



Wilson  
Center



November 2022

### Author

**Jamila Venturini,**

is one of the Executive Directors of Derechos Digitales, a Latin American-based non-profit organization which defends and promotes human rights in digital environments since 2005. Jamila is a journalist and researcher in social sciences. She is the author of books and papers on technology and human rights; and a member of the Latin American Network of Surveillance, Technology and Society Studies (Lavits).

This paper was written with guidance and support from UNFPA and the Wilson Center.



## Policies for tackling tech-facilitated gender-based violence: multi-stakeholder perspectives and learnings from around the world

**Overview:** This is a brief summary and analysis of a series of papers developed by different stakeholders around policy proposals, initiatives and analysis for responding to tech-facilitated gender based violence (TF GBV) to inspire discussions at the Global Symposium on Technology-facilitated Gender-based Violence.

Photo: © UNFPA



## Case Studies of Nepal, Pakistan and African Countries

Two of the background papers analyze existing legislation from Global South countries to respond to TF GBV and their limits. Kayastha and Baramu, from Body & Data, analyze the case of Nepal in: [“Mapping Laws relevant to online violence in Nepal: A study.”](#)<sup>1</sup> The authors start by presenting data on the prevalence of the experience of physical and sexual violence of women in Nepal, as well as information on structural inequalities that exclude them from decision-making and the broader public life.

The authors identified legislation that could be used to prevent and respond to TF GBV, but warn of the underlying value system behind them. That is, “generally the court punished perpetrators not for violating women’s right to privacy or self-autonomy, but for violating a patriarchal notion of ‘honor’ as prescribed by society, which even the court associates with women’s bodies and sexuality.” They also identified that “women are seen as ‘victims’ whose value and dignity need protection from the law.” Such conclusions on how State authorities perceive gender violence could be shared with other countries and represents a broader issue of the design, development and implementation of laws and policies addressing violence against women and girls.

The authors also explore the threat that some of the concepts included in the existing legislation (such as “public morality”; “social harmony”; “hate and jealousy” and “obscenity”) are weaponized to criminalize legitimate expression, particularly by women and LGBTQIA+ people. This is complemented by a ban on pornography which creates a legal mechanism to restrict sexual expression, regardless of consent. They identified cases of activists and journalists who were arrested for “disturbing public moralities” and “cybercrime” after posting criticism against State authorities in their social media.

“Such curtailments are often justified on the basis of protecting an individual’s reputation, national security or countering terrorism, safeguarding women and minorities from violence, but in reality are used to censor content that the government and other powerful entities do not like or agree with.” As such, the authors warn against legislating against privacy, security and encryption, a principle which is highlighted again below in the work of Access Now.

The moral policing of gendered expression was also documented by the Digital Rights Foundation in Pakistan, where “concepts such as honor, decency and shame are used as tools for censorship, surveillance and control to morally police individuals into abiding by the dominant standards of society.” According to the study [“Moral Policing and the Phenomena of ‘Raids’ in Online Spaces”](#)<sup>2</sup>, violence, harassment and abuse against women are not exclusive to online environments, although “the rise of the internet and social media is also tied to the escalation of moral policing cases.” Such types of attacks are experienced by women internet users, sometimes in a coordinated format as “raids” against prominent female opinion leaders.

In Pakistan, morality is presented as a legitimate restriction to the rights of freedom of association, speech and religion by the Constitution. Several criminal offenses derive from societal conceptualizations of decency, morality and obscenity. These arguments are also relied upon to authorize the blocking of websites and online applications. For instance, they were used to block dating apps in 2020, TikTok in 2020 and 2021. In 2016, the government had already blocked a list of over 400,000 websites under allegations of pornography and obscenity, including online shopping, Disney cartoon’s websites, and Tumblr.



