SUBMISSION ON TECHNOLOGY-RELATED AND ONLINE VIOLENCE AGAINST WOMEN

RESURJ – Realizing Sexual and Reproductive Justice

INTRODUCTION

RESURJ[1] is a Global South-led transnational feminist alliance dedicated to upholding and advancing sexual and reproductive justice by engaging strategically with decision-makers globally, regionally and nationally, while mobilizing other young women advocates. We welcome this opportunity to share our input and views on technology-related and online violence against women.

For the purposes of this submission, we are adopting the following definitions.

Violence against women means "any act of gender-based violence that results in, or is likely to result in, physical, sexual or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or in private life." - Article 1 the Declaration on the Elimination of Violence against Women[2]

Technology-related violence against women "encompasses acts of gender-based violence that are committed, abetted or aggravated, in part or fully, by the use of information and communication technologies (ICTs), such as phones, the internet, social media platforms, and email. Technology-related violence against women is part of the same continuum as violence against women offline." Association for Progressive Communications (APC).[3]

Online abuse and gender-based violence is a part of gender-based violence (GBV), where information and communications technologies (ICTs) are used to commit, abet or aggravate GBV. In addition to existing structural inequality and discrimination, disparity in access to, participation in and decision-making over ICTs tend to contribute to online abuse and GBV. - 2015 UN Internet Governance Forum, Best Practice Forum on Countering Online Abuse and Gender-Based

---

[1] http://www.resurj.org/

[2] UNGA (20 December 1993). *Declaration on the Elimination of Violence against Women* (A/RES/48/104). Available online: http://www.un.org/documents/ga/res/48/a48r104.htm

[3] http://www.genderit.org/onlinevaw/

Violence.[4]

In addition to the definitions above, this submission pertains to technology-related and online violence against women in all their **diversity**. We recognize and aim to convey that **non-normative expressions of gender identity including lesbians, bisexual and trans women** disproportionately experience violence online and offline which is seldom addressed by existing legislations related to technology based violence and GBV.

As supported by these definitions, we assert that technology-related and online violence against women in all their diversity does not exist in isolation and is an extension, and often forms an integral part of, the violence experienced by women and girls offline. One differentiation of online behavior could be that most of the time it is by perpetrators not known to the victim (though not always the case), resulting in a sense of anonymity, asynchrony and related impunity experienced by perpetrators. Human rights and related freedoms including women's sexual rights apply in the online world as they do offline and addressing technology-related and online violence against women requires acknowledging and addressing structural inequalities that perpetuate the violence.

Women are not a homogenous group and our access to technology is also affected by a number of other factors such as race, ethnicity, caste, sexual orientation, gender identity and expressions, abilities, age, class, income, culture, religion, urban or rural locality, etc. Therefore, our experience of, use of and need for technology is varied, and we have to overcome multiple discriminations in order to gain access. These include, but are not limited to, the lack of infrastructure, high cost of devices and connectivity, limited access to technology training and ICT literacy, education and work, cultural and religious restrictions, geographical location, language and accessibility barriers, and full and informed consent to share personal data, etc.

Even when we overcome those barriers, often women and girls' increased access to the Internet is directly proportional to the increase of violence against women online[5], including threats against women human rights defenders[6] and the increased risk for human trafficking, particularly of adolescents girls.[7] Many a time, rather than address the structural causes of violence, the possibility of violence is used as a

[4] http://intgovforum.org/cms/documents/best-practice-forums/623-bpf-online-abuse-and-gbv-against-women/file
[5] http://www.genderit.org/sites/default/upload/issue_womenrights_digital.pdf
[6] http://www.genderit.org/resources/infographic-sexual-rights-activism-internet
[7] https://www.unodc.org/documents/blueheart/BOOKLET_FINAL_09_abril_impresion.pdf

reason to restrict women and girls' access to the Internet and censor their freedom of expression and right to bodily integrity. Or, as we've seen in our countries[8], laws that purportedly address cyber crime are put in place to grant the State sweeping powers to restrict people's, and especially women's, right to information, freedom of expression, sexuality, sexual rights, right to bodily integrity, etc. It is also important to note that technology-related and online violence does not happen exclusively on the Internet and the same is applicable to the consequences of such violence such as violations of women's right to privacy, education, work, health, etc.

