society advocates in July 2019.

102 Key informant interview with civil society advocate, April 2020.

In many countries, measures implemented during the COVID-19 pandemic, such as limited online court hearings, have negatively impacted investigative and judicial processes due to the reduced ability to implement them in person.[103]

Specialized investigators

India has established special cybercrime cells as well as an online portal – www.cybercrime.gov.in – with focal point officers to facilitate lodging complaints online.[104]

The Pakistan Prevention of Electronic Crimes Act 2019 designates specialized prosecutors and investigators. Advocates noted, however, that the Federal Investigation Authority designated under the Act is mainly located in urban centres. Measures need to be taken to ensure that courts and other services are accessible to rural women.

Advocates also suggested that States should clearly inform the public about which agencies to approach and which protocols are involved to avoid confusion, the potential for complainants to be shuttled from one agency to the other, or even cases settled/resolved by agencies that are not empowered to do so.[105]

Law enforcement investigators, for their part, complained about the lack of cooperation among ICT intermediaries in identifying alleged perpetrators. Investigations can be hampered by the use of "anti-forensics" such as end-to-end encryption that hides perpetrators' identities. Consequently, investigators have to resort to setting up stings with victims/survivors who arrange meetings with perpetrators.[106]

In the Philippines, government stakeholders shared information on the Philippine Internet Crime against Children Centre (Box 5). While in general commending government initiatives pertaining to child sexual abuse, however, advocates also stressed that similar measures should be extended to women victims/survivors of ICT VAW.

BOX 5:

A CENTRE IN THE PHILIPPINES STOPS ONLINE CRIMES AGAINST CHILDREN

In collaboration with the National Bureau of Investigation, and Australian and British law enforcement agencies, the Philippine Police established the Philippine Internet Crime against Children Centre to handle cases of online trafficking and sexual exploitation of children and women. A mix of police and National Bureau of Investigation officers undertake proactive investigations or cyberpatrolling, and receive referrals of cases from other countries. News reports confirmed that the centre has led successful global stings. It has forged links with authorities in Canada, Germany, the Netherlands, Sweden and the United States.[107]

Punishment of perpetrators

Advocates for women's rights have struggled for decades to have VAWG recognized as a public wrong, a crime and a violation of human rights, even when such crimes take place in families or out of the public view. Since rights should be protected offline and online, ICT VAWG should receive the same legal treatment as other forms of VAWG. This means that if offline sexual harassment and stalking are crimes, online harassment and cyberstalking should similarly be criminalized.

As stated above, most governments have criminalized ICT VAWG through laws that carry sentences of imprisonment and fines. After the last crackdown on yet another online sex ring, the Government of the Republic of Korea announced that it is considering strengthening punishments for both producers and

103 UN Office on Drugs and Crime, 2020, "Ciberdelito y Covid-19: Riesgos y Respuestas," 14 April, https://www.unodc.org/documents/Advocacy-Section/ES_-_Ciberdelito_y_COVID-19_spanish.pdf.

104 Key informant interview with government official, October 2019.

105 For example, the resolution of ICT VAWG cases through district/village alternative dispute resolution mechanisms.

106 Interviews and focus group discussions with investigators.

107 Matt Bloomberg, 2019, "Global taskforce tackles cybersex child trafficking in the Philippines," *REUTERS*, 15 April, https://www.reuters.com/article/us-philippines-trafficking-children/global-taskforce-tackles-cybersex-child-trafficking-in-the-philippines-idUSKCN1RR1D1.

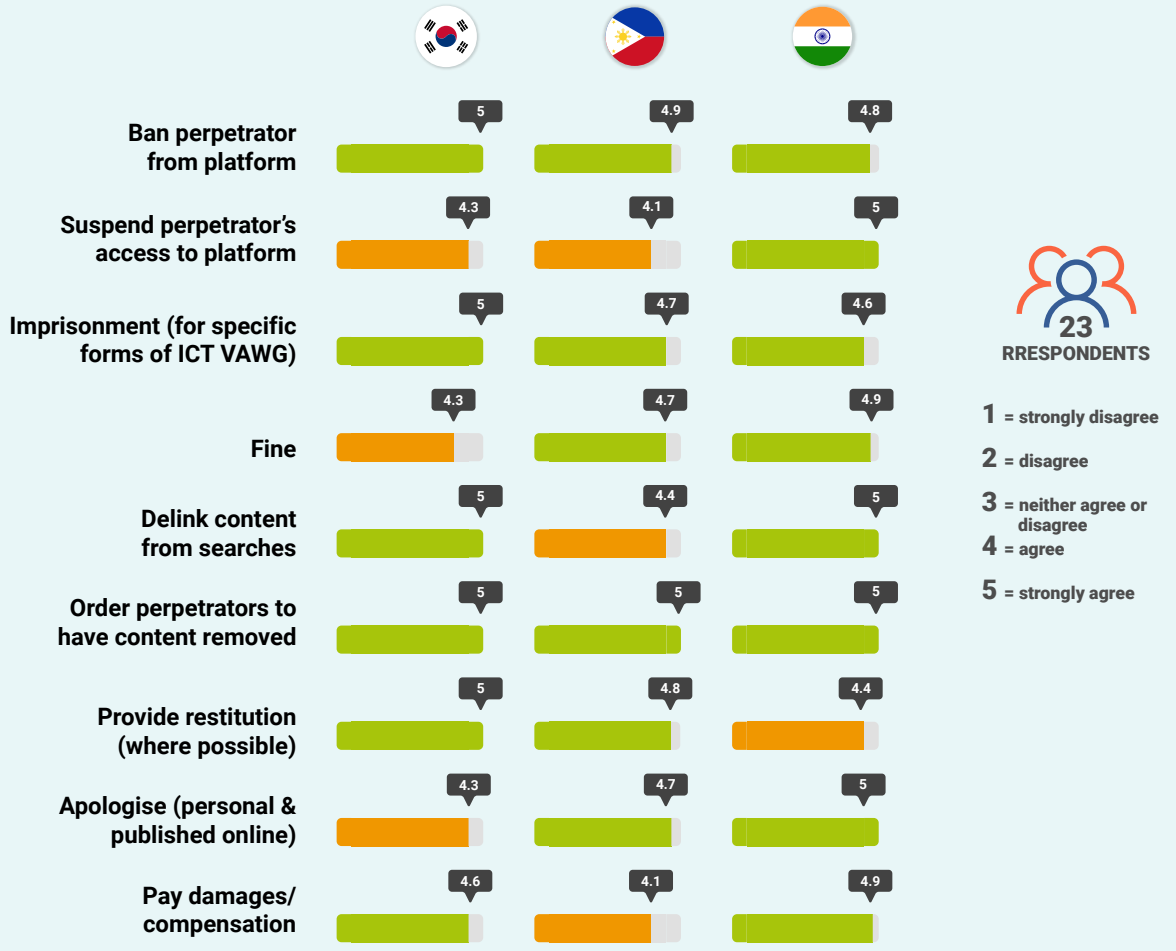
consumers of illegal "pornography" or sexual abuse material.[108]

CSOs were asked about punishments for ICT VAWG (Figure 5). All respondents saw the most effective option as being an order for perpetrators to remove content (by engaging private contractors, if necessary). Other sanctions perceived as effective are fines, delinking content from searches, and, where possible, ordering restitution. Incarceration was considered a possible sanction for some forms of ICT VAWG. There is a need to rethink and broaden the range of sanctions, aiming to prevent recidivism, deter others and rehabilitate the perpetrator.

