Week 5: Digital Rights under International Law

Part 1: Freedom of Expression Online – Basic Principles

Freedom of Expression Online: An Overview

- Sometimes people refer to 'digital rights'. These generally refer to the application of fundamental human rights to the digital age.
- Freedom of expression as guaranteed in the ICCPR and UDHR is clearly applicable to online expression as it recognises that freedom of expression applies "regardless of frontiers" and through any "media".
- Online digital communication differs from previous forms of communication due to the rapidity and scope of its information-sharing. This raises certain new challenges for freedom of expression.

Access to the Internet-Overview

- No human rights treaty explicitly recognises a right to access the internet. The main ones (including ICCPR) pre-date the Internet.
- However, in recognition of its key role in facilitating freedom of expression and the right to information, a growing body of authoritative statements indicate that States must take progressive steps to ensure universal access to the Internet.
- As a human right, access to Internet is realised by States gradually over time, rather than immediately (similar to many economic, social and cultural rights).

Access to the Internet-Content of the Right

- Access to Internet is not analogous to recognising a right to other technologies due to its significance to daily life, especially as an expressive medium. (For example, there is no similar right to broadcasting or print media)
- The Internet is increasingly recognised as indispensable to the enjoyment of an array of fundamental rights. For example:
  - A lack of access to the Internet exacerbates existing socio-economic inequality.
  - A lack of access to the Internet can impede an individual's ability to obtain key information, search for jobs, purchase goods, etc.
- Access entails the technological ability to make use of the Internet in a manner that is affordable, safe, secure, effective and meaningful.

Recognition of Internet Access as a Human Rights Issue

- In 2003, UNESCO was among the first international bodies to call on States to take steps to realise a right of Internet access (*Recommendation concerning the Promotion and Use of Multilingualism and Universal Access to Cyberspace*)
- 2011 Joint Declaration of the special international mandates on freedom of expression: "Giving effect to the right to freedom of expression imposes an obligation on States to promote universal access to the Internet."

Recognition of Internet Access as a Human Rights Issue (cont'd)

- In 2012, the United Nations Human Rights Council passed the 'Resolution on the promotion, protection and enjoyment of human rights on the internet'.
  - "3. Calls upon all States to promote and facilitate access to the Internet and international cooperation aimed at the development of media and information and communications facilities in all countries".
- In *Kalda v Estonia* (2016), the European Court of Human Rights held that the applicant's right to freedom of expression had been violated through a prison's refusal to grant him access to Internet websites containing legal information, as this had breached his right to receive information.

Recognition of Internet Access as a Human Rights Issue (cont'd)

- "52. The Court cannot overlook the fact that in a number of Council of Europe and other international instruments the public-service value of the Internet and its importance for the enjoyment of a range of human rights has been recognised. Internet access has increasingly been understood as a right, and calls have been made to develop effective policies to attain universal access to the Internet and to overcome the 'digital divide'. The Court considers that these developments reflect the important role the Internet plays in people's everyday lives."

  -- *Kalda v Estonia* (European Court of Human Rights, 2016)

Net Neutrality

- "There should be no discrimination in the treatment of Internet data and traffic, based on the device, content, author, origin and/or destination of the content, service or application."

  –2011 Joint Declaration of the special international mandates on freedom of expression.

Net Neutrality (cont'd)

- Can be impacted in two key ways:
  - **Paid prioritisation schemes**: providers give preferential treatment to certain types of Internet traffic over others for payment or other commercial benefit and not just for technical traffic management purposes.
  - **Zero-rating:** the practice of not charging for internet data associated with accessing a particular application or set of services while such data is charged to access other services or applications.

Net Neutrality (cont'd)

- Proponents say that zero-rating services can help promote Internet access.
- In practice, they can lead users into 'walled gardens' where they access only a limited amount of information and may even think this comprises the entirety of the Internet.
- Certain jurisdictions have taken actions in support of net neutrality (e.g. India effectively banned the practice of zero-rating).