In this submission, we will be viewing, critiquing and assessing existing practices of law and policy on technology-related and online violence against women based on this context.

Existing legislative models, criminal or administrative, on prosecuting and punishing various forms of online violence against women

In most cases of technology-related and online violence against women, it is apparent that victims/survivors are looking for immediate relief over legal remedies and redress[9]. Given the speed at which information is disseminated over the Internet, it is more important to be able to offer prompt and practical solutions that give women agency and uphold their bodily integrity as compared to legal remedies, which move at a slower pace. At the same time, violations of the human rights of women online including sexual rights should not be dismissed as lesser violations[10] and there needs to be awareness raising for both women as well as law enforcement on reporting and responding to violations of rights online.

The current trend all over the world is to increase criminalization of online behavior through laws and policies.[11] This trend shows that states continue to rely on legislation as the main solution to technology-related and online violence against women without setting up or strengthening institutions mandated by the state to provide cyber security and support[12]. Not only does over reliance on criminalization as a solution fail to deliver the urgent solutions needed by users including women in

[8] http://www.reuters.com/article/us-pakistan-internet-idUSKCN10N0ST

[9] https://digitalrightsfoundation.pk/wp-content/uploads/2017/07/Cyber-Harassment-Helpline-Six-Month-Report.pdf

[10] http://www.genderit.org/sites/default/upload/csw_eng_web.pdf

[11] https://www.theguardian.com/technology/2016/apr/12/online-abuse-how-harrassment-revenge-pornography-different-countries-deal-with-it

[12] https://www.facebook.com/CERT.lk/posts/1510843422320819

all their diversity and those who have historically experienced discrimination and violence including LGBT individuals and people with disabilities, but it also results in not acknowledging and addressing structural problems that lead to rights violations. "From our various experiences across the globe in advocating for sexual and reproductive justice, it is clear that criminal law has not adequately addressed impunity nor has it sufficiently addressed/reduced sexual and reproductive rights violations"[13].

Many countries in the Global South are still in a norm setting phase when it comes to the internet and ICTs but examples from many countries point to missed opportunities to develop laws and policies with the participation of diverse stakeholders and with the most marginalized people at the center. Online behavior is regulated and criminalized through the use of legislation focused on the Internet, such as cybercrime laws as well as through the use of other existing laws such as the penal code and laws on national security. This leads to incoherence and confusion as well as to disproportionate penalties[14], especially when the various laws and policies deemed applicable to online behavior are not consistent with each other.

India

Indian Information Technology (IT) Act of 2000 and the Criminal Law Amendment Act of 2013 address different aspects of online violence and "may be contributing to confusion among both victims/survivors and law enforcement about recourse in cases of abuse"[15]. The Act of 2000 also contained a provision that criminalized political and religious opinion and while this was later struck down, it had already been used by the state "to arrest people over their posts on social media, often for content that officials claimed was "seditious," "communally sensitive," or abusive"[16]. Indian Supreme Court recently recognized privacy as a fundamental right, which has opened up legal recourses for women to address online violence[17]. The current judgment for the first time acknowledged that the LGBTQI+ community has a right

---

13 http://resurj.org/sites/default/files/2017-05/Shortcomings%20of%20Penal%20Policies%20Meeting%20Statement-English.pdf

14 https://www.digitalrightslac.net/en/delitos-informaticos-la-necesaria-perspectiva-desde-los-derechos-humanos/

15 https://feminisminindia.com/wp-content/uploads/2016/05/FII_cyberbullying_report_website.pdf

16 Ibid.

17 http://www.hidden-pockets.com/debarati-halder-legal-reourse-revenge-pornography-cyber-stalking

to privacy with respect to their sexual orientation. In addition to protecting sexual orientation, this judgment also opens up debate around abortion laws in India[18].

