sflc.in

SFLC.IN
2nd Floor, K9
Birbal Road, K-Block
Jangpura Extension, Delhi – 110014
sflc.in | mail@sflc.in | +91-11-43587126

30.08.2020

To,

Dr. Shashi Tharoor

Chairperson

Standing Committee on Information Technology

Parliament of India

Respected Dr. Tharoor,

Subject - Women safety in the Digital Space

SFLC.in is a civil society organization working in the Digital Rights space. The current pandemic as well as the ongoing technological revolution have pushed our entire ecosystem to be online. This means that there are greater threats for women and marginalized communities in various forms over digital spaces especially social media platforms.

1. Introduction

SFLC.IN, in its capacity as a non-profit organisation seeking to protect and promote civil liberties in the digital world, has worked closely on issues affecting free expression in digital space. We have studied online harassment as a form of censorship that forces people out of participating in the online discourse. A study conducted by Amnesty International in India, UK and USA to measure online abuse faced by women politicians found that Indian women politicians experienced 13.8% problematic or abusive tweets, which was substantially higher. In one of SFLC's reports on online harassment, activist Kavita Krishnan had highlighted the abuse faced by her in an online chat by Rediff. Similar incidents were narrated by Meena Kandasamy, Rega Jha and Sheeba Aslam. Only recently, a student of GNLU Iqra Khilji, and a comedian, Agrima Joshua were harassed on social media where their address was leaked and they received rape threats too. Amongst other issues faced by women on these platforms include impersonation, doxing, identity theft, cyber bullying and cyber stalking.

Doxing (also spelled as "doxxing") is the practice of harvesting and publishing personally identifiable information i.e. information that can be used either on its own or in combination with other information to identify, locate or contact and individual.

Identity theft and identity fraud are when someone obtains and wrongfully uses another person's personal data in a way involving fraud or deception. The goal of this is to impersonate the victims and leverage their identities to build negative opinions around them, or use their credentials for personal profit.

Cyber-bullying refers to the deliberate act of abusing or harassing someone over the internet. It can be as simple as sending harassing emails or messages but also includes action such as repeated threats, sexual remarks, or defamatory false accusations. Cyber-bullying can be more harmful that traditional bullying because there is no escaping it, and that it is an intense form of psychological abuse, whose victims are more than twice as likely to suffer from mental disorders compared to traditional bullying.

Cyber-stalking is use of internet or other electronic means to stalk or harass an individual, a group, or an organisation. It includes false accusations, defamation, slander or libel and may include monitoring, identity theft, threats, vandalism, solicitation for sex etc.

2. Questions for Ministry Representatives

1. Apart from existing content reporting mechanisms available to users, how is the government ensuring the digital safety of citizens particularly women?
2. How many orders have been served to social media platforms to take down content hampering the digital safety of citizens?
3. Is the MeitY maintaining data of sub-judice cases on cyber stalking, bullying and harassment across the country? If so, provide state-wise details.
4. What steps have MeitY taken to address these issues? Has MeitY or Ministry of Home Affairs or Ministry of Women and Child Development had consultations with social media platforms on these issues?
5. If so, provide details of these consultations and plan laid down for ensuring digital safety?
6. Has the MeitY provided any guidelines/inputs to the Ministry of Education on including digital safety curriculum in schools as well as colleges? If so, provide details.
7. Have there been any guidelines issued by MeitY to social media intermediaries to counter online harassment against women?
8. Has the Ministry conducted any security trainings for women to deal with online threats during the pandemic? If not, are there any future plans to do so?

3. Suggestions

Based on our experience of working in the digital sphere, we have come up with some suggestions that we feel that the committee can benefit from -

a. Clear and Concise Rules: Intermediaries such as Twitter and Facebook (Intermediaries) should have clearly articulated rules to prohibit hateful, disparaging, and harassing content online. Such rules should be accompanied with examples of prohibited content designed for easy consumption and understanding.

b. Awareness Creation: Stakeholders including the ministry as well as intermediaries should generate awareness about prohibited content using innovative methods such as notification system and promotional banners.

c. Easy Reportage Mechanism: Intermediaries as well as Law enforcement agencies should deploy mechanisms to ensure easy and accurate reportage, with tools such as prominent identifiable report button, adequate opportunities to substantiate why content should be report. Users should not be burdened with burden of articulating the complaint in a particular language and/ or format. They should have the liberty to file the complaint in different languages and/or in written, audio or visual (via shooting videos) formats as well.

d. Dedicated Teams:Intermediaries should have specific teams which work with automated tools to review and disable content. Such teams should be made to undergo periodic training on efficient identification and disablement based on objective standards per applicable national laws.

e. Prompt Response and Appeal Mechanism:Intermediaries should have mechanisms to ensure review and action of disputed content within a prescribed time frame (ranging from 24, 48 to 72 hours). However, care should be taken to ensure that such steps do not cause chilling effects on right to freedom of speech and expression. Thus, creators of disabled content should be accorded opportunities to justify themselves- along with provisions for timely restoration of content and/ or reinstatement of terminated accounts.

g. Engagement with different stakeholders: Ministry as well as intermediaries should engage with civil society, subject matter experts and academia for awareness generation, conduct training workshop for law enforcement officials to facilitate effective handling of complaints, hold training sessions, innovative workshops for school/ college students to help them understand the nuances of online harassment at an early age.

h. Promote Counter Speech: Work towards promoting counter speech- inviting counter narratives, offer incentives and work towards conceptualizing additional means to promote counter narratives.

Through this letter, we would like to urge you to look at this matter in depth on an urgent basis. We would also be honored to assist the committee in any manner deemed fit. We at SFLC.in conduct regular 'Digital Security Training' Workshops designed to raise awareness in this regard and educate attendees on the fundamentals of digital security.

SFLC.IN is the first Indian legal services organization that works exclusively on technology, law, and policy. As a not-for-profit organization engaged in the empowerment of Indian citizens about their digital freedom and rights, it operates as a collective bringing together different stakeholders to a common platform to further the cause of digital rights. SFLC.in promotes innovation and open access to knowledge by helping policy makers make informed and just decisions regarding the use and adoption of technology. As of 2020 SFLC.in is the only Indian organization to be inducted as a member of the IFEX, a global network to defend the right to freedom of expression and information.

Yours Sincerely,

Prasanth Sugathan

prasanth@sflc.inin

Legal Director

SFLC.in