



ELIMINATING ONLINE VIOLENCE AGAINST WOMEN AND ENGENDERING DIGITAL EQUALITY

Submission by the Due Diligence Project to
the Office of the High Commissioner for Human Rights
Pursuant to Human Rights Council Resolution 32/13 on
Ways to Bridge the Gender Digital Divide
from a Human Rights Perspective

ELIMINATING ONLINE VIOLENCE AGAINST WOMEN AND ENGENDERING DIGITAL EQUALITY

Zarizana Abdul Aziz
Due Diligence Project

The Due Diligence Project welcomes the opportunity to contribute to the report by the Office of the High Commissioner for Human Rights (OHCHR) on ways to bridge the gender digital divide from a human rights perspective. This submission is focused on eliminating online violence and engendering digital equality.

Introduction

The due diligence principle obligates States to take reasonable action to address and eliminate violence against women, whether committed by the State or non-State actors. The Due Diligence Project looked at State compliance in five areas, namely **p**revention, **p**rotection, **p**rosecution, **p**unishment and **p**rovision of redress and reparation (5Ps) and developed a Due Diligence Framework on State Accountability to Eliminate Violence against Women.

Increased prevalence of online violence against women, the lack of effective measures to prevent and contain it, and the ensuing impunity must be addressed as part of the struggle to eliminate all forms of gender-based violence. Since 2015, the Due Diligence Project has been working on developing a Due Diligence Framework on eliminating online violence, looking at the responsibilities of both the State and internet intermediaries.

Information and communications technology is no longer the privilege of select members of society but in many instances has overtaken more conventional forms of communications to become the main form of communication in commercial dealings, personal, political and social interaction.

The Sustainable Development Goals recognize that “gender equality is not only a fundamental human right, but a necessary foundation for a peaceful, prosperous and sustainable world. Providing women and girls with equal access to education, health care, decent work, and representation in political and economic decision-making processes will fuel sustainable economies and benefit societies and humanity at large”.¹ Violence against women, offline and online, must be acknowledged as a manifestation of systemic marginalization of women throughout society. Enhancing “the use of enabling technology, in particular information and communications technology,² to promote the empowerment of women” requires the elimination of online violence against women.

Removing violence against women from the digital and online platforms has the net effect of promoting and strengthening freedom of expression as it creates an environment that allows more individuals, especially sections of society who face most discrimination in other public spaces, to participate in these media.³

¹ <http://www.un.org/sustainabledevelopment/sustainable-development-goals/>

² Goal 5 target, Sustainable Development Goals, <http://www.un.org/sustainabledevelopment/gender-equality/>

³ A 2015 report on the status of freedom of expression in Norway cites the Norwegian survey on the status of freedom of speech from 2014 that “shows that hate speech can have harmful effects for those who participate in public debate. In the survey, it emerges that the harm is greater among people with ethnic minority backgrounds than those with majority background,” it further notes that there is no reason to assume that the same harmful effects don’t also apply to other groups who are particularly vulnerable to hate speech related to actual or perceived personal characteristics.” The report also documents that such speech intimidates people and deters them from speaking publicly. See Equality and Anti-Discrimination Ombud’s Report (2015). Hate speech and hate crime. Available online: http://www.genderit.org/sites/default/upload/hate_speech_and_hate_crime_v3_lr.pdf.

This submission outlines the framework on State and internet intermediaries obligation to eliminate online violence against women which was developed pursuant to the Expert Group Meeting on Due Diligence and Accountability for Online Violence against Women in October 2015.⁴

State and Internet Intermediaries Obligation to Eliminate Online Violence against Women

1. Freedom of Expression and Online Violence against women

Principle: It is not an exercise of freedom of expression to consciously intimidate women online, express the wish to rape them, threaten to harm them or incite others to do so.

Human rights are universal, inalienable, inter-related, inter-dependent and indivisible. An individual's human rights are not absolute in that it cannot be enjoyed at the expense of the human rights of others. Freedom from gender-based violence against women, freedom of expression and rights to privacy are protected by international human rights law.

The exercise of these rights under international human rights law is not absolute and may be subject to certain restrictions, but these shall only be such as are provided by law and are necessary for respect of the rights of others; and for the protection of national security or of public order. The application of these restrictions by States however, "may not put in jeopardy the right itself".⁵

This is different from freedom of opinion. The right to hold opinions without interference is an absolute right and "permits no exception or restriction".⁶ However, the expression of an opinion, that is the right to freedom of expression bears "special duties and responsibilities". The free exchange of and access to information does not equate to unregulated violence. Freedom of expression or access to information cannot be bought at the expense of women's security and safety.