Provision of redress and reparation

In cases of VAWG, and particularly recurring incidents, the first concern of a victim/survivor is for the violence to stop. Because there is little understanding of the harm caused by ICT VAWG, few women are likely to take action against perpetrators, particularly if the violence does not also occur offline. Rather than seeking assistance from the authorities, many women prefer instead to reduce or cease their online activities altogether. According to CSOs, seeking the intervention of the authorities or even ICT intermediaries is often a last resort (see Figure 6).

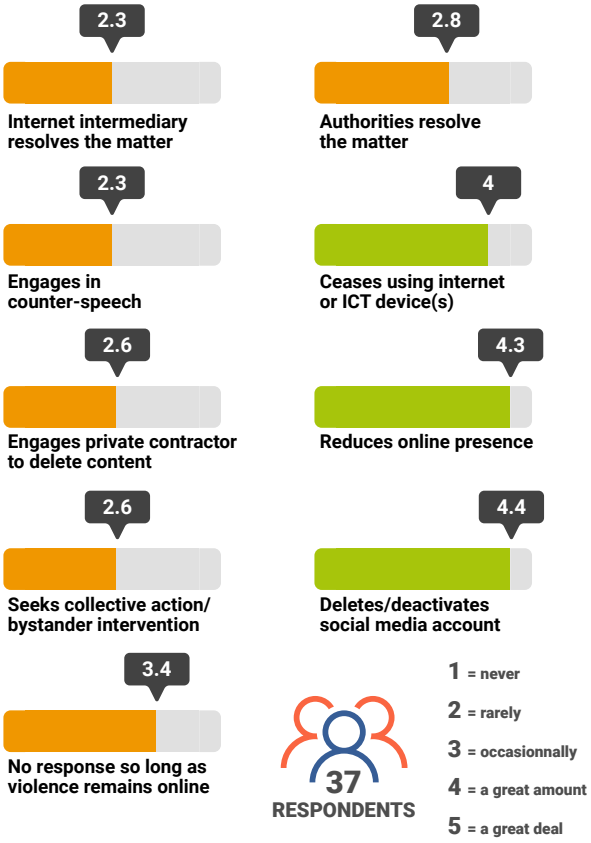
Figure 5: CSO perceptions of suitable and effective punishments[108]



108 *Korea Joong Ang Daily*, 2020, "New measures crack down on digital sex crimes," 23 April, https://koreajoongangdaily.joins.com/news/article/article.aspx?aid=3076441.

109 Chart indicates the aggregate responses of points 4 and 5 on a five-point Likert scale.

Figure 6: CSO perceptions of common responses to ICT VAWG among victims/survivors



States have established agencies empowered to delete data and images from digital spaces, either through directives issued to telecommunications companies or court orders issued to ICT intermediaries.[110] Yet once violent content is uploaded on the Internet, messaging services, social media platforms or video-sharing apps, it is difficult if not impossible to remove it. As a result, the violence continues.

In the Republic of Korea, the Act on Promotion of Information and Communications Network Utilization and Information Protection may be used to compel the deletion of content. Even though the target audience and operators are Korean, however, perpetrators may circumvent the law by using websites based abroad.[111] See also Boxes 6 and 7.

Some victims/survivors hire private contractors ("digital undertakers") to periodically delete the violent content for a fee.[112] In all countries surveyed, private contractors were hired in varying degrees by victims/survivors.

BOX 6:

THE REMOVAL ACTION TEAM TAKES DOWN VIOLENT CONTENT

In the Republic of Korea, a promising practice is the Digital Sexual Violence Victim Support Centre set up by the Women's Human Rights Institute of Korea, which is an affiliated organization of the Ministry of Gender Equality and Family. The centre offers counselling services and a Removal Action Team tasked to search for and liaise with platforms, websites and blogs to remove violent content (frequently consisting of images provided by the victim/ survivor). The team also uses a nascent artificial intelligence tool to search for violent/illegal content on websites.

In 2018, the tool identified 46 such websites. A more adept tool is being developed to track images that have been distorted (cropped or stretched) or have watermarks (added by certain sites, including pornographic ones). Current technology is unable to track images that have been morphed using "deep fake" technology, however. About 85 per cent of the removal requests are achieved, but content that could not be removed poses critical problems due to redistribution by secondary perpetrators.[113]

110 Interviews with government stakeholders, for example, the Korean Communications Standards Commission. The number of pornographic materials deleted increased from 1,404 cases in 2014 to 7,325 cases in 2016. Report of the National Human Rights Commission of Korea submitted to the UN CEDAW Pre-sessional Working Group.

111 Interview with civil society and government stakeholders in the Republic of Korea in October 2019.

112 Report of the National Human Rights Commission of Korea submitted to the UN CEDAW Pre-sessional Working Group. In the Republic of Korea, this may cost 500,000 to 3 million won (approximately USD 400 to 2,400) a month.

113 Key informant interview, November 2019.

Seeking bystander intervention is a less common response. If carefully undertaken, this can be effective, as ICT VAWG is frequently witnessed by hundreds, if not thousands, of users.

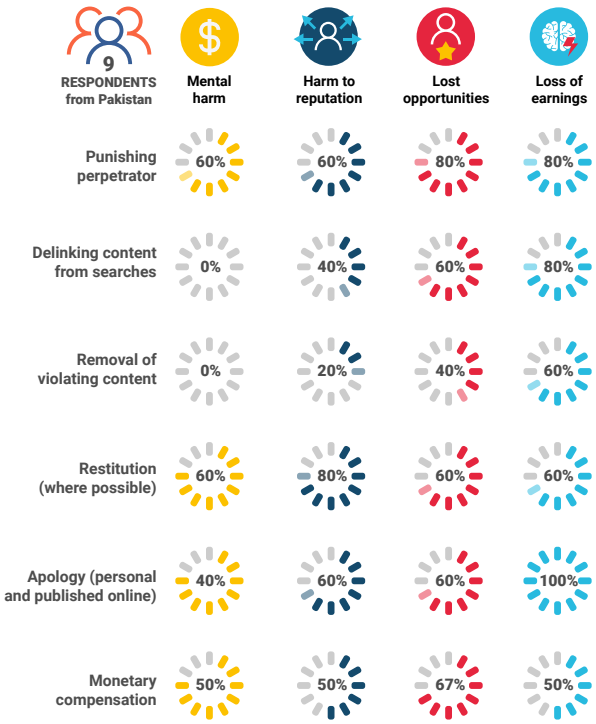
BOX 7:

LAWS TO BLOCK CONTENT IN INDIA AND MALAYSIA

Legislation in India allows blocking content as an alternative to removing it. Under section 69A of the Indian Information Technology Act, the "Central Government may, in the interest of preventing incitement to the commission of cognizable offences, direct any agency or intermediary to block access by the public of any information…".

Similarly, the Malaysian Communication and Multimedia Commission is empowered to instruct telecommunications companies to block violent content.[114] This only denies access within a country, however. It does not necessarily result in the removal of content from the digital space.

Figure 7: CSO perceptions of appropriate redress and reparations for harm resulting from ICT VAWG



Note: For losses such as expenses related to medical and legal interventions and engaging a technical expert to remove violent content, respondents indicated that the most appropriate remedies apart from punishing the perpetrator would be restitution and monetary compensation.