Photo: © Luca Zordan for UNFPA

The Body & Data study concludes that Nepal has a legal framework capable of addressing several forms of TF GBV and there is no need to formulate new laws but rather to reform the existing policies to remove ambiguity and the criminalization of expression. They warn of the need for an intersectional approach given that “legal protection that doesn’t take into account caste, class, sexuality, gender, religion and other factors will always fall short of delivering justice to communities facing these intersections”

The analysis also sheds light on other measures required to ensure an effective response to TF GBV. These include the need for sensitizing police and judicial authorities on the emotional and psychological harm to victims as well as a need to strengthen mechanisms by State and non-State actors to support victims by providing, for example, shelter for physical safety (regardless of the digital or online nature of the offending), legal counseling and assistance to ensure digital safety and security.

A similar situation is observed in African countries by Pollicy’s study [“Fighting Violence Against Women Online: A Comparative Analysis of Legal Frameworks In Ethiopia, Kenya, Senegal, South Africa, and Uganda.”](#)<sup>3</sup> Nwaodike and Naidoo reviewed existing legislation in five countries to conclude that the main instruments available for victims of TF GBV

are defamation laws, which are not designed for this purpose. Similar to Kayastha and Baramu, they use a feminist lens to analyze an alleged protection system based upon ideations of honor and reputation: “standards defined in the context of the patriarchal society and standards to which women are often held hostage.” According to Pollicy, these standards force “... women to seek redress by upholding these standards” which further entrenches them within the legal system and society more broadly.

In the African context, the application of legislation enacted to presumably protect vulnerable groups has also been used to silence them. These include hate speech and disinformation laws, as well as cybercrime and criminal defamation norms. Targeted victims usually include journalists and human rights defenders who criticize authorities. Assuming the cost of staying online in harmful digital environments authors recommend the adoption of specific TF GBV laws to remove the burden from women, of defending themselves from violence. Authors recommend the adoption of specific TF GBV laws to remove from women the burden of defending themselves from violence. Such laws should include “appropriate measures to genuinely mitigate the impact of online GBV on their social, economic, political, and emotional lives”



## A Survivor-Centric and Intersectional Approach

Sharma and Kolisetty, in their paper, [“Advancing Survivor-Centric, Intersectional Policy to Tackle Tech-facilitated Gender Based Violence,”](#)<sup>4</sup> develop a framework to guide decision-makers while developing policies to respond to TF GBV. They argue that in order to design legislation that provides survivors with trauma-informed pathways to justice, it is necessary to understand the plurality of survivors’ needs and experiences.

**The framework they designed, through consultation with civil society, is composed of seven principles which include:**

- 1 Equity, as the recognition of the underlying differences among victims and the need to develop policy responses that take into account individuals’ position, identity and skills when proposing access to resources, support and justice;
- 2 Consent, relating to the need of all actors involved in the response to TF GBV so “survivors retain control over their stories” and “each step of the justice-seeking process shapes their sense of self and agency, and helps in healing”;
- 3 Confidentiality, fundamental to avoid stigma resulting from patriarchal norms that blame the victim for sexual violence;
- 4 Accessibility, to allow understanding by linguistically diverse groups and disabled people;
- 5 Intersectionality, referring to harms that manifest differently to people living in multiple sites of oppression, and redress should consider a plurality of approaches;
- 6 Decentralization, to guarantee the participation of people ultimately affected by TF GBV in policy-making; and
- 7 Accountability for those who hold power and perpetuate harm including social media platforms that allow the proliferation of abuse and perpetrators themselves.

The framework relates not only to State legislation, but also to social media policies and reporting mechanisms. The framework includes several examples of good and bad practices in each of the principles.





## Perspectives and policy priorities from Australia

One of the positive examples highlighted in the framework is the Australian Online Safety Act 2021. This is the enabling legislation for the eSafety Commissioner (eSafety), Australia's independent regulator for online safety. eSafety's functions also include providing online safety education and coordination across government, industry and civil society groups in Australia.

eSafety takes a risks- and harms-based approach to its work. Their work is complementary of other institutions in charge of investigating and prosecuting cybercrime. eSafety helps to keep Australians safer online by countering online harms, improving online safety, and exercising regulatory powers under a holistic framework that comprises three pillars:

- (i) prevention, through research, awareness raising programs, evidence-informed resources and education, among other initiatives;
- (ii) protection, through operating regulatory schemes and investigating abuse and online harm, and offering complaint mechanisms to victim-survivors, as well as information about available law enforcement, counseling and legal services, and advice on strategies to mitigate online harm; and
- (iii) proactive and systemic change, through environmental and horizon scanning to identify emerging trends in online harm, supporting industry to develop codes to detect and remove illegal or restricted content, focusing on transparency and accountability, and developing voluntary guidance materials and tools, such as the Safety by Design initiative, among other actions.