Mexico

A 2015 report[19] states that while the country has an abundance of legislation on violence against women (though with weak implementation), the country's ICT legislation is still in its infancy. "Debate on VAW and ICT is still academic and, in practice, self-regulation has filled the void left by the lack of national laws on technologies. Laws regulating VAW committed through the use of ICT are still a long way off.[20]" Recommendations put forward by civil society include strengthening the existing legislation on VAW as well as harmonizing federal laws with local laws, given that the former have incorporated many of the international human rights obligations undertaken by the state, while being cognizant that "laws should balance the rights to privacy, the right to live free from violence and harassment, and the right to freedom of expression.[21]"

Nigeria

In 2015, Nigeria passed the Cybercrime (Prohibition, Prevention, etc.) Act into law, a piece of legislation that was expected to address the country's prevalence of cybercrime. However, the law has been found to violate various rights including right to privacy and freedom of expression and gives the state the power to criminalize online behavior. A 2016 report shows that "the number of bloggers, online journalists, and ordinary users arrested for their online activities increased dramatically in the past year, many under Section 24 of the cybercrime law[22]". The Digital Rights and Freedom Bill of 2016 is a response to the rights violations experienced by such legislation although it is yet uncertain whether it will be passed [23]. The Violence Against Persons (Prohibition) Act of 2015[24] has no provisions explicitly referring to online VAW although, section 46, which is the interpretation section of the Act, includes telephone, email, text messages and "other objects" in its definition of harassment.

---

[18] http://www.resurj.org/ReflectionsOnOurCountriesOctober2017

[19] http://www.genderit.org/sites/default/upload/mexico_analytical_report.pdf

[20] Ibid

[21] Ibid

[22] https://freedomhouse.org/report/freedom-net/2016/nigeria

[23] https://lawpavilion.com/blog/the-violence-against-persons-prohibition-act-2015/

[24] https://lawpavilion.com/blog/the-violence-against-persons-prohibition-act-2015/

Pakistan

Pakistan has been using a range of laws from the Pakistan Telecommunications Act of 1996 to the Pakistan Penal Code to the Anti-Terrorism Act of 1997 to the Electronic Transactions Ordinance of 2002 and the Defamation Ordinance of 2002 (and Amendment Act of 2004) in order to criminalize both legitimate and otherwise online behavior and stifle freedom of expression. In the recent past, the situation has exacerbated with more legislation such as the Protection of Pakistan Act of 2014 (PPA), and the Prevention of Electronic Crimes Bill (PECB). While the wide scope of legislation such as the PECB can be used to prosecute perpetrators of online violence against women[25], "human rights activists have pointed out that there is a lot of room for the law to be misinterpreted or misused"[26] and this is proving to be true[27]. During the Asia Pacific regional Internet Governance Forum in 2017, the Digital Rights Foundation, Pakistan shared that often the laws introduced to address online harassment and VAW are paternalistic and protectionist and government services that assist in instances of cybercrime are centered in urban areas and lack capacity to meet the needs of women.

United Kingdom

In 2015, new legislation on controlling or coercive behaviour[28] in an intimate or family relationship was introduced in the UK (Section 76 of the Serious Crime Act 2015), which includes coercion and control that takes place through Internet and communications technologies. Domestic violence is not defined in UK law, nor is the online violence that can be part of it, and there is no statutory offense of domestic violence or abuse. A new Domestic Violence and Abuse bill[29] is set to come into law by 2019, which will consolidate existing legislation related to domestic violence in other laws that will define domestic abuse in law. There are some offences included across UK law related specifically to cyber-enabled VAWG, such as disclosing private sexual images without consent (Section 33 of the Criminal Justice and Courts Act 2015), however there is no specific legislation or definitions of cyber stalking and cyber harassment in relation to VAWG. As with legal provisions related to domestic violence, there have been calls for the consolidation of legislation related to cyber-enabled crime, into one act. Ongoing efforts to introduce a bill on domestic