In answer to a question on the appropriate redress or reparation for harm resulting from ICT VAWG, a Pakistani CSO suggested that, apart from punishing perpetrators and delinking content from searches, perpetrators should also be ordered to apologize for the mental harm caused to the victim/survivor (see Figure 7). While punishing the perpetrator is still an essential form of redress, restitution and monetary compensation may be similarly important, and can assist victims/survivors to rebuild their lives and online presence.

CSOs in general stated that just punishing the perpetrators is insufficient. Rethinking suitable remedies outside of criminal punishment may help not only to provide victims/survivors with the reparation they need, but also encourage them to report ICT VWAG.

(F) ICT INTERMEDIARY MEASURES TO PREVENT AND RESPOND TO ICT VAWG

One of the objectives of this research was to assess how ICT intermediaries prevent and respond to ICT VAWG, given that human rights violations occur in spaces they control, and from which they profit.

114 Jamie Fullerton, 2019, "Teenage girl kills herself 'after Instagram poll' in Malaysia," The GUARDIAN, 15 May, https://www.theguardian.com/world/2019/may/15/teenage-girl-kills-herself-after-instagram-poll-in-malaysia. A teenage girl committed suicide after an Instagram poll where 64 per cent of her followers, upon being asked to choose life or death, chose death.

The Internet is often regarded as a public forum, where innovation sprouts and ideas are exchanged freely. Yet access to digital spaces typically runs through private entities, commonly transnational corporations.

Defining the legal obligations of businesses is not a new concept. Businesses must exercise due diligence to ensure that their premises are safe, are not used by drug traffickers, and do not serve as centres for human trafficking or to detain women forced into prostitution. By failing to abide by these obligations, offenders risk the revocation of business licenses and the loss of their premises.

ICT intermediaries have to balance their business imperative to encourage traffic on and to their platforms with protecting freedom of speech and removing violence (Box 8). Finding this balance often generates tensions.

Interviews with ICT intermediaries disclosed a need for more clarity in understanding of ICT VAWG.[115] Industry representatives noted that it was sometimes challenging to identify ICT VAWG and requested clearer definitions.

A complication is that understanding of what constitutes ICT VAWG is coloured by different cultures. Advocates in all five countries discussed geographical and cultural differences. As can be seen in the Kohistan video case, in one context, even the most innocent videos of women celebrating an event could be used as justification for femicide. In the Republic of Korea, morphing a woman's facial image onto a composite image called "ahegao" is a form of ICT VAWG. ICT intermediaries should take steps to acquaint themselves with what constitutes ICT VAWG, what can potentially trigger it in the different countries in which they operate, and the myriad harmful consequences this has on women, including the eventual avoidance of online spaces out of safety fears.

115 Interviews conducted in person in October 2019 and via video conferencing in September 2019.

BOX 8:

AN INTERMEDIARY OFFERS TIPS ON SAFETY

During the COVID-19 pandemic, Mozilla issued an advisory on Internet safety. Everything you need to know to browse fast and free provides tips on password protection, Zoom-specific best practices and keeping personal information private, among other issues.[116]

Advocates in India and Pakistan said that it is not easy for ICT intermediaries to identify violent content in different languages, especially when it is written in a script other than Latin, as is the case in three of the five countries surveyed.[117] In Pakistan, the trend now is to use hashtags in Urdu or Pashto.[118]

Artificial intelligence and algorithms may detect certain types of violent content. In early 2020, Twitter launched "Safe DM", a plug-in that blocks and deletes unwanted images of genitalia before they reach their intended recipients. The person who developed the plugin had been cyberflashed herself.[119]

In relation to complaints of online VAWG, advocates in group discussions and interviews said that a

116 The Firefox Frontier, 2020, "Everything you need to know to browse fast and free," 26 March, https://blog.mozilla.org/firefox/stay-safe-in-your-online-life-too/.

117 The problem exists in other Asian countries such as Myanmar. See also Steve Stecklow, 2018, "Facebook removes Burmese translation feature after Reuters report," *REUTERS*, 6 September, https://www.reuters.com/article/us-facebook-myanmar-hate-speech/facebook-removes-burmese-translation-feature-after-reuters-report-idUSKCN1LM200.

118 Discussions with advocates in Pakistan in July 2019.

119 Consequently, she used artificial intelligence to build the plug-in and trained its algorithm on pictures of penises she solicited using a callout on Twitter. Isobel Asher Hamilton, 2020, "A new Twitter filter can delete unsolicited dick pics from your DMs," *BUSINESS INSIDER MALAYSIA*, 17 February, https://www.businessinsider.my/twitter-filter-deletes-dick-pics-direct-messages-2020-2?r=US&IR=T. A 2018 study among millennials in the United Kingdom found that 41 per cent of female millennials have been cyberflashed. See Matthew Smith, 2018, "Four in ten female millennials have been sent an unsolicited penis photo," YouGov, 15 February, https://yougov.co.uk/topics/politics/articles-reports/2018/02/16/four-ten-female-millennials-been-sent-dick-pic.

complaint was more likely to solicit a response from ICT intermediaries if it was lodged multiple times by multiple users. A similar finding came from a survey of 1,000 women.[120] It revealed that of the complaints from women to ICT intermediaries – on receiving offensive, graphic or insulting messages or images, on seeing their private photos posted online without their consent, and on receiving repeated messages that made them fear for their safety – more than half were either ignored or dismissed because they did not breach community guidelines.

Advocates suggested that ICT intermediaries should be open to receiving complaints from third parties. This is especially critical if the victim/survivor has terminated or suspended her account prior to lodging a complaint.[121] Requiring that the complaint be lodged from the affected account diminishes the ability of victims/survivors to report ICT VAWG.

ICT intermediaries maintained that their mechanisms are set to respond to all complaints, and that the perception that complaints lodged multiple times are more likely to receive urgent attention is wrong. They also indicated that they are increasingly taking initiatives to address ICT VAWG.[122]

ICT intermediaries deploy artificial intelligence, issue policies and community rules on etiquette and behaviour online, and employ people to filter and screen content.[123] Admittedly, some responses undertaken by ICT intermediaries have been motivated by the law and massive fines.[124] A first for such laws was the German Networking Law, which imposes fines of up to 50 million euros (USD 58.3 million) for social media companies that fail to delete comments and posts deemed in violation of German law. Unfortunately, a legal motivation may result in the uneven implementation of corporate policies, with users in some countries receiving better protection than in others. The challenge is to ensure that any policy issued by ICT intermediaries is applied equally for the benefit of all users globally.

Lengthy community rules are not effective because they are frequently not read by users, who may not be conversant in the convoluted legal jargon of community rules, despite being sufficiently tech savvy to use platforms and apps. Since users just want to start using apps and platforms, they click on "agree" without reading the rules.[125] Also, because one cannot complete a download without ticking the "accept" box, users tend to click on it without reading the terms or grasping their details.[126] For ICT intermediaries to continue relying on these terms is ineffective, even though it is legally sound. Some level of innovation is required to draw the attention of users to the more important terms of service. They should be easy to find, and expressed

120 The study was commissioned by Level Up, with 1,000 women. Fifty-four per cent of those surveyed said they had little trust in Facebook's ability to deal with harassment in a compassionate manner, and 72 per cent said the platform needed more moderators to handle complaints. Poppy Noor, 2019, "Facebook criticised after women complain of inaction over abuse," *The GUARDIAN*, 4 MARCH, https://www.theguardian.com/technology/2019/mar/04/facebook-women-abuse-harassment-social-media-amnesty.