Empowered by the Online Safety Act, guided by its priorities, and enabled through domestic and international partners, these interconnected pillars support eSafety to deliver its mission.

In November 2021, eSafety detailed its regulatory priorities in the document "Regulatory Posture and Regulatory Priorities". eSafety explains its goals are to prevent and remedy harm, enhance transparency and accountability, and examine the effectiveness and impact of what online services do to keep their users safer.

eSafety has been focused on operationalizing the enhanced protections of the Online Safety Act 2021 since it came into force in January 2022. (See summary of Online Safety Act changes).

One of the regulatory schemes eSafety operates is an Image-Based Abuse scheme. This involves responding to complaints about the sharing, and threatened sharing, of intimate images, where the person shown has not given consent to have their images shared.

Under the legislation, an intimate image is defined as showing any of these:

- private body parts
- private activity, such as being in a state of undress, using the toilet, showering or bathing, or sexual activity
- a person who normally wears clothes of religious or cultural significance in public without them such as being in a state of undress, using the toilet, showering or bathing, or sexual activity.

An intimate image can be fake or digitally altered. This includes where a person's face is photoshopped onto sexually explicit material and 'deepfake' videos generated by apps that use artificial intelligence to make people appear to do and say things they never did do or say. It also includes where an intimate image is tagged with a person's name, implying that it is an image of that person even if it is not of them.



The Image-Based Abuse scheme is complaints-based. Complaints must be made by either the person depicted in that image or by someone authorized by the depicted person. A complaint can only be made on behalf of another person if they are:

- authorized by the person shown in the intimate image, or
- the parent or guardian of a child less than 16 years of age who is shown in the intimate image, or
- the parent or guardian of the person shown in the intimate image who has a mental or physical condition (whether temporary or permanent) that makes them incapable of managing their affairs.

When a complaint is made on behalf of someone else, eSafety needs to be satisfied that the person making the complaint is authorized to do so. eSafety will work with the person making the complaint and the person shown in the image or video to confirm that the person making the complaint is authorized to do so.

eSafety also works directly with companies to promote the rapid removal of “child sexual exploitation and abuse material, along with other forms of illegal content that cause the most severe harm through their production, distribution and consumption.” They state that “[w]here collaborative efforts are insufficient or inappropriate, we may use the formal options available to us to require removal of material and deter further harm. Formal options range from issuing a Service Provider Notification or Removal Notice through to taking enforcement action such as imposing civil penalties and fines, court-ordered injunctions and legally enforceable undertakings. Enforcement action is more likely in serious matters, for example, where we encounter deliberate non-compliance that creates an ongoing risk of harm.” Service providers have a standard 24-hour time period to comply with removal notices, which eSafety can extend in certain circumstances.

eSafety also aims to identify and promote better solutions to prevent and reduce the types of harm that are most commonly reported to us. This includes exploring technological solutions to scale up assistance and reduce the spread of harmful online content and behavior.

### Summary of Online Safety Act changes

The Online Safety Act expanded and strengthened Australia’s online safety laws, giving eSafety improved powers to help protect all Australians from the most serious forms of online harm. This includes:

- A world-first Adult Cyber Abuse Scheme for Australians 18 years and older, across a wide range of online services and platforms.
- A broader Cyberbullying Scheme for children to capture harms that occur on online services and platforms other than social media.
- An updated Image-Based Abuse Scheme to address the sharing and threatened sharing of intimate images without the consent of the person shown.
- Targeted powers to require internet service providers to block access to material showing abhorrent violent conduct.
- Stronger information-gathering powers.
- A modernized Online Content Scheme to regulate illegal and restricted content no matter where it’s hosted, bringing in app distribution services and search engines.
- New Basic Online Safety Expectations that ensure online service providers take reasonable steps to keep Australians safe online.
- New industry codes requiring online platforms and service providers to detect and remove illegal or restricted content.



