**[Evolving frameworks and protecting users online](https://nation.com.pk/24-Dec-2020/evolving-frameworks-and-protecting-users-online%22%20%5Ct%20%22_new)**

Tayyaba Iftikhar December 24, 2020

Social media platforms such as Facebook, Twitter, Instagram and others have given a new definition to the term “connected” whereby we are always connected and inundated with data and information from around the globe. However, it is important to note that this unprecedented level of exposure comes with new hazards and regulatory issues that need to be managed in order to safeguard the quality of the user’s online experience and their ability to harness the positive impact of these technologies.

The broad dilemma of the internet is that it makes it easy for bad actors, ranging from trolls to spammers to malicious hackers, to infiltrate and manipulate a community’s online experience. In some cases, it deters users from using the platform. Notable examples include: Facebook’s failure to curb posts, comments and images attacking the Rohingya and other Muslims; other social media platforms such as YouTube and Twitter’s negligence to stop far-right extremist content and white supremacists’ spiel.

So based on these scenarios—is government regulation on the internet inevitable? A necessity?

Up until now, the regulation of content has been focused on traditional media platforms—television, radio, film and print—in domestic or regional settings, with rules enforced by regulators and industry. When it comes to regulating online transnational content there is no international agreement on how states should exercise their jurisdiction, or on what kind of content should be considered abusive, when or whether internet companies should be responsible for their users’ content at all, how or if they should remove content considered harmful or abusive, and whether such removals are global or limited in scope.

These problems are so intertwined with the sovereignty of each state that these issues require immediate addressing. Globally, tech giants tend to argue that their community standards are best suited to govern the entire internet and are suitable for each country however, these standards are a reflection of mostly American or western norms and culture and may conflict with local values. A recent example of Facebook making new anti-Semitism rules while the same platform is not sensitised to look into anti-Islam content.

We cannot ignore the fact that different countries have different cultures, imperatives, and legal and constitutional frameworks. In Singapore, the Minister for Communications and Information in January 2017 unveiled plans to amend the Films Act and the Broadcasting Act in 2017 to clarify the application of content regulation to ‘over the top’ (OTT) video providers. This will mean that strict broadcasting standards such as censoring nudity, and extreme language will apply to global players in that market.

Notably, Netflix was blocked in Indonesia by Indonesia’s largest telco Telekomunikasi Indonesia (Telkom), for not submitting content for approval and displaying ‘violence and adult content’.

The borderless nature of the internet has enabled internet users to access content created and hosted from all over the world, and it is not always possible to tell where it has come from or where it is hosted. This leaves governments with a thorny problem to tackle when it comes to content that is harmful or does not conform to the social, legal and political context of the country. Under international law, one of the primary means for states to exercise their jurisdiction is the territorial principle, the right to regulate acts that occur within their territory.

States have interpreted the principle to argue that the mere accessibility of online content from within their territory is deemed sufficient to regulate online content. For example, in court cases against Perrin and Yahoo, UK and French courts respectively applied their national laws to online content accessible in their countries, even though it had been uploaded from and was hosted in the US. The act of publishing content online, the courts argued, is equal to physically acting or producing adverse effects within their territory irrespective of its origin.

A common criticism to the internet and social media regulation is state censorship and encroachment of an individual’s right to freedom of expression. However, all speech should be and is already subject to some form of rule/regulation such as prohibition of hate speech, defamation etc. Studies have shown the significance of the internet and social media in spreading information; regardless of the accuracy or inaccuracy of the content shared.

In 2018, the Turkish government investigated 403 social media accounts and took legal action against 267 users on accusations of disseminating propaganda for terrorist organisations.

The actions of social media giants and the way in which they manage online content can negatively affect internet users’ rights worldwide. Tech companies’ choices of where to host their data, the country in which they are based, and consequently the laws with which they have to comply, what they include and exclude from their terms of service and who within the host and company can access the data all significantly affect the rights to privacy and freedom of expression of internet users worldwide.

While governments can make content restriction requests to social media platforms for moderation of content in violation of local laws, social media platforms are not obliged to entertain these requests because their community standards do not include the social and religious context of the country. In Pakistan, these requests are made by the Pakistan Telecommunication Authority (PTA) as per the criteria laid down in Section 37 of the Prevention of Electronic Crimes Act 2016 (PECA). However, a large part of these requests are not responded to/action is not taken.

The ability of foreign social media companies to make decisions regarding which content is removed or allowed, as well as which content is prioritised, translates into enormous political and social power. These companies do not take into account the cultural, religious, social and legal aspects of Pakistan. Due to low literacy, users in Pakistan are also not well versed with using social media responsibly. Content that includes pornography, violence, child sexual abuse, extremism, anti-state narratives and immorality can be accessed, shared and spread to large groups of people instantly. In view of this, the law enforcement agencies also face hindrances in their attempts at investigating the source behind the objectionable content and criminal prosecution that may follow.

Many countries are already recognising this problem and are crafting rules that are appropriate to their particular domestic social, legal and political contexts. Germany’s NetzDG law came into effect at the beginning of 2018, applying to companies with more than two million registered users in the country. The European Union has introduced the General Data Protection Regulation (GDPR) which set rules on how companies, including social media platforms, store and use users’ data. It has also taken action on copyright. Its copyright directive puts the responsibility on platforms to make sure that copyright infringing content is not hosted on their sites.

As markets evolve, so do regulatory frameworks. Flexibility in adopting a regulatory approach is arguably the key, but there is little doubt that new arrangements, approaches and regulations on online content specifically in Pakistan’s context are necessary. Until that is done, we all, as users, will continue to come across unwanted, harmful and illegal online content we do not want to see on our social media feeds.