121 Discussions with civil society advocates in August and October 2019.

122 Discussion with ICT intermediaries in September and October 2019. In May 2020, Facebook announced the setting up of the Oversight Board, an idea first floated by its CEO in 2018, among others, to hear appeals on the removal of posts. Critics calling for immediate oversight (particularly in the run-up to the United States presidential election) have established a group comprising 25 experts to analyse and critique Facebook's content moderation decisions, policies and other platform issues. Catalina Botero-Marino and others, 2020, "We Are a New Board Overseeing Facebook. Here's What We'll Decide," *The New York Times*, 6 May. Olivia Solon, 2020, "While Facebook works to create an oversight board, industry experts formed their own," ABC News, 25 September, https://www.nbcnews.com/tech/tech-news/facebook-real-oversight-board-n1240958.

123 PHYS.ORG, 2017, "Facebook adding 3,000 people to screen out violent content," 3 May, https://phys.org/news/2017-05-facebook-adding-people-filter-violent.html.

124 The first of such laws was the German Networking Law, which imposes fines of as much as 50 million euros (USD 58.3 million) if social media companies fail to delete comments and posts that are deemed to violate German law. See Soraya Sarhaddi Nelson, 2017, "With Huge Fines, German Law Pushes Social Networks to Delete Abusive Posts," NPR, 31 October, https://www.npr.org/sections/parallels/2017/10/31/561024666/with-huge-fines-german-law-pushes-social-networks-to-delete-abusive-posts, last accessed 4 May 2020.

125 Focus group discussion with civil society in India, October 2019.

126 Ronald J. Diebert, 2019, "The road to digital unfreedom: Three painful truths about social media," *Journal of Democracy* 30(1): 25-39.

in a succinct manner allowing quick understanding of the limits of acceptable online behaviour.

Often, ICT intermediaries resort to posting disclaimers stating that they are not responsible for content posted by users. Advocates suggested that such disclaimers should not result in zero liability when violence occurs, however, particularly if ICT intermediaries do not remove violent content once they know about it.[127]

Another concern is the need to alert other ICT intermediaries of identified ICT VAWG. Simple measures like watermarking can help pinpoint the source of the violent content, making it possible for ICT intermediaries to track an image or video even if it is shared and posted on other platforms.[128] While it is standard practice for business entities to guard confidential information and know-how, the cross-platform sharing of information on ICT VAWG could go some ways towards eliminating it.

Finally, ICT intermediaries can provide victims/survivors with assistance in rebuilding their online presence after ICT VAWG, for example, by allowing them to create alternative profiles, including with pseudonyms.

127 Discussions with advocates in July, August, September and October 2019.

128 Discussion with Internet intermediary in October 2019. Watermarking means overlaying embedded text or image on a video.

PHOTO: UN Women/Staton Winter

V. ANALYSIS OF ISSUES AND CHALLENGES

V. ANALYSIS OF ISSUES AND CHALLENGES

Undoubtedly, the Internet provides a fertile environment for widespread and systemic structural discrimination and VAWG. The inequalities and imbalances of offline VAWG are replicated in online and digital spaces. In other words, ICT VAWG can be understood as a continuum of offline VAWG and considered part of the systemic discrimination and gender-based violence that many women and girls experience.

Research confirms that both men and women may be subjected to online harassment. Men are more likely to experience name-calling and embarrassment ("a layer of annoyance so common that those who see or experience it say they often ignore it"), however, while women are vulnerable to more severe physical threats, harassment over a sustained period of time, stalking, sexual harassment and cyberbullying.[129]

Overall, this current research highlights that ICT VAWG is common in the five countries surveyed. Often, women are subjected to multiple forms of ICT VAWG simultaneously. They experience trolling, doxing and hacking of their social media accounts. Younger women particularly are susceptible to nasty rumours or being taunted because of how they look (body-shaming).[130] Negative cultural perception and religious interpretations provide a basis to incite hatred and threats of violence.

State responses to ICT VAWG may be based on how it is perceived both by the public and, to some extent, by state actors. These perceptions are likely to be informed by the same myths and social norms that inform offline VAWG, such as the acceptance of violence against women as "normal", the trivialization of non-physical violence, victim blaming and stigmatization of victims/survivors.

ICT VAWG presents particular challenges that must be addressed, however. These are due to ICT specificities such as ease, reach and speed of transmission, encryption, anonymity, the disinhibition that accompanies computer-mediated communications, aggregated harm as well as bystander participation.

ICT VAWG IS NOT TRIVIAL

Consequences and harm of ICT VAWG

ICT VAWG tends to be trivialized, regardless of whether or not it is a crime, and particularly when it does not involve immediate physical violence. Therefore, it receives inadequate and inappropriate responses from concerned actors, including governments, the private sector, civil society, society at large and even victims/survivors themselves. As with other forms of VAWG, women are often blamed for ICT VAWG and are reluctant to report it. In fact, "women themselves may have trouble thinking of the attacks they experience on social media platforms as 'violent,' and are more likely to block or ignore their assailants than report them".[131] Yet they may still suffer traumatic effects from a violation of their rights.

The easy and rapid dissemination of ICT VAWG across multiple platforms and networks makes the harm egregious. To advise women to block or mute harassing images and messages is to ignore the associated psychological trauma they may suffer.

129 Maeve Duggan, 2014, *Online Harassment*, Pew Research Center, https://www.pewinternet.org/2014/10/22/online-harassment/.

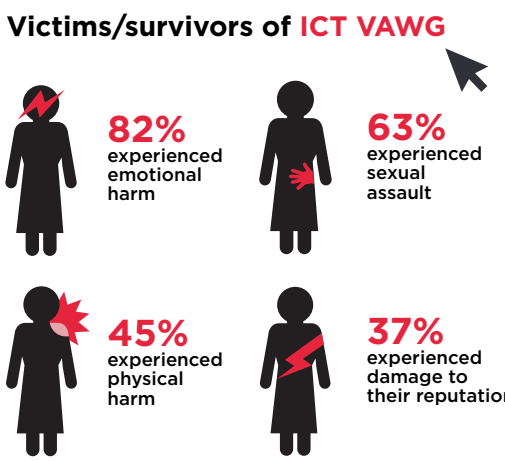
130 Ibid.

131 See Pasricha, *Violence online in India*.

It also allows the perpetrators to move on to other women. In the context of public and political life as well as mob attacks, blocking may not even be feasible.

ICT VAWG has real consequences and costs. It can result in psychological, physical, sexual or economic harm to women and girls. It can lead to depression, the inability to find employment and even suicide. The continuum between ICT VAWG and offline VAWG also means that the former can lead to physical and sexual harm, and vice versa.

An analysis of documented cases in the Philippines disclosed that victims/survivors of ICT VAWG experienced emotional harm (82 per cent), sexual assault (63 per cent), physical harm (45 per cent) and damage to their reputations (37 per cent).[132] In Pakistan, online harassment has led to suicide,[133] murder, physical assault,[134] emotional distress,[135]



132 Lopez, "Recognising and responding to online gender-based violence." The mapping was undertaken by a civil society organization, Foundation for Media Alternatives, based on victims/survivors who sought assistance from the group from 2012 to 2018.

