



Group discussions and case studies: Inter-American Human Rights System instruments and their application to the digital environment

Luis Fernando García

This document forms part of a module for the APC Internet Rights Are Human Rights training curriculum. The module was produced through the APC project Examining Internet Freedom in Latin America (EXLILA), which was funded by the Open Society Foundations (OSF) and APC and coordinated by ONG Derechos Digitales.

1. Questions for group discussion (first part of workshop)

These questions should give participants the opportunity to share experiences and to explore some of the issues mentioned in the handout.

1.1. General questions

1. How has the internet changed your life and the life of people in your country? What rights have been affected positively or negatively due to access to the internet?
2. Do you think online and offline human rights should be understood differently?
3. What do you think the role of the state should be regarding the exercise of human rights online? What are the implications of the global nature of the internet for national human rights laws and international human rights instruments?

1.2. Thematic questions

1. Should internet access be considered a right? What specific obligations should the state have to guarantee universal internet access?
2. How should the right to freedom of expression online be regulated?
3. Should internet intermediaries be held accountable for users' behaviour? What are the limits of states' action to regulate the behaviour of intermediaries?
4. Are online protests that temporarily block access to a website legitimate?
5. Should protection of copyrights take precedence over the right of access to culture and knowledge, even when copyrights are infringed by persons who would otherwise not have access to the cultural or scientific goods in question?
6. Should privacy be sacrificed in the interests of the protection of security?

2. Case studies for group discussions

Case 1: Internet service interruption in the context of protests

In 2012, members of the Ngäbe-Buglé indigenous people carried out several protests against hydroelectric plants and mining activity in their territories. As part of the protests, members of the Ngäbe-Buglé people blocked the Inter-American Highway in Panama. Some demonstrators used accounts on the social network Twitter to report what was happening and take political stands.

For example, the General Cacique of the Ngäbe-Buglé Region, Silvia Carrera, used the Twitter account @caciquegeneral for sending messages to the outside world. Several journalists were also present, covering the protest events for the media.

Anti-riot police were sent in to break up the protest in order to clear the highway. As part of this operation, Panama's Ministry of Security ordered the suspension of mobile phone and internet services in the area. The authorities invoked "national security" reasons for the interruption of communications. Journalists emphasised the difficulty of doing their work in these conditions.

During the dispersal of the protest, two indigenous protesters died, and about 100 more were injured and detained.

Information about this case:

- agencias.abc.es/agencias/noticia.asp?noticia=1098310 (in Spanish)
- www.facebook.com/notes/colegio-nacional-de-periodistas-conape-panam%C3%A1/comunicado-de-cobertura-de-periodistas-en-zona-de-conflicto-en-san-felix/267343383338166 (in Spanish)
- www.oas.org/en/iachr/media_center/PReleases/2012/013.asp (in English)
- www.oas.org/es/cidh/prensa/comunicados/2012/013.asp (in Spanish)

Discussion questions:

1. How is the right to freedom of expression affected by interruption of internet services in whole populations or geographical areas?

2. Is it legitimate for the state to interrupt internet services in whole geographical areas for the purpose of security, even when journalistic coverage or the right to expression of demonstrators may be affected?
3. Should companies cooperate with the government to interrupt internet services, or should they refuse such orders?

Case 2: De-indexing of information in search engines

Recently, several individuals have tried to use personal data laws to oblige search engines on the internet like Google or Yahoo to remove information and links that affect them in some way.

This kind of action has been potentiated by a recent ruling by the Court of Justice of the European Union granting a Spanish citizen's petition to compel Google to de-index search results linked to his name, which in his view affected him negatively and were no longer relevant.

Court rulings about similar petitions have begun to emerge in Latin America. For example, in Argentina, model Belén Rodríguez sued search engine companies, demanding that they remove all porn and sexually explicit sites showing her image, which in some cases had been digitally altered. While the search engines only provided links to these contents, Rodríguez wanted them to be held liable for the damages caused by dissemination of the images.

Eventually the Supreme Court in Argentina ruled that intermediaries (like internet search engines) could not be held responsible, mainly because they are not obliged to monitor and supervise the content to which the service enables access. In Rodríguez's case, it decided, an intermediary could only be held accountable if it had actual knowledge of the content's illegality and failed to exercise due diligence.