2. Definition: Violence against women

Principle: Violence against women as a legal concept has been extensively interpreted and its definition can be found in various international human rights instruments. Actionable online gender-based violence (including threats of violence) is gauged by intent to harm, content, credibility or imminence of harm and context.

- (a) While states do not have the obligation to protect individuals from offense, it does have the obligation to protect individuals from harm. Non-physical gender-based violence can approximate and sometimes exceed the harm of physical violence.
- (b) Violence against women has been rigorously defined in several international instruments. The 1993 UN Declaration on the Elimination of Violence against Women defines 'violence against women' as an act of gender-related 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, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life.⁷

⁴ The Expert Group Meeting was convened by the Due Diligence Project jointly with the Association for Progressive Communications and hosted by the Robert F Kennedy (RFK) Center for Justice and Human Rights. The principles have also been enriched by comments and inputs from international and regional experts and civil society.

⁵ UN Doc. CCPR/C/GC/34, Human Rights Committee, General Comment 34 on Article 19 of the ICCPR, Freedoms of opinion and expression, adopted at the 102nd session, 12/9/11, para 21.

⁶ UN Doc. CCPR/C/GC/34, Human Rights Committee, General Comment 34 on Article 19 of the ICCPR, Freedoms of opinion and expression, adopted at the 102nd session, 12/9/11, para. 9.

⁷ Violence against women has been defined and elaborated in many human rights and feminist instruments and discourse 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.

- (c) Online violence against women are acts 'committed, abetted or aggravated' in part or fully by the use of information and communication technology (ICT) acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communication technologies⁸
- (d) Gender-based hate speech (advocacy of gender-based hatred that constitutes incitement to discrimination, harm, hostility or violence) should be prohibited.⁹ Incitement to harm comprises of both incitement against a group and incitement against an individual.
- (e) Even where perpetrators are held liable, further reflection is needed on how to hold re-transmitters responsible for the re-transmission of violating materials. Intent, or more specifically, lack of intent, can arguably be an issue with secondary transmitters. Still, holding persons accountable despite lack of intent is not without basis under the law. In many jurisdictions, criminal law has developed the concept of reckless indifference and the civil (non-criminal) law, the concept of negligence where intent cannot be established.

3. Consent and privacy

Principle: Consent is pivotal in online gender-based violence and key in differentiating lawful behaviour from unlawful and harmful behaviour. It is the pillar around which preventive measures and post-incident responses are implemented and must be addressed in any mechanism dealing with online violence.

Consent is important in gauging whether there has been violation of privacy with regards to dissemination of private data. Consent that is specific to an individual cannot be expanded to consent for the data to be shared and disseminated. Protection of women's agency is intrinsically linked to the rights to give informed consent on what and with whom material can be shared.

In the digitalized world of big data, what is personal and public data is blurred. Our personal data is continuously being handled and commoditized.¹⁰ Such personal data however, is no less personal for the fact that it may be available in the public domain. Consent for its dissemination is crucial in determining whether a violation of privacy has been committed.

4. Human Rights Approach

Principle: The State has an obligation under international human rights law to eliminate violence against women, both online and offline and to promote, protect and fulfill human rights. Business enterprises, including internet intermediaries should respect and protect human rights, and remedy adverse human rights impacts in which they are involved.

Eliminating online violence requires States fulfilling their obligation to promote, protect and fulfill human rights, in collaboration with and with the intercession of internet intermediaries, particularly transnational corporations serving the role of internet intermediaries.

Eliminating online violence ensures that the internet remains a platform for everyone to exercise their rights to freedom of opinion and expression. Measures to eliminate online gender-based violence

⁸ Association for Progressive Communications (APC) (2 March 2015). From Impunity to Justice: Domestic legal remedies for cases of technology-related violence against women . Available online: http://www.genderit.org/sites/default/upload/flow_domestic_legal_remedies.pdf. [Accessed 2 February 2016].

⁹ Currently Rabat Plan of Action prohibits advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence. Gender-based hatred should be similarly prohibited. http://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf (last visited ** 2016)

¹⁰ Personal data means any information relating to an identified or identifiable individual; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number (e.g. social security number) or one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity (e.g. name and first name, date of birth, biometrics data, fingerprints, DNA...)

should respect freedom of expression and be limited to what is necessary and proportionate to address online violence against women.