133 Nighat Dad and Shmyla Khan, 2017, "Naila Rind killed herself because Pakistan's cybercrime laws failed her," *DAWN*, 7 January, https://www.dawn.com/news/1306976.

134 The Newspaper's Correspondent, 2014, "Two Girls, Mother Killed Over Family Video," DAWN, 25 June, http://www.dawn.com/news/1020576/two-girls-mother-killed-over-family-video. *BBC*, 2013, "Pakistani Women Shot in 'Honour Killings'," 27 June, http://www.bbc.co.uk/news/world-asia-23084689 as quoted by Digital Rights Foundation, *Measuring Pakistani Women's Experience of Online Violence*.

135 Jannat Fazal1, Shmyla Khan and Nighat Dad, 2017, "Online harassment: a retrospective review of records," MÉDECINS SANS FRONTIÈRES SCIENTIFIC DAY SOUTH ASIA, 6 June, https://f1000research.com/slides/6-785.

and women leaving their jobs and online spaces. Not having an online presence is detrimental, at a time when the Internet has assumed greater significance, even more so during the COVID-19 pandemic, in obtaining and maintaining a job, accessing information, exercising democratic rights, having a voice, getting an education and conducting commercial transactions.

The physical, sexual and economic harms of ICT VAWG may unfold over time. As one example, an explicit image may make it difficult for a victim/survivor to seek or find employment, given shame and fear that potential employers could discover the images.[136]

There is a significant risk that ICT could further broaden sexual and gender-based discrimination and violence against women and girls. Where online violence forces women to retreat from the Internet or public life, it prevents them from exercising their freedom of expression and democratic rights.[137]

Aggravated harm

Traditionally, most sexual assaults, domestic violence acts and rapes have been committed in "private", without witnesses, irrespective of whether they occur in public or private spaces. Yet ICT VAWG cases are often committed in the "online public square" in plain sight of other users. ICT VAWG may also involve masses of people who either join in the mob attack and dog-piling, or who further "like", download, forward and share violent content in numerous ways. This can take place on multiple platforms and across vast networks. A celebrity from the United States, whose intimate photos were hacked and released online, said it felt like a "ransom situation", where she was assaulted by the entire planet.[138]

Bystander participation in violent crimes online refers to third parties who recklessly download, forward and share violent content, whether they

136 Šimonović, Report of the Special Rapporteur.

137 Ibid.

138 Scott Fienberg, 2017, "Awards Chatter Podcast – Jennifer Lawrence ('Mother!')," *HOLLYWOOD REPORT*, 20 November, https://www.hollywoodreporter.com/race/awards-chatter-podcast-jennifer-lawrence-mother-1059777.

are conscious or ignorant of the fact that the content is violent or was disseminated without the consent of the subject. Although bystanders have no legal obligation to stop a wrongful act offline or online, their actions can result in continued ICT VAWG. In amplifying the harm, they can be deemed secondary perpetrators and made accountable (Box 9). Secondary perpetrators are frequently used by primary perpetrators to worsen ICT VAWG.

So far, laws have not given much attention to secondary perpetrators. A notable exception is when the violating material consists of child pornography. Unlike other crimes, child pornography is a strict liability offence. In fact, the mere possession of offending images, irrespective of intent, constitutes a crime.

BOX 9:

A CAMPAIGN CALLS OUT SECONDARY PERPETRATORS

In 2018, in the Republic of Korea, the Ministry of Gender Equality and Family actively called out secondary perpetrators under the campaign tagline: "Illegal filming is a crime. The moment you watch it, you become an accomplice". The Ministry aimed to "fundamentally improve the social culture that objectifies the female body and consumes it as entertainment as well as to eliminate the distribution structure that makes profit from illegally taken photos and videos".[139]

Holding persons accountable despite their lack of intent therefore is not without basis under the law. Further, in many jurisdictions, criminal law has developed the concept of reckless indifference where criminal intent cannot be established.[140] Secondary perpetrators can be seen, at the very least, as aiders or abettors of a wrongful act although they may not personally know the perpetrator or the victim/survivor. After all, ignoring the identity of the victim/survivor does not make ICT VAWG harmless.

In the non-criminal realm, negligence is a wrongful offence for which intent need not be established.[141] Another legal principle establishes the liability of persons who repeat slanderous or defamatory statements. Liability occurs irrespective of whether the person is aware that a statement is defamatory. Dissemination does not render an act less offensive or harmful.[142]

STIGMA

A unique feature of violence against women is that these crimes consistently involve blame, shame and stigma for the victim, not the perpetrator. Unlike other crimes, women and girls are questioned, asked what they did to bring it about, and often directly or indirectly blamed for something they did not commit.

More than the perpetrator himself, the victim/survivor bears the brunt of societal condemnation. Due to unequal gender norms around sex and sexuality for men and women, societal condemnation can be particularly sharp when the violence involves the uploading of suggestive or sexually explicit images and conversations recorded maliciously or without consent. In some contexts, women are deemed to have transgressed culturally appropriate behaviour when they establish cyberfriendships or relationships, and when women experience violence, they are blamed for not fitting into various narrow perceptions of what is acceptable, as if that might keep women safe. (Tragically, the most common form of violence against women is intimate partner violence, which occurs in the very places where women should be safest.) .

139 Ministry of Gender Equality and Family, 2019, "Illegal filming is a crime. The moment you watch it, you are an accomplice," *MOGEF NEWS*, 5 September, http://www.mogef.go.kr/eng/pr/eng_pr_s101d.do?mid=eng001&bbtSn=705865.

140 See James B. Brady, 1980, "Recklessness, negligence, indifference and awareness," *MODERN LAW REVIEW* 381, https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1468-2230.1980.tb01599.x.

141 Ibid.

142 "A false statement is not less libelous because it is the repetition of rumor or gossip or of statements or allegations that others have made concerning the matter." Ray v. Citizen-News Co., 14 Cal. App. 2d 6, 8–9 (1936).

Like offline VAWG, there is a widespread misconception that reports of sexual ICT VAWG are false. Those who have raised issues of sexual violence and expressed support for victims through online platforms in some cases have been sued or threatened with suits.[143]

CONSENT

The notion of consent is pivotal in determining whether the sharing of intimate data and images constitutes ICT VAWG. Consent must be specific to the act in question. If this act is the sharing of intimate images, consent must pertain specifically to sharing them.

Advocates indicated that law enforcers continue to overlook the non-consensual *dissemination* of content and focus instead on whether the victim/survivor consented to the *creation* of the image. This is again a case of blaming victims/survivors instead of the perpetrators. According to advocates, law enforcers frame the non-consensual sharing of images under obscenity laws, often penalizing the victim/survivor for allowing the perpetrator to capture or keep the images.[144] In Pakistan, for example, instead of investigating an offence under the new Prevention of Electronic Crimes Act in relation to the transmission of an image, an investigation may focus on whether the victim/survivor is the object of the obscene image.

By conflating the complainant as both victim and perpetrator, such decisions surely embolden perpetrators who know that victims, including minors, will not report ICT VAWG for fear of risking prosecution. This inability to report violence renders victims/survivors susceptible to sextortion and other forms of blackmail and extortion.