In Colombia, a person named in a newspaper article in 2000 among those arrested for alleged human trafficking demanded the elimination of the Google link to the article. The plaintiff had never been acquitted of the crime, but the charges had lapsed because of the statute of limitations. The Colombian Constitutional Court ruled that when a person who has been prosecuted is acquitted, the information in the medium that published the article must update the information, and it suggested that searching for the information should be hindered. However, the Constitutional Court set limits upon these obligations in the case of public figures.

In Mexico, on the other hand, the personal data protection agency ordered Google to de-index links referring to a business owner which appeared as the first results when his name was searched. One of these links was to a news article about alleged acts of corruption involving a former president of Mexico and his family and a transport company linked to the businessman. The ruling mentioned the European Union Court of Justice decision, but did not consider whether or not the information was of public interest.

Information about this case:

- www.palermo.edu/cele/pdf/Policy_Paper_Derecho_al_Olvido.pdf (in Spanish)
- flip.org.co/es/content/corte-constitucional-colombiana-decide-sobre-caso-de-derecho-al-olvido-en-internet (in Spanish)

- www.fayerwayer.com/2015/01/ifai-busca-aplicar-el-derecho-al-olvido-a-google-mexico/ (in Spanish)

Discussion questions:

1. What are the risks when search engines are held responsible for information on web pages to which they facilitate access, but are not the authors?
2. Are there any cases in which “de-indexing” can be legitimate? What factors should be taken into account in determining these cases?
3. What criteria can be used to determine that certain content is not relevant, and could therefore be eliminated? Is it possible to claim that something that is not relevant at present may become so in future?

Case 3: Retention of communications data

In recent years, several Latin American countries have enacted laws obliging telecommunications and internet service providers to preserve, indiscriminately and en masse, data about the communications of all their users, arguing that this is justified by public security or national security interests.

Specifically, countries like Paraguay, Peru, Colombia and Mexico have proposed or implemented laws of this kind, obliging companies to store – for up to five years in the case of Colombia – data such as the phone numbers of callers and recipients, the date, time and duration of communications, and also the geographical location of communication devices.

Although these data, known as communications “metadata” or “traffic data”, do not include the content of communications, they do reveal highly sensitive information about individuals. Their analysis can disclose patterns of movement leading to knowledge about the social circles frequented by an individual, their political, religious or sexual preferences and their health status; overall, a fairly detailed map of a person’s activities can be constructed.

Some laws stipulate which authorities may access these data, in some cases even without a court order. The need for speedy investigation or the seriousness of threats to security are argued as reasons to dispense with judicial authorisation. On the other hand, it has been argued that lack of controls can lead to cases of abuse and impunity.

Information about this case:

- www.youtube.com/watch?v=iKccR3E6jn4 (in Spanish)
- www.digitalrightslac.net/en/la-retencion-de-datos-en-colombia-una-de-las-mas-largas-del-mundo/ (in English)
- www.digitalrightslac.net/es/la-retencion-de-datos-en-colombia-una-de-las-mas-largas-del-mundo/ (in Spanish)
- www.digitalrightslac.net/en/pyrawebs-archivo-digitalizado-del-terror/ (in English)
- www.digitalrightslac.net/es/pyrawebs-archivo-digitalizado-del-terror/ (in Spanish)
- www.derechosdigitales.org/9753/que-sigue-con-la-ley-telecom/ (in Spanish)
- www.hiperderecho.org/2015/07/norma-policia-geolocalizacion-sin-orden-judicial-1182/ (in Spanish)

Discussion questions:

1. Is mass, indiscriminate data retention disproportionate, or is it a necessary measure to protect the security of the population?
2. Should communications metadata be protected by law in the same way as the content of communications?
3. What measures should be adopted to prevent the authorities or other actors from abusing internet users' data to which they have access?

3. Questions for final group discussion

1. What should be the role of Inter-American Human Rights System bodies in the protection of human rights on the internet?
2. What should be the role of states in the protection of human rights on the internet?
3. What should be the role of companies in the protection of human rights on the internet?
4. How can human rights organisations use the internet to improve their work?