Internet Shutdowns

- One way Internet access can be restricted is through Internet shutdowns which affect an entire geographic area, as has been a significant problem in Myanmar and other countries.
- This already occurred in Myanmar pre-coup but has become more serious and widespread since.
- The techniques for imposing shutdowns vary (e.g. blocking a network, throttling speed).
- They amount to a prior restraint (i.e. prohibiting expression before it can occur).
- International human rights law is very sceptical of prior restraints, which must meet a high burden of justification.

Internet Shutdowns (cont'd.)

- Unlike more tailored blocking of online content, such as measures to block child pornography, Internet shutdowns are a blunt instrument which is not well tailored to a specific harm and raise a variety of human rights concerns.
  - Shutdowns sometimes fail to meet the "provided by law" standard, as they are often ordered without a clear legal basis or based on a vague law.
  - Where they aim to quash peaceful dissent or cover up abuses, Internet shutdowns fail to pursue a legitimate interest.
  - They also fail the 'necessity' part of the test because they are disproportionate.

Internet Shutdowns (cont'd.)

"Necessity requires a showing that shutdowns would achieve their stated purpose, which in fact they often jeopardize. Some governments argue that it is important to ban the spread of news about terrorist attacks, even accurate reporting, in order to prevent panic and copycat actions. Yet it has been found that maintaining network connectivity may mitigate public safety concerns and help restore public order…"

– 2017 Report of the UN Special Rapporteur on FOE, para. 14

Blocking and Filtering of Content

- While less drastic than a full Internet shutdown, blocking and filtering content can still significantly impact FOE.
  - Blocking: preventing access to specific, listed websites, domains, IP addresses, protocols or services.
  - Filtering: the blocking of pages based on certain features (e.g. keywords, traffic patterns, etc.).
- 2011 Joint Declaration of the international special mandates on FOE:
  - "Mandatory blocking…is an extreme measure – analogous to banning a newspaper or broadcaster – which can only be justified in accordance with international standards, for example where necessary to protect children against sexual abuse."
  - "Content filtering systems which are imposed by a government or commercial service provider and which are not end-user controlled are a form of prior censorship and are not justifiable as a restriction on freedom of expression."

Discussion

- Any comments or questions?

Part 2: Cybercrimes and Introduction to Intermediary Liability

Content Restrictions-Overview

- Any restrictions to freedom of expression online must meet the same three-part test for offline expression, i.e. they must be:
  - Provided by Law
  - For a legitimate interest (protection of national security, public order, public health or morals or respect of the rights and reputations of others)
  - Necessary

Cybercrimes: Background

- The rapid growth of the Internet has led to many States adopting overbroad cybercrimes laws which do not respect freedom of expression.
- There is at the same time a need to adopt some new criminal penalties for abuse of online communications, some of which have a particular gendered impacts, such as cyberstalking and the non-consensual dissemination of intimate images.
- Ordinary criminal rules often suffice to cover cybercrimes, while some new online crimes do need to be specifically addressed through cybercrimes laws where the activity is sufficiently different online (i.e. where there really is a new crime).

Cybercrimes: Regional Trends

- A 2021 INTERPOL report noted: "Given their position among the fastest growing digital economies in the world, ASEAN member countries have become a prime target for cyberattacks."
- To combat this, every State in South and Southeast Asia, with the exceptions of Cambodia, Myanmar and the Maldives, have adopted some form of cybercrimes legislation, and ASEAN became the first regional organisation to adopt the UN's 11 voluntary, non-binding norms of responsible state behaviour in cyberspace.
- However, such cybersecurity laws in Southeast Asia have often been abused to suppress dissent through overbroad and/or vague prohibitions. See, for example, Bangladesh's *Digital Security Act*, which has been used to target critics of the government.

Cybercrime Legislation: Some Common Issues

- Some cybercrimes laws contain overbroad wordings of crimes, unclear or missing definitions of key terms. This can lead to granting officials far too much discretion → possibilities for abuse
- Several replicate existing laws, providing duplicative offences of offline offences but with harsher penalties→ unnecessary + disproportionate.
- Some cybercrimes laws allow for surveillance or enhanced policing powers with inadequate procedural protections, such as not providing for effective judicial oversight.