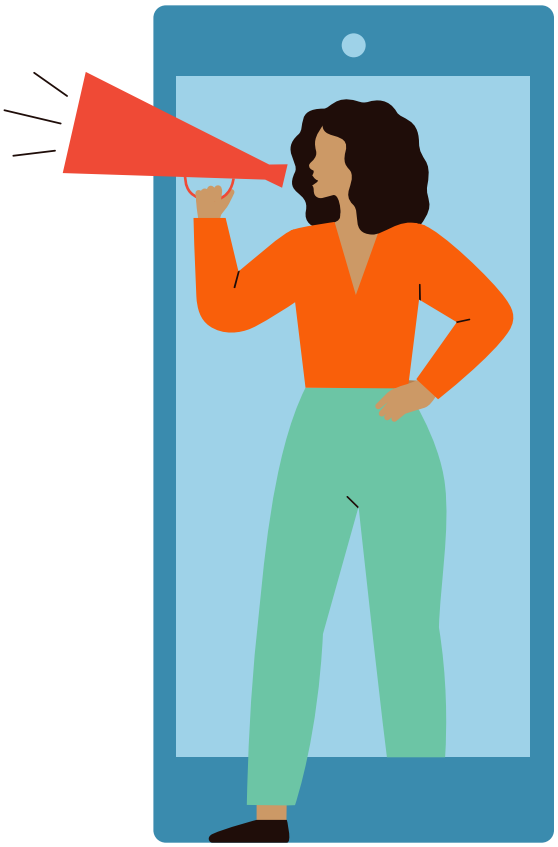
143 Concerns and Recommendations on the Republic of Korea, NGO submission to the UN Committee on the Elimination of Discrimination against Women, 2018, https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/KOR/INT_CEDAW_NGO_KOR_30063_E.pdf. Similar sentiments were expressed during focus group discussions with Pakistani and Malaysian civil society in July and August 2019, respectively.

144 Discussions with civil society advocates in India and Pakistan.

In Malaysia, perpetrators of non-consensual dissemination of intimate images were charged for misusing the Internet to distribute obscene content under the Communications and Multimedia Act 1998, instead of for violating the rights of victims/survivors.[145]

ANONYMITY, ENCRYPTION AND FREEDOM OF EXPRESSION

Law enforcement agencies have raised concerns over the difficulty of identifying perpetrators of ICT VAWG given use of end-to-end encryption. It is challenging to investigate, for example, exploitative



145 Zatul Iffah Zulkiply, 2018, "Padah sebah gambar lucah ex-girlfriend," *MY METRO*, 17 April, https://www.hmetro.com.my/mutakhir/2018/04/331480/padah-sebar-gambar-lucah-ex-girlfriend.

rings set up to be accessible only by members and protected with this technology.

On the other hand, it is simplistic to propose that anonymity and encryption be broadly restricted or removed altogether. The Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression warns that "[o]utright prohibitions on the individual use of encryption technology disproportionately restrict the freedom of expression, because they deprive all online users in a particular jurisdiction of the right to carve out private space for opinion and expression".[146]

In international law, restrictions on freedom of expression may be legally established if they are necessary for the respect of the rights or reputations of others, or for the protection of national security, public order, public health or morals, and are proportionate to the aim they seek to address.[147] The Special Rapporteur notes that the Pakistan Telecommunication Authority requires prior approval for the use of VPNs and encryption. India has ruled that service providers may not deploy "bulk encryption" on their networks, and that individuals may only use easily breakable 40-bit key length encryption without prior permission. It also requires anyone using stronger encryption to provide the Government with a copy of the encryption keys.

Key disclosure also exists by law in several European countries.[148] According to the Special Rapporteur, the law must clearly set up safeguards to ensure that the orders are limited in scope, and implemented under an independent and impartial judicial authority.

OBLIGATIONS OF THE STATE AND ICT INTERMEDIARIES

States and ICT intermediaries have different and complementary roles and functions. The State has the obligation to exercise due diligence to ensure that private individuals (non-state actors, both individuals and business entities) within its jurisdiction do not commit VAWG, including ICT VAWG. While criminal prosecution helps to punish and deter perpetrators, it is equally important for the State to create a violence-free environment where freedom of expression, human rights and gender equality are realized at the same time.[149]

Eliminating ICT VAWG cannot be achieved without the robust participation of ICT intermediaries in assuming their obligation to prevent, address and eliminate ICT VAWG. Their obligation is reflected in the 2011 United Nations *Guiding Principles on Business and Human Rights on Implementing the United Nations "Protect, Respect and Remedy" Framework*.[150] Also known as the Ruggie Principles, they provide that "business enterprises should respect human rights. This means that they should avoid infringing on the human rights of others and should address adverse human rights impacts with which they are involved."[151]

Both States and ICT intermediaries are obligated under international human rights principles to prevent and eliminate ICT VAWG. Towards this end, they must work with victims/survivors to understand the harm caused and provide appropriate responses.

146 David Kaye, 2015, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, UN Human Rights Council, A/HRC/29/3.2, 22 May.

147 United Nations General Assembly Resolution 2200A (XXI), International Covenant on Civil and Political Rights, 16 December, 1966, Article 3. The application of these restrictions by States "may not put in jeopardy the right itself". See United Nations Human Rights Committee, General Comment No. 34: International Covenant on Civil and Political Rights, Article 19: Freedoms of opinion and expression, CCPR/C/GC/34, 21, 12 September 2011.

148 United Kingdom, Regulation of Investigatory Powers Act (mandatory key disclosure); France, Law No. 2001-1062 (disclosure of encryption keys on authorization by a judge); Spain, Law on Telecommunications 25/2007 (key disclosure), as quoted in Šimonović, Report of the Special Rapporteur.

149 Report of the National Human Rights Commission of Korea submitted to the UN CEDAW Pre-sessional Working Group.

150 John Ruggie, 2011, Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, A/HRC/17/31, 21 March, http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

151 Ibid.

PHOTO: UN Women/Anam Abbas

VI. RECOMMENDATIONS AND ACTION POINTS

VI. RECOMMENDATIONS AND ACTION POINTS

PROTECTING THE INTERNET

Protecting digital public forums is imperative to encouraging innovation and public exchange. Yet human rights are also an imperative in public spaces. While these spaces require the promotion and protection of freedom of expression, they also demand freedom of association, opinion, religion and belief as well as freedom from discrimination. The consequences of ineffective measures against ICT VAWG, alongside the very damaging consequences of the violence itself, are many. They comprise the silencing of women's voices, and the denial of equal access to ICT and equal participation in education, employment, social interaction, culture, politics and the economy. This has the effect of reducing women to second-class citizens. Unless safeguards are strengthened, women risk falling farther behind in the global digital revolution.

RECOMMENDATIONS

Due diligence and a human rights approach

It is incumbent on States and ICT intermediaries to jointly collaborate to eliminate ICT VAWG, to respond to reports of violence and harassment effectively, and to predict and prevent violence from happening. Inaction or "remaining neutral" in the face of violence is not an option. States and ICT intermediaries must ensure that women are able to equally access ICT and use technology to promote their empowerment and exercise their right to freedom of expression, without fear of harassment and violence.

States are obligated, both under human rights principles and their respective national constitutions, to protect people from harm. Laws, policies and regulations must comply with human rights and constitutional norms and standards. After all, despite the sovereignty of States to promulgate laws within their territorial jurisdiction, they are guided and bound by international norms stipulated in customary international laws and treaties they have ratified.

Likewise, ICT intermediaries are obligated to protect people from harm arising from their operations. This requires removing or at least reducing the toxicity associated with Internet presence and use, noting the gendered differences in online safety.