---

[25] http://content.bytesforall.pk/sites/default/files/CaseStudies-TechnologyDrivenViolenceAgainstWomen.pdf

[26] http://content.bytesforall.pk/sites/default/files/Pakistan_Internet_Landscape_2016_Web.pdf

[27] https://www.voanews.com/a/bloggers-detained-face-blasphemy-charges/3781042.html

[28] http://www.cps.gov.uk/legal/a_to_c/controlling_or_coercive_behaviour/

[29] http://researchbriefings.parliament.uk/ResearchBriefing/Summary/SN06337

violence in the UK, should take into account technology-related and online violence against women, including against women who are disproportionately affected by racist and xenophobic online abuse and violence, also outside of intimate and family relationships.

Recommendations

Based on these lessons learnt from our countries, we recommend that criminalization and regulation through civil law should be just one strategy of a multi-pronged approach towards addressing technology-related and online violence against women. Other strategies include awareness-raising for both internet users and law enforcement on rights and violations of online behavior and related remedies/legal framework, inclusion of online behavior and use of technology in sexuality education curricula in and out of school, and strengthening institutions and platforms that can support and empower all women and girls in all their diversity subjected to online violence against women. Instead of a piecemeal approach to passing and applying various legislation to address technology-related and online VAW, states should focus on fully implementing existing legislation on VAW by interpreting as well as amending them to comprehensively address technology-related and online VAW.

Existing policies that allow identification, reporting and rectification of incidents of harassment or violence against women via the Internet service providers

We feel that examining these policies via just Internet service providers (ISPs) is too narrow an approach. ISPs are just one of many Internet intermediaries[30] and this is especially true for some countries from the Global South in which the internet is synonymous with Facebook[31]. Internet intermediaries range from network infrastructure providers to ISPs to mobile network operators to social networks and search engines to Internet cafes[32]. We will be sharing experiences from our countries within this broader framing and examining how identification, reporting

---

[30] Internet intermediaries' bring together or facilitate transactions between third parties on the Internet. They give access to, host, transmit and index content, products and services originated by third parties on the Internet or provide Internet-based services to third parties (Source: OECD), https://www.oecd.org/internet/ieconomy/44949023.pdf

[31] https://qz.com/333313/milliions-of-facebook-users-have-no-idea-theyre-using-the-internet/

[32] https://www.apc.org/sites/default/files/READY%20-%20Intermediary%20Liability%20in%20Africa_FINAL_0.pdf

and rectification of incidents of harassment and violence is done via internet intermediaries.

It is also important to contextualize our experiences against what is largely a neoliberal model of internet governance[33] in which policies, programs and decisions that shape the internet are centered around the interests of private companies that often exploit personal data for profits and in the process may endanger internet user personal integrity. While Internet governance spaces strive to be multistakeholder, the influence private companies wield over public policy is becoming more apparent, especially in the case of technology and ICTs where states and other stakeholders often lack resources and capacities. In a world and global economy in which "data is the new oil[34]", women are viewed primarily as data by internet intermediaries rather than rights holders.

Internet intermediaries have a responsibility towards internet users including women and being held accountable for this responsibility should not be conflated with policies which enable states to compel internet intermediaries to share, edit or remove content in violation of freedom of expression. Experiences from our countries show that it is necessary for countries to come up with context specific policies and solutions that allow identification, reporting and rectification of incidents of harassment or violence against women and girls via the internet service providers which are not framed as blanket provisions that could unduly restrict freedom of expression, including sexual expressions of women.

