UNITED NATIONS HUMAN RIGHTS OFFICE OF THE HIGH COMMISSIONER

Internet Freedom and Censorship

By Levente Kardkovács

Overview

In recent years online safety legislation has been on the rise in countries around the world. It is common for such laws to be aimed at protecting the online safety of children (e.g. the Children's Online Privacy Protection Act 2.0 (COPPA 2.0) in the United States). Governments have also been increasingly regulating the flow of information and data privacy due to both the interests of the state and the interests of the citizens. These do not always align and internet regulation is increasingly used to erode democratic freedoms and to silence and prosecute individuals opposing the government. Due to the borderless nature of the internet, international cooperation is required to effectively tackle crimes committed and facilitated online.

Protecting Children

Several countries, especially Western nations have increasingly focused on the protection of minors online. One notable approach is expanding age verification requirements to limit access to age restricted content such as pornography, for example by requiring the user to enter their ID or take a photo of themselves (e.g. Online Safety Act in the UK). They have been criticized for being ineffective, as well as for raising privacy concerns. Governments have also been targeting social media due to the increased risk it poses to children and teenagers. Measures include demands for more strict content moderation by the platforms themselves, as well as requiring a minimum age to access the site in the most extreme case(s), such as the Online Safety Amendment (Social Media Minimum Age) Act 2024 in Australia.

Freedom of Information

Authoritarian regimes around the world are using internet restrictions more and more to maintain their grip on power. They block opposition websites, restrict access to social media, or block access to the internet altogether (although due to the measure being deeply unpopular, this is most often used to combat protests or disrupt the opposition’s ability to communicate with voters ahead of an election. Countries like China and Russia have escalated their control over the internet by making VPN-s illegal. The incumbents complete their control over narratives via content manipulation, boosting their own message, as well as spreading false or misleading information. The rise of generative A.I. in recent years has made the problem even more prominent, and difficult to combat. Beyond A.I. politicians have also been outsourcing content manipulation to social media influencers, and public-relations firms with political connections to have plausible deniability about their involvement.

Large international actors, such as Russia have also weaponized their vast resources and propaganda network to (attempt to) influence elections beyond their borders. Countries are still struggling to combat state-sponsored mis- and disinformation campaigns, and electoral campaigns funded in large part by foreign actors. Their best tool is potentially the same kind of censorship the offenders apply, raising questions about what is ‘fair’ or ‘justified’ censorship and also drawing accusations of bias and a distortion of the democratic process.

Freedom of Expression

Internet Freedom and Censorship

By Levente Kardkovács

In many states the government not only suppresses opinion but also uses internet activity to crack down on opposition. In three quarters of the countries covered by Freedom House's annual report on internet freedom, internet users have faced arrest for non-violent expression, sometimes followed by harsh prison sentences. People were physically attacked or killed in retaliation for their online activities in a record high of at least 43 countries. Legislation aimed at regulating online activity is often used to jail, torture or even kill opposition figures or anyone speaking against the government or the royal family.

Privacy and Surveillance

The collection of personal data by state and non-state actors alike leads to further erosion of the freedom of expression as such data can make it easier to target, capture, and prosecute people with undesired opinions. Some governments attack encryption publicly, demanding 'backdoor access' to private messages with the justification of combatting crime. Some privacy issues are a result of clumsy implementation of legitimate government interests in collecting some data of their citizens, some are the consequence of deliberate lobbying by private companies looking to profit off of user data. Access to this data can also prove vital in election interference, resulting in pushback from the state due to security reasons (e.g. the 'ban' of TikTok in the United States).

The Role of the Private Sector

Despite the difficulty of the task, private companies (such as Meta) have been increasingly held responsible for moderating the content appearing on their platforms (often in relation to child protections). Beyond large fines, personal responsibility of the executives (i.e. legislation threatening jail for non-compliance) has been an effective method of forcing social media companies to crack down on illegal, and in cases simply harmful content. The European Union has been especially active in combatting 'big tech' by leveraging access to its large market (making operation in the EU conditional on compliance with EU regulations).

International Frameworks

Due to the international nature of the internet, multilateral collaboration is necessary. There have been some early agreements between developed nations and more are sure to follow. It is important that the committee considers this topic, as the restriction of internet freedom,as outlined above, is often closely connected with the erosion of human rights.

Read more:

Online safety: A global regulatory overview | Herbert Smith Freehills Kramer | Global law firm
Freedom of the Net 2024 | Freedom House
Putin accuses West of persecuting Russian journalists | Reuters
Governments continue losing efforts to gain backdoor access to secure communications