It is thus crucial to look at responses of different actors, particularly, the identification and role of first responders (including the police, internet intermediaries and helplines), regulators and the judiciary to map the reality of women's experiences and facilitate women's access justice/remedies.

States should also set out clearly the expectation that all business enterprises domiciled in their territory and/or jurisdiction protect, respect and remedy human rights throughout their operations.¹¹ Internet intermediaries should also ensure that their platforms are not abused to perpetrate and perpetuate violence against women, and if they are, take immediate action to remedy it.¹²

5. *Independent regulating mechanism*

Principle: The State is responsible to set up an independent entity that is authorized to hear and decide on cases involving online violence against women and issue effective remedies for the victim/survivor.

The regulatory framework must address the role and responsibility/liability of the primary perpetrators, secondary perpetrators (re-transmitters) and internet intermediaries. It must also include provision for the possibility of ordering the internet service provider to divulge the information required to identify the perpetrator where circumstances warrant it, injunction or injunction-like orders, take down or de-linked from the result of searches orders. An independent monitoring entity should not serve to authorize itself. Neither should it be used as a form of surveillance in violation of human rights. Ensuring timeliness, affordability and responsiveness would facilitate women's access to these mechanisms.

The State has a positive role in creating an enabling environment for freedom of expression and equality, while recognising that this brings potential for abuse. At the same time, State regulation must be conscious of not violating freedom of expression yet at the same time, prioritize women's access to online technology in a safe environment where perpetrators of online violence do not enjoy impunity. Strong democratic structures — including free and fair elections, an independent judiciary and a vibrant civil society — are needed to prevent abuse and to realise more fully the goals of pluralism and equitable access.¹³ States must also include women's rights organizations in development of the regulations, and adopt a human rights' approach.

6. *Duties and responsibilities of information communication technology intermediaries*

Principle: Self-regulation, where effective, remains the most appropriate way to address professional issues relating to internet and digital intermediaries. Reporting procedure and mechanisms, as well as remedies must be accessible and transparent.

Victims/survivors of violence require that the violence cease; yet postings on the internet not only maintains a certain level of permanence, it can continually be searched, accessed and

¹¹ John Ruggie, Guiding Principles on Business and Human Rights: Implementing the United Nations "Respect, Protect and Remedy Framework," UN Human Rights Office of the High Commissioner (2011). The Guiding Principles were proposed to the United Nations Human Rights Council as part of the 2011 report to the Council by then-UN Special Representative on business & human rights, John Ruggie: Report of the Special Representative of the Secretary-General on the Issue of Human Rights and Transnational Corporations and Other Business Enterprises, John Ruggie, UN Doc. A/HRC/17/31, 21 Mar. 2011. Available at http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf. See also Guidelines for Multinational Enterprises of the Organisation for Economic Co-operation and Development.

¹² *Ibid.*

¹³ See for example, Article XIX, Camden principles on Freedom of Expression and Equality, available at <https://www.article19.org/data/files/pdfs/standards/the-camden-principles-on-freedom-of-expression-and-equality.pdf> (accessed 24 July 2016)

disseminated. Cessation of online violence and restoration of privacy can only be provided by internet intermediaries and platform providers.

Reversing the notion that human rights are the product of the social contract between the State and the individual allows us to presume that human rights are entitlements enjoyed by everyone to be respected by everyone.¹⁴ The net result being States, corporations and individuals all have human rights obligations. The obligation exists irrespective of whether they are enforceable.

Internet intermediaries' duty however, is not on all fours with the duty borne by the States. Intermediaries for example do not owe the obligation to prevent violence wherever it may occur but only violence occurring on their platforms.¹⁵ This may also better accord with the Ruggie principles of not "infringing on the human rights of others" and "addressing adverse human rights impacts with which they are involved".

Intermediaries should seek to empower users to work through hotlines, awareness raising and education. Complaints and remedies should be archived. Intermediary corporations must recognize violence against women as unlawful behaviour, and demonstrate increased and expedited cooperation in providing relief to victim/survivors within the corporations' capacities, for example, as systems for cooperating with law enforcement, takedown (including system-wide removal of content, where possible), or de-linking from the result of searches procedures for abusive and harmful content and the possibility of account termination for misconduct. In this regard, the intermediaries' reporting procedure and mechanisms, as well as remedies must be accessible and transparent. Exercising due diligence includes setting out circumstances under which intermediaries are deemed to have had notice of such violence.

