Protection of ‘Digital Rights’ Amid Fight Against Covid-19: The Missing Responsibility of ICTs Platforms

By:

Arunender Singhh

May 14, 2020

Introduction

It is often stated that the new technology is changing what it means to be human. The digital world is rapidly transforming society. On the one hand, it allows unprecedented advances in the human conditions and at the same time gives rise to profound new challenges. Social media is a dominating force in modern social life as internet technology has taken hold of our cyber-driven society. The oft-use of information and communication technology (ICT) to fight the battle against Covid-19 crisis has opened up new challenges for the governments, especially, for populous countries like India. There are genuine concerns that fake news has assumed a pernicious character that is harmful to citizens and society at large. The use of big data in the global world has come

to stay with ICT corporations commonly using data analytics to forecast customer preferences, boost their productivity and improve decision-making. It appears that big data may have a huge positive effect in defeating Covid-19, by promoting efficiency, monitoring health security and enhanced services, but that it might also result in discrimination, privacy violations, and other chilling effects. Further, it is inevitably true that the internet has increased the availability and accessibility of child pornography and provided new opportunities to groom. In this trying times these developments have squarely brought under the scanner the role and legal responsibility assumed by the ICTs platforms.

Anatomy of Fake News

The malaise of (dis)information, popularly called as 'fake news', potentially represents risks for democratic processes, national security, social fabric, and can undermine trust in the digital society. In the past few days, there are several instances of fake news spreading fear and chaos in the pandemic time. In India, for example, fake news triggered panic as to causes of corona virus, home remedies for the treatment, healthy Muslims injected with virus, licking of vegetables by the sellers before selling, declaration of general emergency in the country, reduction in pension by 30% and so on. The efforts of government to control and contain the spread of disease has been impaired.

The term fake news does not have a straightforward meaning, and covers a wide ambit of different types of information. It can range from the honest mistakes made by journalistic reporters to hyper-partisan political discourses to minting money through the use of clickbait headlines. A 2018 UNESCO report highlighted that fake news "is an oxymoron which lends itself to undermining the credibility of information which does indeed meet the threshold of verifiability and public interest – i.e. real news". This rightly captures the ambiguity arising out of this complex phenomenon, which can involve fake content, but also content that is not actually or entirely fake, for instance, blending fabricated information with facts by means of manipulated or fabricated videos as well as through targeted advertising, organized trolling, visual memes, and much more.

The large-scale exodus of migrant labourer working in the cities due to fake news caught the attention of the Hon'ble Supreme Court. In its order dated 31 March 2020 it prodded the media (print, electronic and social) to maintain sense of responsibility as to verify news before its dissemination. It directed them to refer and publish the official version of corona-related developments. In compliance with the order, the government of India quickly rose to the action and launched a chatbot on WhatsApp to dispel rumours and disinformation. It is called as 'MyGov Corona Helpdesk' that can be accessed by sending a text to +91-9013151515. Besides that the Press Information Bureau, the government's media arm, has started special webpage for Covid-19 as well as a page to check facts. WhatsApp on its own has tightened the norms for forwarding the message to only limited number of people. Although it won't completely stop the spreading of fake news but would slow down its viral speed. The WhatsApp group admins would be held responsible for the spread of fake news

The efficacy of these measures still needs to be assessed. This kind of ad hoc, as well as knee jerk solutions that too coming from private and non-state actors, would not obviate the need to put in place a robust legal architecture to tackle disinformation. The ICTs ever-expanding capacities and control lead naturally to viewing them as a new form of 'private governance'. It includes governance in the form of online speakers, communities, and populations, rather than thinking of them as merely facilitating or hindering digital communication.

Data Protection and Privacy

The governments around the world are facing the challenge of protecting the personal data of their citizens. The issue assumes heightened importance for a country like India when its teeming population is rapidly getting digitally connected. In a move to fight Covid-19, the government has launched an app called 'Aarogya Setu' that would enable and assist in contact tracing of corona positive patient. It would also send alert to persons that they are prone to infection being in the proximity of positive tested people. Apart from collecting location data of the registered user the app asks for personal information such as name, phone number, age, sex, profession, countries visited in the last 30

days and series of questions pertaining to medical data. It puts the personal information and privacy of the user in peril. In fact, information collected from one person can reveal social relationships and characteristics about others unbeknownst to them. The collection of vast amounts of data about individuals could facilitates new forms of surveillance, control and discrimination and manipulation, both by governments and by private companies.