## Beyond encryption myths

Automated removal of content, as well as technological intervention into private communications may represent a threat to other human rights, such as privacy, freedom of expression and information –also key to address TF GBV and promote gender equity– and therefore require strict considerations on legality, necessity and proportionality.

On a related topic, Access Now in the document [“10 Facts to Counter Encryption Myths”](#)<sup>7</sup>, responds to arguments often used by governments to justify demands for weakening encrypted communications, including in order to protect vulnerable groups. One of them is that “weakening encryption will not stop criminals and terrorists from using strong encryption”, arguing that this is a disproportionate approach that jeopardizes the privacy and security of all without evidence that it helps to stop attacks.

They also emphasize “strong encryption contributes to children’s safety online”, explaining that as general encryption is weakened, criminals will shift to other platforms where they can better hide their activities and evade investigation. Access Now recalls that privacy is not only part of children’s recognized rights, but also valued as important by over 90% of youth respondents in an UNESCO survey. Respondents also indicated that they “can stay safe online by acquiring the necessary information and technological competencies” – which includes information on how to use encrypted tools to protect their communications.

Other facts included in the document are: strong encryption is essential for internet security; giving law enforcement exceptional access threatens human rights and democracy; strong encryption strengthens both privacy and security; law enforcement has entered the golden age of surveillance — without breaking encryption; mandating “traceability” will risk privacy and chill free expression; strong encryption is crucial for cybersecurity and protects national security; strong encryption maintains trusted in the digital ecosystem and supports economic growth; and that law enforcement and intelligence agencies don’t have to break encryption to investigate crime.



Photo: © UNFPA Egypt



## Private sector responsibilities

Several authors point out the need to embed human rights law into private sector responsibility to address TF GBV, particularly in light of the transnational nature of their operations.

Suzor et al, "[Human rights by design: The responsibilities of social media platforms to address gender-based violence online](#)"<sup>8</sup>, build upon the arguments developed in the past decade regarding the application of the UN Guiding Principles on Business and Human Rights to the internet and telecommunications' sector.

After recognizing the complexity, structural nature and impact of TF GBV within a human rights framework, the authors identify the main actions online intermediaries should develop. These include monitoring impact, mitigating harm through design and developing effective remedies. While recognizing recent advances by major social private actors, the paper identifies their limitations in terms of the way private companies

understand and apply human rights (generally focusing on their response to State abuse rather than on the impacts of their own operation and their content moderation systems), the fact that social media business models may contribute to the exacerbation and spread of abusive content and harassment and finally, that content moderation systems place the burden of reporting on survivors and are ineffective to prevent abuse, while harm becomes normalized on many platforms.

"While most major platforms have clear rules against abusive behavior, these are inconsistently applied and enforced. In order to make meaningful progress on changing user cultures, platforms will need to more systematically respond to abuse and, critically, ensure that these responses are clearly signaled to their users in order to more effectively change the norms of acceptable behavior"; they state, and call for non-legal measures to complement a policy approach, including human rights capacity building.





# Recommendations for Future Discussion

Background papers analyze existing frameworks and propose recommendations to both State and private policies. Some of them bring evidence on the limits of existing policies and criminal responses—in particular to groups who face historic and structural oppression—as well as expose how the Judicial system is often unprepared to assist victims in the search for justice. They also highlight how generic concepts have been used to silence women and vulnerable groups, particularly in Global South countries, and how private companies have also failed to give a satisfactory response to TF GBV.

Several call for an intersectional approach to policy-making and recommend considering the plurality of lived experiences by victims instead of an one-size-fits-all solution. They also call for norms that promote and respect the full spectrum of rights women and LBTQIA+ people have guaranteed; and bring concrete examples of good and bad practices.

In face of such elements, continuing the conversation on policies tackling TF GBV, it is key to advance on concepts that can be operationalized towards a survivor-centric and human rights based approach. There are concrete advances from the UN in identifying the risks TF GBV represent to the exercise of rights by women and LBTQIA+ people. However, it is necessary to continue developing frameworks to guide a proper balance of rights, including the rights to privacy, freedom of expression and access to information which, among others, are central to assist victims of violence.

