1. What do you believe are the key challenges raised by disinformation? What measures would you recommend to address them?

Creating and spreading false information and false narratives constitutes information *warfare* that creates highly vulnerable consumers within media ecosystems. It has the potential to erode public trust in institutions, democratic processes, and journalism. By blurring the distinction between organic rumours and the organised intent to fulfil an objective, disinformation is able to manipulate human responsiveness to news events, reactions, new information, fears, biases, passions, and beliefs. The digital space and information overlap and overload has only further amplified this process.

As electoral disinformation campaigns launched by States or corporate entities become increasingly coordinated and frequent, disinformation poses a direct threat to democracy. It has been tactically employed to mould public opinion and shape the outcomes of elections and even demonstrations, often at the risk of polarisation and violence. This has led to real consequences for voter participation, voter suppression, freedom of expression, and credibility of democratic institutions. Authoritarian regimes have used it to attack the democratic instinct of citizens.

Meanwhile, rampant disinformation in online spaces has also stained the work of professional journalism with counter narratives, verbose irrationality, and factual inaccuracies. At the cost of informed truths, journalists continue to be identified, threatened, and attacked for their reportage across the world, even as audiences grow an appetite for sensationalism.¹ Both, what is said and what is consumed are crucial in the emergence of vulnerable and reactionary communities. In India, ‘fake news’ disseminated over WhatsApp has led to multiple cases of mob lynching.² Unscientific information continues to pose a number of public health risks as online spaces are rife with ‘fake news’ surrounding the COVID-19 pandemic and the vaccines.³

---

The absence of a legislative framework, specifically targeting disinformation, has further created gaps. While the more alarming concern in the international community at present is the deliberate and reckless nature of disinformation campaigns, it is important to note that the current international jurisprudence on freedom of expression does not necessitate that an expression or information imparted has to be correct. The Special Rapporteur’s report on the issue should also look at the framing of policies that give due importance to the correctness of expression or information without violating international human rights norms. Governments, platforms and other relevant stakeholders should work together with the Special Rapporteur in developing parameters to identify such wilful disinformation based on mens rea (wilful guilty intent) as well as the consequential and collateral impact of the information shared. There is an urgent need for standard setting in this respect that is responsive and in line with international human rights standards.

Intermediary platforms showing greater resolve in tackling misinformation online by supporting governments in promoting official and reliable information has not reduced production and consumption of false information. Instead, it has caused a two-fold blow: standard application of intermediary rules is being used to curb freedom of expression online. Given the vacuum in international jurisprudence laying down standards and a definitive yet responsive framework related to disinformation, there has been an increasing focus on implementing solutions at the national level, notwithstanding the challenges that it may pose.

Preventing disinformation from adversely impacting electoral systems, media freedom, and rights of journalists globally requires collective and coordinated efforts on three fronts:

(i) The government must introduce effective legislative safeguards and processes as well as build international cooperation.

(ii) Platforms must introduce self-regulation or co-regulation for countering disinformation. Prescriptive regulation has not proven to be effective in this regard. Platforms must also engage more with governments in the developing world. Increased proactive transparency from technology platforms and holding them accountable for keeping their users safe online is an essential aspect of counter measures against disinformation. They must engage more with local contexts, local legal institutions, and civil society.

(iii) Communities, who on their own cannot fight disinformation, must be empowered with media, information and data literacy. Government, platforms and civil society must together to educate and build awareness among users of internet, a large section of whom are first are users.

---


2. a. What legislative, administrative, policy, regulatory or other measures have Governments taken to counter disinformation online and offline?

National responses to rampant disinformation in digital spaces have taken many forms across different regions. Most notably, the European Union’s Code of Practice on Disinformation invites technology platforms on a voluntary basis to sign and build a roadmap for implementing the objectives agreed upon. A key feature of the European Union Code is that it is uniformly binding upon all signatories, thereby enabling greater collaboration and coordination between all stakeholders.6 The United Kingdom’s Online Harms White Paper employs a ‘harm-based approach’, which is centred on the experiences of the user to create a safer online space. It establishes a “duty of care” on digital companies to “improve the safety of their users online”.7 The Australian Communications and Media Authority (ACMA) has also published a position paper encouraging technology companies to develop their own codes of practice to tackle disinformation.8 On the other hand, ‘fake news’ legislation introduced in Singapore – the Protection from Online Falsehoods and Manipulation Act (POFMA)9 – appears to have raised legitimate concerns from different quarters, including free speech advocates and technology giants. There are fears that such a legislation could be misused by authoritarian governments to shape alternative narratives and stifle voices of dissent.10