In 2016, a court order in Brazil threatened blocking Facebook unless a parody profile of a politician was removed from the platform[35]. A 2015 report from Mexico shows that the country's ISPs often breach users' rights to privacy and that "with more than 100,000 government data requests in Mexico in 2014, Mexican Internet users are increasingly a target for government investigation[36]". The #KeepItOn campaign tracks internet shutdowns in India[37] (114 in total and 55 in just 2017), a majority of which occur in Jammu and Kashmir with the reason given being

---

33 http://www.academia.edu/30757621/The_Anatomy_of_Neoliberal_Internet_Governance_A_Queer_Critical_Political_Economy_Perspective

34 http://fortune.com/2016/07/11/data-oil-brainstorm-tech/

35 http://gizmodo.uol.com.br/justica-eleitoral-bloqueio-facebook/

36 https://www.eff.org/deeplinks/2015/06/new-report-shows-which-mexican-isps-stand-their-users

37 https://www.internetshutdowns.in/

deterioration of law and order[38]. In Nigeria there is uncertainty, both legislative and regulatory, on how much protection is provided for Internet intermediaries with a draft legislation that could "seriously impact the ability of Nigerians to access and share information on the internet".[39]

While companies such as Google and Facebook have introduced methods of reporting and rectifying incidents of technology-related and online violence, especially the unauthorized dissemination of private content[40], there are added challenges in accessing such remedies. In Sri Lanka, a key challenge in reporting incidents of harassment and violence is language. Most incidents seem to occur on Facebook with around 200 complaints daily[41], a majority from women, lodged each month with the Sri Lanka Computer Emergency Readiness Team (SL CERT). However, the advice given from SL CERT is to directly report to Facebook[42] which in turn is a weak solution given that Facebook is not equipped to moderate posts in local languages[43].

A recent report from Pakistan show that depending on the context and situation, women may not even want to report, whether to law enforcement or to internet intermediaries, as they feel that reporting may tarnishes their name and reputation, and could put them in more danger[44]. And frequent censorship of women's bodies, gender expressions and identity as well as sexuality by Internet intermediaries (sometimes based on their own policies and sometimes at the behest of the state)[45], especially social media platforms, has contributed towards women's lack of confidence in them.

A 2017 report elaborates how India has adopted a safe-harbor approach to intermediary liability, which provides immunity from legal liability to

---

38 http://www.ndtv.com/india-news/internet-suspended-in-kashmir-ahead-of-burhan-wanis-death-anniversary-1721598

39 http://www.apc.org/en/news/internet-intermediary-liability-nigeria-new-legisl

40 https://support.google.com/websearch/answer/6302812?hl=en

41 http://www.dailymirror.lk/43482/nearly-200-cyber-crime-related-incidents-reported-in-sl-each-month-

42 http://www.sundaytimes.lk/111113/BusinessTimes/bt24.html

43 https://roar.media/english/tech/insights/getting-harassed-on-facebook-heres-what-you-need-to-know/

44 http://digitalrightsfoundation.pk/wp-content/uploads/2017/05/Hamara-Internet-Online-Harassment-Report.pdf

45 https://www.apc.org/en/pubs/issue/media-brief-censorship-sexuality-and-internet

intermediaries with the provision of certain exceptions[46]. The Supreme Court of India has previously ruled that intermediaries should only act upon judicial or executive orders, which is challenging given the urgent remedies required by those subjected to technology-related and online VAW.

It is apparent that some policies and practices do exist in our countries with regard to content moderation, with varying degrees of effectiveness. Most instances of Internet intermediaries taking action don't seem to be on the basis of their accountability towards Internet users. The Electronic Frontier Foundation states, "It's clear that Internet technology companies—especially those further "upstream" like domain name registrars —are simply not equipped or competent to distinguish between good complaints and bad in the US much less around the world. They also have no strong mechanisms for allowing due process or correcting mistakes. Instead they merely react to where the pressure is greatest or where their business interests lie.[47]"

We recommend that states, as duty bearers, must hold Internet intermediaries accountable for their human rights commitments, including as set out in the United Nations Guiding Principles on Business and Human Rights[48]. States must also report under their various human rights obligations[49] and sustainable development commitments[50] on steps they are taking to address technology-related and online violence against women, including steps taken to hold Internet intermediaries accountable.