Cybercrime Legislation: General Human Rights Considerations

- To respect human rights, cybercrimes legislation should:
  - Have narrow and clear definitions of cybercrimes well-tailored to advancing legitimate aims and minimally restrictive of freedom of expression and privacy rights
  - Require proof about the likelihood of an identified harm arising from a given activity before criminal liability may ensue.
  - Not create new rules for online behavior unless it is fundamentally different from its offline equivalent (or there is no offline equivalent)

    (…)

General Human Rights Considerations (cont'd)

To respect human rights, cybercrimes legislation should:

- Only impose prison sentences for expression-related offences where these contain adequate safeguards against abuse and are fully in line with international standards
- Provide for a public interest defence re: the obtention and dissemination of information classified as secret.
- Any provisions relating to search, seizure and surveillance must have sufficient safeguards, including effective judicial oversight.
- Where cybercrimes laws provide for data collection and preservation obligations, they should be accompanied by comprehensive and robust data protection legislation.
- Avoid imposing bulk data collection/retention requirements.

The Role of Intermediaries

- Freedom of expression online is enabled by a variety of private actors ('intermediaries').
- They provide different kinds of services (for example, hosting content, routing Internet traffic, search engine functions, social media networks, etc.)
- A key issue is how to deal with liability for content which can be legitimately restricted under international human rights law.

‘Mere Conduits’

- The ‘mere conduit’ principle:
  - “No one who simply provides technical Internet services such as providing access, or searching for, or transmission or caching of information, should be liable for content generated by others, which is disseminated using those services, as long as they do not specifically intervene in that content or refuse to obey a court order to remove that content, where they have the capacity to do so”.

    –2011 Joint Declaration on Freedom of Expression and the Internet, para. 2(a).

Liability for Other Intermediaries

- For other intermediaries, questions of liability are more complicated.
- Strict liability is not appropriate
  - Not practical for intermediaries to monitor their systems and would incentivise excessive take-downs.
  - This would "radically discourage the existence of the intermediaries necessary for the Internet to retain its features of data flow circulation."– *Freedom of Expression and the Internet*, a 2013 report by the Inter-American Commission on Human Rights' Special Rapporteur on FOE, para. 97.

Liability for Other Intermediaries (cont'd)

- 'Notice and Takedown' approach (common in Europe): after an intermediary has been notified about illegal content, it must take it down to avoid liability.
  - Less problematic than strict liability from an FOE perspective but still can be problematic
- 'Notice and Action' approach: intermediaries required to act upon receiving notice, but no liability if their action is ultimately not correct.
- 'Notice and Notice' approach: after an intermediary receives a notification about allegedly illegal content, it must notify the user and give them an opportunity to defend or take down the content. If the user fails to act, the intermediary should take down the content.

Jurisdiction

- The borderless nature of the Internet raises certain challenges when it comes to jurisdiction.
- Authorities can struggle with how to enforce laws when much of the content online originates or is hosted in other countries.
- On the Internet, publication anywhere is publication everywhere.
- At the same time, if there is potentially liability for content in every jurisdiction, this creates confusion for content creators and can lead to a ‘chilling effect’

Jurisdiction (cont'd)

- Jurisdictional issues for online content is particularly challenging for defamation.
- 'Libel tourism' is when plaintiffs seek to sue in jurisdictions where the law is more friendly to defamation suits.
- There is a need to address this issue:
  - "Jurisdiction in legal cases relating to Internet content should be restricted to States to which those cases have a real and substantial connection, normally because the author is established there, the content is uploaded there and/or the content is specifically directed at that State. Private parties should only be able to bring a case in a given jurisdiction where they can establish that they have suffered substantial harm in that jurisdiction (rule against 'libel tourism')"—2011 Joint Declaration, para. 4(a)

Discussion

- Any comments or questions?

Exercise

- Go into breakout groups
- Discuss whether the scenarios amount to breaches of freedom of expression or what further information would be needed to determine this.

Thank you

Raphael Vagliano, Legal Officer, Centre for Law and Democracy

raphael@law-democracy.org

www.law-democracy.org