To counter the disinformation epidemic, the Ministry of Electronics and Information Technology (ME&IT) of the Government of India published a new set of amendments to the Information Technology (Intermediaries Guidelines) Rules, 2011 that have raised serious concerns regarding privacy and surveillance. Among other things, the provisions require intermediaries to “enable tracing out of such originator of information on its platform” as required and “deploy technology based automated tools to… identify and remove public access to unlawful information or content.”11

6 Ibid.
Outside of legal recourse, several countries such as Sri Lanka and India have increasingly resorted to blanket internet shutdowns to counter the spread of disinformation. These shutdowns violate the right to freedom of opinion and expression as well the right to information. Blanket internet shutdowns violate the normative threshold set by the Siracusa Principles and often do not comply with the mutually inclusive standards of legality, evidence-based necessity, proportionality, and gradualism. It also inhibits fact-checkers and journalists from doing their jobs and reporting facts that counter misinformation. Such excesses bolster illegalities and allow human rights violations to go unaccounted for.

b. What has been the impact of such measures on i) disinformation; ii) freedom of opinion and expression; and iii) other human rights?

Shutting down access to the internet is fast becoming a preferred tool of social control and censorship in the hands of governments in several parts of the world. In the information age, internet shutdowns amount to one of the most serious human rights violations, affecting “freedom of expression, access to information, association, peaceful assembly, political participation, metal and physical health and education”. In many countries, governments have employed internet shutdowns as a means to disrupt online access and information of grassroots civil society groups. In Mali and Chad, governments have elected to impose suspensions on specific social media websites to prevent grassroots organisations from planning protests. Multiple analyses of internet shutdowns lend credence to the argument that the primary goal of such abuses of power is to quell dissent.

3. Please share any suggestions or recommendation you may have for the Special Rapporteur on how to protect and promote the right to freedom of opinion and expression while addressing disinformation.

The Code of Practice on Disinformation adopted by the European Commission to counter online disinformation in the European Union shows significant promise in this regard. It offers a robust self-regulatory framework that can be adopted in other parts of the world with context-specific alterations where needed. A 2020 Assessment of the Code highlighted its key

---

16 Internet Sans Frontières, ‘Internet Shutdowns by Governments in West and Central Africa’. Available at: https://www.ohchr.org/Documents/Issues/Expression/Telecommunications/InternetSansFrontieres.docx
18 European Commission, ‘Assessment of the Code of Practice on Disinformation: Achievements and areas for further improvement’ Staff Working Document (SWD(2020)180), September 2020. Available at:
achievements since its adoption in 2018 to have “provided a framework for a structured dialogue between relevant industry actors, the Commission, and European Regulators Group for Audiovisual Media Services (ERGA) authorities, and greater transparency of platforms’ policies against disinformation” in the European Union. The Code has enabled signatories such as Facebook, Google and Twitter to increase transparency surrounding disinformation and political advertising, thus ensuring accountability from tech platforms in this sphere. The Code’s notable success in the European Union suggests that best practices involving self-regulation may prove useful in addressing the disinformation epidemic.

We underline that to effectively counter the wave of disinformation, States must work in collaboration with technology platforms. At the same time, both States and tech platforms must work together to educate and communicate about media, information, and media literacy.

We call on the Special Rapporteur to strongly encourage and facilitate such collaborative efforts that are premised upon self or co-regulation as government and platforms must work together to make reasonable distinctions between illegal content and other types of disinformation. Legislative measures and policies must recognise that the latter is protected by the right to freedom of opinion and expression. Mutual oversight will discourage both States and technology platforms from overstepping the boundaries of what is ethical, legal, and justifiable.

We also call on the Special Rapporteur to encourage increased investment in media literacy efforts that helps users navigate the digital media environment.19 Similarly, States may be encouraged to provide better access to public data and reliable information to enable journalists and media to exercise their legitimate functions.

19 Nieman Lab, ‘The EU does not have a sense of its disinformation problem – this report suggests the policy changes it can make’, November 2019. Available at: https://www.niemanlab.org/2019/11/the-eu-doesnt-have-a-sense-of-its-disinformation-problem-this-report-suggests-the-policy-changes-it-can-make/