Alliances with digital rights organizations and experts will be key to advancing this type of framework in a context in which censorship, surveillance and control continue to affect historically marginalized groups, sometimes justified by moral policing.

Thinking on how to advance a coordinated global agenda for tackling TF GBV should also involve recognizing that while some countries have the conditions to develop refined legal and institutional models and are able to influence global internet companies, others struggle to sustain effective judicial and support mechanisms to assist victims. This brings a question on the role of multilateral and multi-stakeholder cooperation, not only in terms of how global standards can take into account the diversity of national contexts and lived experiences, but also on ways to share responsibilities to respond to increasing global inequalities.

Further reflection is also needed on the legal and non-legal mechanisms to foster the private sector in reviewing their own interpretations of human rights, and create effective responses. It is necessary to prioritize multi-stakeholder participation in the development of private policies that impact on fundamental rights. Such participation has to be followed by accountability on how their perspectives and expertise are considered and how policies were changed. Advancing dialogues with actors involved in business responsibility in other sectors can also help to find effective mechanisms in such direction.








## List of Resources

1. Kayastha, S., Baramu, R. (2021). *Mapping Laws Relevant to Online Violence in Nepal: A Study* <https://bodyanddata.org/wp-content/uploads/2021/12/OnlineGBVLawsMapping-min.pdf>
2. Digital Rights Foundation. (2021). *Moral Policing And The Phenomena Of 'RAIDS' In Online Spaces*. <https://digitalrightsfoundation.pk/wp-content/uploads/2021/05/Moral-Policy.pdf>
3. Nwaodike, C., Naidoo, N. (2020). *Fighting Violence Against Women Online: A comparative Analysis of Legal Frameworks In Ethiopia, Kenya, Senegal, South Africa, and Uganda*. [https://www.apc.org/sites/default/files/Legal\\_Analysis\\_FINAL.pdf](https://www.apc.org/sites/default/files/Legal_Analysis_FINAL.pdf)
4. Sharma, C., Kolisetty, A.. *End Cyber Abuse - Advancing Survivor-Centric, Intersectional Policy to Tackle Tech-facilitated Gender Based Violence* <http://endcyberabuse.org/advancing-survivor-centric-intersectional-policy-to-tackle-tech-facilitated-gender-based-violence/>
5. eSafety Commissioner, Australian Government. (2021). *Regulatory Posture and Regulatory Priorities*. <https://www.esafety.gov.au/sites/default/files/2022-03/Regulatory%20Posture%20and%20Regulatory%20Priorities.pdf>
6. eSafety Commissioner, Australian Government. *Online Safety Act 2021 Fact Sheet*. <https://www.esafety.gov.au/sites/default/files/2022-02/OSA%20fact%20sheet%20updated.pdf>
7. Maheshwari, N., (2021). *Facts to Counter Encryption Myths*, Access Now. <https://www.accessnow.org/cms/assets/uploads/2021/08/Encryption-Myths-Facts-Report.pdf>
8. Suzor, N.. (2019). *Human rights by design: The responsibilities of social media platforms to address gender-based violence online*. <https://onlinelibrary.wiley.com/doi/abs/10.1002/poi3.185>

Woodrow Wilson International Center for Scholars  
One Woodrow Wilson Plaza  
1300 Pennsylvania Avenue NW  
Washington, DC 20004-3027



### The Wilson Center

 [www.wilsoncenter.org](http://www.wilsoncenter.org)  
 [wwics@wilsoncenter.org](mailto:wwics@wilsoncenter.org)  
 [facebook.com/woodrowwilsoncenter](https://facebook.com/woodrowwilsoncenter)  
 [@thewilsoncenter](https://twitter.com/thewilsoncenter)  
 202.691.4000



### The United Nations Population Fund

 [www.unfpa.org](http://www.unfpa.org)  
 [EndTFGBV@unfpa.org](mailto:EndTFGBV@unfpa.org)  
 [@unfpa](https://twitter.com/unfpa)