Where voluntary self-regulation by intermediaries fails to deliver the remedies needed, States need to establish independent judicial or quasi-judicial mechanisms to assist victims/survivors in obtaining these remedies.

7. *Due Diligence*

Principle: States and internet intermediaries should exercise due diligence to eliminate online gender-based violence. This extends to reasonable measures to prevent violence before they occur, and effectively investigate and take action against perpetrators once they occur as well as provide redress and reparation to victims/survivors.

Though this principle evolved to focus principally on State obligations, the principle is also useful in guiding internet intermediaries in developing and implementing policies to end violence against women on their platforms. The five areas where states and internet intermediaries need to exercise due diligence are –

(a) Prevention

Prevention includes measures to thwart the occurrence of violence against women. Good prevention programmes provide awareness of online violence against women and of information services and legal protection available post the incident. States and internet intermediaries should deem online violence not merely as another form of violence but violence that is grounded in discrimination and prevents women from exercising their freedom of

¹⁴ Andrew Clapham, *Human Rights Obligations of Non-State Actors*, Academy of European Law, European University Institute, Oxford University Press, 2006. Also available at http://graduateinstitute.ch/files/live/sites/iheid/files/sites/international_law/shared/international_law/Prof_Clapham_website/docs/HR%20obligations%20of%20non-State%20actors.pdf (Last accessed 6 July 2015)

¹⁵ Comparison can be drawn from imagining a person drowning. Generally an individual does not owe a duty, even if he is an excellent swimmer, to attempt to save a drowning person. However, the pool owner who obtains economic benefit from the use of the pool by others, owes a duty to ensure that there are sufficient safeguards to prevent death or drowning in his pool.

expression and access to technology and internet spaces and develop preventive policies accordingly.

(b) Protection

Protection focuses on avoiding the recurrence of further violence (which should be immediate if the perpetrator can be identified) the provision of accessible services, and adequate training and sensitization of first responders.

As information and communication technology allows for the easy and rapid dissemination of information and content, the harm of online violence can be quickly amplified. The obligation to protect does not merely refer to the treatment of the original material, but the uploading and dissemination of that material which constitutes recurrence of the violence. Protection from further violence requires not only immediate action on the part of States and internet intermediaries; it sometimes necessitates extra-territorial reach.

(c) Prosecution

Prosecution refers to investigation and instituting proceedings against the perpetrators. Where internet intermediaries are concerned, such proceedings may consist of inquiries. Given the speed and breadth of dissemination of data and material online, States and internet intermediaries must take prompt effective action upon having notice of the perpetration of the act of violence.

(d) Punishment

Punishment refers to the obligation to impose sanctions/negative consequences on perpetrators. The certainty of adequate punishment creates a level of predictability and sends a message that online violence against women will not be tolerated.

(e) Provision of redress and reparation

Generally, reparations and restitution to victims of violence include compensation for the costs of quantifiable losses (cost of medical care, loss of wages, and damage to property), injuries and non-quantifiable losses and for the needs of the victims/survivors of violence to re-build their lives in the short, medium and long terms, as they transition from a violent situation to a life free from violence are granted as civil remedies. For online violence, remedies must include the ability of victims/survivors to have content removed (where possible) or delinked from the results of searches.

Conclusion

The free exchange of and access to information does not equate to unregulated violence. Although access to the internet and other digital spaces is most often facilitated by private entities, it is crucial to regard this space not as private spaces but public spaces, albeit ones controlled by private entities. After all, some of these spaces are accessed by millions of users.

Admittedly, intermediaries are not responsible nor can they be made liable for the initial act of violence, namely that of posting the violating material online. However, the continued accessibility or dissemination of these materials means that the victim/survivor is continually subjected to violence.

Specific laws on online violence as well as specialized mechanisms with trained and skilled personnel is required to confront and eliminate online violence. Merely criminalizing online violence does not necessarily provide the remedy required by online violence victims/survivors. Experience has shown that women's access to justice should be a mix of criminal, civil and administrative processes and include the areas of all the 5Ps, namely in prevention of online violence; protection of victims/survivors; prosecution and punishment of perpetrators and provision of redress and reparation for the victims/survivors.