The role of preventive measures

Both States and ICT intermediaries should commit to eradicating online gender-based violence. This starts with allocating resources for information and behaviour change campaigns on preventing ICT VAWG, including though collaboration with CSOs.[152]

Preventive measures must address Internet norms and behaviour. At the same time, while the promotion of digital security and safe attitudes online plays a huge role in prevention, there is a critical need to address misogyny, hate and the toxic use of digital media. Prevention strategies must aim to change mindsets and modify behaviours both online and offline. This requires reaching out not only to women and girls but to all digital media users, including boys and men, to alter online behaviour, the Internet culture and harmful notions of masculinity.

152 For example, Facebook launched #HerVoice, a safety policy training programme for CSOs and policymakers on building strong social media campaigns to help address online harassment of women.

For ICT intermediaries, prevention measures can include simple pop-up reminders and warnings for users not to upload ICT VAWG materials.[153]

States, ICT intermediaries and CSOs can develop a counternarrative contesting gender-based hate speech. This can include providing guidance for safe bystander interventions and anti-VAWG narratives. The latter should not only address hate crimes, but also lawful hate speech based on gender.[154] Bystander interventions or collective action can be harnessed online to empower victims/survivors to "fight back" and create communities of resistance.

Engage more women at all levels

Eliminating ICT VAWG requires political will, expertise and collaboration among Internet intermediaries, technology communities, civil society and constituents. New measures must be developed within the framework of human rights and democratic institutions as well as in consultation with key stakeholders, namely civil society (including academia) and the technical community.[155] Women must be engaged at all levels, from conceptualization to implementation, to ensure that policies, laws and other interventions fulfil women's needs and expectations for VAWG-free ICT.

Diversifying the technical community and technology industry by increasing women's involvement and participation is necessary to sensitize the industry to women's needs and perspectives.

The need for a survivor-centred approach

Laws and legal recourse must be accessible and responsive to victims/survivors. States and ICT intermediaries must train law enforcement and grievance officers to discern the nature of ICT VAWG and its constituent elements, to adopt a victim/survivor-centred approach and to respect women's sexual autonomy.

A survivor-centred approach to women's access to justice along with gender-responsive laws and policies will foster confidence in the legal process and effective enforcement of the law. Such an approach evolves around ease of reporting, the treatment of victims/survivors, the familiarity and technical know-how of first responders and those conducting investigations, suitable charges (for example, against invasion of privacy and not merely under obscenity laws), and the protection of victims/survivors from reprisals.[156]

Victims/survivors need a holistic approach that includes passing and implementing laws to protect women and girls, a boost in the prosecution of offenders, and comprehensive services accessible to all women who experience violence. The last include medical support, counselling, safety planning and legal advice, similar to what is provided for offline VAWG.

153 This is similar to the pop-up warning not to upload materials that violate copyrights.

154 See, for example, the Norwegian Ministry of Children and Equality, *The Government's strategy against hate speech 2016-2020*, https://www.regjeringen.no/contentassets/72293ca5195642249029bf6905ff08be/hatefulleytringer_eng_uu.pdf.

155 Technical community refers to experts or specialists in electronics/computing or knowledge and skills related to ICT.

156 See UN Women, UNODC and UNDP, 2017, "The trial of rape: Understanding the criminal justice system response to sexual violence in Thailand and Viet Nam," https://asiapacific.unwomen.org/en/digital-library/publications/2017/09/the-trial-of-rape.

Furthermore, strengthening specialized, clear, and efficient internal and external protocols and codes of conduct for law enforcement officials addressing ICT VAWG is particularly critical during the Covid-19 pandemic given the increased risk of ICT VAWG.[157]

Laws and services to respond to and prevent ICT VAWG would benefit from taking a "human-centred design" approach that revolves around the victim/survivor, and integrating the views, needs and recommendations of survivors into new measures.

ICT intermediary user rules and grievance procedures

ICT intermediary user and community rules should be available in local languages, user-friendly and easy to find.[158] They should be expressed succinctly to draw attention to the more important terms of service and provide a quick understanding of the limits of acceptable online behaviour.

ICT intermediary mechanisms to address ICT VAWG need to incorporate human rights safeguards, and be streamlined and transparent.[159] People in charge of reviewing complaints should be sensitized to gender and trained on ICT VAWG and its implications and impacts on victims/survivors, and on women in general. Sanctions against ICT VAWG (e.g., apologies, and suspension and banning from the platform) must reflect the harm and gravity of the violence. Constant monitoring is required to ensure that those who are suspended or banned have not created alternative accounts or profiles.

Collecting and publicizing gender-disaggregated data on ICT VAWG occurring on platforms, sites and networks can assist intermediaries, users, States and advocates to monitor, evaluate and streamline responses.

Coordination among ICT intermediaries to stop ICT VAWG

Apart from strengthening reporting mechanisms, ICT intermediaries should ensure that their platforms are violence-free by employing reasonable measures to identify and delete ICT VAWG content. Many intermediaries are now famous – and wealthy – for highly innovative online solutions. These same approaches can be harnessed to stop violence and create safe online experiences for women and girls.

ICT intermediaries have already taken initial steps to collaborate with civil society organizations and advocates. The next step is to explore ways in which intermediaries may alert each other of ICT VAWG content, and collaborate to quickly remove it as it travels across platforms and networks. Simple protocols such as watermarking videos originating from their platforms may help in quickly identifying the source. This in turn may assist secondary platforms in taking down the material without violating community guidelines.

Self-regulation by ICT intermediaries is critical, but they should also be regulated by common standards and norms that cover all forms of ICT VAWG. Due to the different laws and social norms of each country, this may be best achieved through an intergovernmental, organizational framework agreed by States and ICT intermediaries.

A clear definition of ICT VAWG

States, ICT intermediaries and civil society need clarity on what constitutes ICT VAWG. This requires a robust definition that reflects the gravity and impact of the issue, which must be deemed a crime, recognizing the grievous physical, sexual, economic and psychological harm it can cause.

It is also time to rethink notions of *consent* and *images*, not only in terms of copyright ownership, but a different kind of ownership that belongs to the subjects of images. This is required to create a paradigm shift where human subjects are not treated as objects without rights.

157 See https://www.unwomen.org/-/media/headquarters/attachments/sections/library/publications/2020/brief-online-and-ict-facilitated-violence-against-women-and-girls-during-covid-19-en.pdf?la=en&vs=2519.

158 Šimonović, Report of the Special Rapporteur.

159 Ibid.

Specialized mechanisms and processes

Specific legal provisions are required to address gender-based offences,[160] including specialized courts and gender-sensitized investigators.[161] The same is true for addressing and responding to ICT VAWG, including secondary perpetration.

States need to ensure response mechanisms stop ICT VAWG by expanding sanctions against perpetrators (e.g., apologies, or ordering perpetrators to remove violent content) as well as reparations for victims/survivors such as restitution, compensation and ways to assist victims/survivors to rebuild their lives and online presence. This will increase women's confidence in coming forward with complaints.

Further interaction among States, ICT intermediaries and other structures

In an age of globalization and digitalization, international and cross-boundary collaboration is fundamental in combatting crimes with international implications.