The Supreme Court of India delivering a landmark decision in August 2017 on public interest litigation filed by retired judge K.S. Puttuswamy unequivocally held right to privacy is a fundamental right recognized under the Constitution. The nine-judge bench recognized that law particularly the Constitution, needs to be interpreted in the light of dramatic social transformation underway due to rapid technological innovations and globalization. As a quick response, the government constituted a committee under the chairmanship of Justice B N Srikrishna who submitted its report and the draft Personal Data Protection Bill.

The 2018 Bill puts into place the individual right over his or her personal data heralding ‘information self-determination'. It grants the right to access data, the famous ‘right to be forgotten' as well as data portability. The Bill finds an echo with the European General Data Protection Regulation (GDPR). The heart of the Bill lies in the enumeration of eight data protection principles – fair and lawful use, purpose limitation, collection limitation, notice, data quality, data retention, and accountability.

Today, ownership of information-age resources and accountability for information-age harms have become pervasive sources of conflict, and different kinds of change are emerging. We are witnessing the emergence of legal institutions adapted to the information age, but their form and their substance remain undetermined and often hotly contested. In this case, the government has shown a lackadaisical approach to protect the data of its citizens. The Bill was among the proposed bills sought to be discussed and passed on the floor of the House in the last parliamentary session. It was even included in the business agenda. However, it could not see the light of the day and got shrouded in other ‘bigger’ political matters including amendment to the Citizenship Act.

Child Pornography

In order to make the life of people bearing the brunt of lockdown more interesting one of the largest porn aggregator has doled out its premium content for free. A recent report from India Child Protection Fund shows exponential rise in the demand and distribution as well as accessibility of child pornography in the lockdown period. Although the child pornography evokes repulsion yet there is a lucrative market for it. It does exposes children to great physical and psychological harm in the online world. The decentralized and borderless nature of internet as well as anonymity of users makes the legal regulation a herculean task. It makes the legal protection uneven across the countries.

The Optional Protocol to the Convention on the Rights of the Child on the sale of children, child prostitution and child pornography requires State Parties to make or amend laws criminalizing the child pornography. The Indian Information Technology Act 2000 punishes both online child pornography as well grooming. It covers within its ambit the real as well as realistic and simulated representations of child for the purpose of pornography. The computer generated or morphed images of child attracts punishment of five years' imprisonment on first conviction and it is enhanced to 07 years on subsequent conviction. The 2019 Amendment to the Protection of Children from Sexual Offences aims to make mere possession of child pornographic material a punishable offence. Nevertheless, the legal framework does not address with clarity the liability of ICTs platforms including internet service provider to control the offensive content. The safe-harbour clause do not apply where the intermediary engages in the commission of unlawful act. Till date, no internet intermediary has been charged with the online child pornography.

Conclusion

The rapid development and spread of ICT are providing great opportunity to accelerate governmental response to the Covid-19 health crisis. At the same time, this development has exposed the weak enforcement of digital rights and freedoms. The emerging technologies have turned governmental control upside down . It has given a unique opportunity to the ICT platforms not only to govern themselves but also perform governmental functions of maintaining law and

order albeit in the cyberspace. It has become double-edge sword for developing countries like India. They need ICT platforms for developmental activities but are unable to crack down threats arising out of it. Amidst fight against Covid-19 any cavalier approach of the government concerning fake news, data protection and blooming child pornography could trigger the social unrest. It underlies that any legal, as well as a policy response, should be comprehensive, continuously assess the use of ICTs platforms in fight against Covid-19 and adjust its objectives in light of its evolution.

---

* B.Tech; M.Tech (Computer Science and Engineering) and LLB (Hons.) in Intellectual Property Rights from Indian Institute of Technology Kharagpur (India). Currently pursuing LLM in Public International Law from University of Amsterdam (Netherlands). Email: arunender.singhh@student.uva.nl

View online: Protection of ‘Digital Rights’ Amid Fight Against Covid-19: The Missing Responsibility of ICTs Platforms

Provided by Afronomicslaw