Policies to hold Internet intermediaries accountable should include self-regulation through internal policies as well as co-regulation with the state and civil society.

---

46 http://www.itforchange.net/sites/default/files/Technology_mediated_VAW_in_India_issue_paper_ITforChange_Feb_2017.pdf

47 https://renegadeinc.com/10-years-activists-silenced-internet-intermediaries-long-history-censorship/

48 http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf

49 CEDAW General Recommendation No. 19: Violence against women http://www.refworld.org/docid/52d920c54.html

50 SDG 5.2 Eliminate all forms of violence against all women and girls in the public and private spheres, including trafficking and sexual and other types of exploitation
SDG 5.b Enhance the use of enabling technology, in particular information and communications technology, to promote the empowerment of women

These policies should be developed in consultation with feminist and women's rights organizations and should be based on human rights and women's human rights principles. As some of our country example illustrated, content regulation policies cannot be at the expense of unduly restriction of freedom of expression, including sexual expression and diverse gender identity of women and therefore would require a careful balance and cognizance of national and local contexts. Countries should adopt data protection laws[51] that would prevent or mitigate the storing or selling of content, especially content shared non-consensually.

The implementation of these policies should be transparent and have independent monitoring mechanisms that include civil society representatives. State mandated agencies such as Computer Emergency Response/Readiness Teams (CERT) should carry out awareness raising campaigns on the responsibilities and related accountability of Internet intermediaries and create modalities for women to connect with Internet intermediaries for the identification, reporting and rectification of incidents of harassment or violence. Accountability from internet intermediaries should also include internal capacity strengthening of staff on identifying technology-related and online violence against women as well as appropriate response and rectification of such reports. Internet intermediaries such as social media platforms need to commit to making available local language moderation as well as proper training of moderators.

Key Recommendations

Multipronged and intersectional approach to addressing technology-related and online VAW

We imagine and advocate for a feminist internet that "works towards empowering more women and queer persons – in all our diversities – to fully enjoy our rights, engage in pleasure and play, and dismantle patriarchy"[52]. An essential component of a feminist Internet would be recognizing technology-related and online violence against women as a structural issue that needs to be comprehensively addressed as such. As with all other social justice issues we continue to grapple with, our analysis shows that there is no one-size-fits-all solution to technology-related and online violence against women that is applicable to all our countries. It is also apparent that this issue cannot be addressed on its own, as it intersects with a number of other rights and freedoms that all women are entitled to.

[51] https://digitalrightsfoundation.pk/why-pakistan-badly-needs-a-data-protection-law/
[52] Feminist Principles of the Internet by the Association for Progressive Communications https://www.apc.org/en/pubs/feminist-principles-internet-version-20

Recommendations made by the Special Rapporteur on violence against women in the presentation of her report to the Human Rights Council in June 2018 must make note of the following:

Legislation and content regulation might be useful strategies but they will not be effective until they are part of a larger and more comprehensive strategy that is both multi-pronged and intersectional.

Policymaking and Internet governance must be centered around the most marginalized and women in all their diversity, and recognize that women are not a homogenous group and have diverse needs. Feminist and women's rights groups must be a part of the design, implementation and evaluation of policies, processes and projects that aim to address technology-related and online violence against women.

Violence against women not just violates women's sexual and reproductive health and rights but also rights to non-discrimination, education, employment, privacy, etc. as well as fundamental freedoms such as freedom of opinion and expression and of peaceful assembly and association.

States need to move away from a paternalistic and protectionist approach to preventing and ending violence against women including technology-based and online violence against women that can perpetuate gender stereotypes towards an approach that upholds human rights and respects women's decision making.

We thank the Special Rapporteur for this opportunity to provide our input and remain committed and active stakeholders in carrying this work forward.