The elimination of ICT VAWG will depend on effective interactions among States, ICT intermediaries and any other structures that can play a role in stopping violence against women, such as schools, workplaces and the media. States should clearly set out the expectation that all business enterprises in their territory and/or jurisdiction respect human rights throughout their operations. To this end, States should "provide effective guidance to business enterprises on how to respect human rights throughout their operations", and encourage or require business enterprises to address their impact on human rights.[162]

160 For example, domestic violence legislation.

161 For example, Pakistan has established specialized gender-based courts with specially trained judges and prosecutors and plans to set up these courts in all 116 districts. *See* Abdul Qayyum Siddiqui, 2019, "Judicial policy committee directs separate courts be made for gender-based violence cases," GEO TV, 10 October, https://www.geo.tv/latest/250666-judicial-policy-committee-directs-separate-courts-be-made-for-gender-based-violence-cases.

162 Ruggie, Report of the Special Representative.

The implementation of an international framework

A logical next step would be to establish universal norms and standards on ICT VAWG for ICT intermediaries to adopt as part of their obligations to protect and fulfil human rights. This could help reduce the structural discrimination, violence and inequalities that women face, and might enable an online culture free of violence.[163] It could guide ICT intermediaries in navigating complicated but complementary rights that need to be protected online.

A universal definition of ICT VAWG would refer to whether an act is welcome or unwelcome, consensual or non-consensual, and would facilitate a standard response from ICT intermediaries.[164] For this to happen, intermediaries must collaborate with each other, with the assistance of experts and intergovernmental organizations, to develop such a definition. This could potentially facilitate speedier action in preventing, responding to and handling complaints of ICT VAWG.

ACTION POINTS

For States

- Address underlying causes of ICT VAWG (e.g., gender inequality, misogyny and negative perceptions of women) through innovative means to change behaviour, and communicate that VAWG is never acceptable or excusable in any circumstance.
- Develop measures to address and prevent ICT VAWG that are informed by the experiences and perceptions of women and girls, including survivors of ICT VAWG.
- Implement prevention strategies that promote gender-equal, non-toxic, non-violent online etiquette and behaviour as well as online safety and digital security.

163 Šimonović, Report of the Special Rapporteur.

164 Some ICT intermediaries already place their watermark on images uploaded onto their platforms.

- Develop and disseminate counternarratives to push back against cyberattacks and hate speech based on gender.
- Initiate dynamic and engaging behaviour-shaping, education and awareness programmes on ICT VAWG directed at youth.
- Legislate to prohibit all forms of ICT VAWG, specifically non-consensual dissemination of intimate images, sextortion, morphing, trolling, doxing and live-streaming of sexual abuse content/material, with a view to promoting women's equal access to ICT without fear of harassment and violence. Such legislation should consider the specificity of ICT VAWG, including:
  - » The harm caused by ICT VAWG, which, even if not physical, can be traumatic;
  - » The aggregated harm caused by the wide and rapid dissemination of ICT VAWG across multiple platforms and networks;
  - » The difficulty of removing ICT VAWG content from the digital space once it has been disseminated;
  - » The accountability of bystanders (secondary perpetrators) who view and re-transmit ICT content, ignorant of the fact that the content is violent or was disseminated without the consent of the subject, resulting in the perpetuation of ICT VAWG; and
  - » The violation of the rights of victims/survivors, e.g., emphasizing whether an act is welcome or unwelcome, consensual or non-consensual.
- Invest in continuous and ongoing training for specialized law enforcement, prosecutors and judges on the specificities of ICT VAWG, its dissemination and impacts on victims/survivors.
- Ensure that all legislation, policies and trainings on ICT VAWG adopt human rights and gender-sensitized perspectives.
- Ensure that legislation prohibiting ICT VAWG respects freedom of expression, and complies with human rights and constitutional norms.
- Establish reporting protocols that are easily accessible, widely publicized and transparent.
- Provide access to interim court restraining orders to compel alleged perpetrators to delete and stop committing ICT VAWG against the complainant.
- Provide interim remedies to block access to ICT VAWG.[165]

165 Blocking is a measure that is within a respective government's control. On the downside, it only blocks access to the ICT VAWG content within the country.

- Expand sanctions beyond incarceration and fines, including through orders for perpetrators to remove violent content (or engaging professionals to do it), restitution, apology or retraction, and compensation.
- Establish intergovernmental networks and collaboration to address cross-border ICT VAWG.
- Liaise with ICT intermediaries on preventing and addressing ICT VAWG.
- Establish a multistakeholder consultative body of government agencies, civil society, the tech community and academics to develop good practices on preventing, responding to and eliminating ICT VAWG.
- Work towards a shared definition of ICT VAWG in partnership with other States, intergovernmental organizations and civil society.
- Provide comprehensive services for victims/survivors of ICT VAWG, such as psychosocial support, community intervention as well as safety planning.
- Provide effective guidance to ICT intermediaries on how to respect human rights throughout their operations, namely through the application of the Ruggie Principles in the "Protect, Respect and Remedy" Framework.
- Collect gender-disaggregated data on ICT VAWG.
- Monitor and evaluate ICT VAWG policies, laws and strategies as well as their implementation, and initiate modification/reform to accelerate progress where required.

For ICT intermediaries

- Respect human rights and make a public commitment to end ICT VAWG.
- Develop a clear definition of ICT VAWG from a human rights perspective that corresponds to manifestations of ICT VAWG in each country.
- Work to reduce the toxicity and violence associated with an Internet/digital presence and use, change the ICT VAWG narrative, address its underlying causes and perpetuate a healthy online culture.
- Take all reasonable measures to identify, prevent and respond to ICT VAWG, including in local languages and scripts, and considering nuances in local context.
- Train tech personnel and artificial intelligence developers on human rights and gender perspectives related to ICT VAWG.
- Implement pop-up reminders on the prohibition of ICT VAWG before users upload images, e.g., the non-consensual dissemination of intimate images, cyberflashing or morphing.
- Make user and community rules succinct, easy to find and understand, and available in local languages.
- Provide users with a quick understanding of ICT VAWG and the limits of acceptable online behaviour.
- Educate users on online safety and digital security.
- Work with victims/survivors to detect, delete and remove ICT VAWG content, such as rape and death threats, and unwanted images.
- Establish collaborative partnerships with governments and CSOs to prevent and respond to ICT VAWG.
- Establish multistakeholder, gender-sensitized consultations with civil society, the tech community and academics to develop good practices on preventing, responding to and eliminating ICT VAWG.
- Diversify the technical community and technology industry by increasing women's involvement and participation.
- Establish accessible complaint and reporting mechanisms with a process for appeals.
- Allow complaints on ICT VAWG from accounts other than the affected ones (for victims/survivors who have terminated their accounts).
- Incorporate human rights safeguards in redress mechanisms, and make them easy to find, transparent and available in local languages.

- Train persons in charge of reviewing complaints on gender, human rights and a victim-centred approach.
- Collect and publicize gender-disaggregated data on ICT VAWG.
- Monitor and evaluate grievance mechanisms and other ICT VAWG measures periodically.
- Provide victims/survivors with assistance in rebuilding their online presence.
- Adopt protocols such as watermarking to allow the identification of the source of ICT VAWG material.
- Establish cross-industry collaboration to remove ICT VAWG content from all platforms and networks.
- Invest in and collaborate with feminist CSOs, the tech community and academics to develop short, medium and long-term solutions to eliminate ICT VAWG.

UN Women
Regional Office for Asia and the Pacific
5/F, United Nations Building
Rajadamnern Nok Avenue
Bangkok 10200
asiapacific.unwomen.org
@unwomenasia