UNESCO's Comprehensive Study on Internet Related Issues

Submitted by :

Name: Anriette Esteryhusen

Gender: Female

Category of Stakeholder: A. civil society and NGOs including individual users

Country: South Africa

Region: Africa

1. What can be done to reinforce the right to seek and receive information in the online environment?

The freedom to seek and receive information online can be reinforced and supported in many ways. UNESCO Member States should, for example, explicitly endorse Human Rights Council Resolution HRC/20/8, which affirms that the same human rights people have offline must also be protected online. Member States should take steps to protect and promote human rights online, including freedom of expression and regular reporting on progress at UNESCO meetings.

APC is concerned that this survey question does not also highlight “the right to impart” information, which is a critical and often forgotten element of Article 19 of the ICCPR. APC has affirmed this in Article 4.1 of the APC Internet Rights Charter[1] as the right to share:

4.1 The right to share: The internet offers extraordinary opportunity for sharing information and knowledge, and for new forms of creating content, tools and applications. Providers of tools, internet services and content,should not prohibit people from utilising the internet for shared learning and content creation. Protection of the interests of creators must occur in a way consistent with open and free participation in scientific and cultural knowledge flows.

UNESCO Member States need to expressly recognise and respect the right to share components of the freedom to seek, receive and impart information. Taking positive steps to ensure open data policies, especially by Member States, and to ensure access to public information online is another way to reinforce freedom of expression online.

The right to seek, receive and impart information also intersects with women’s rights to freedom of expression and the right to be free from discrimination. Freedom of expression also intersects with sexual rights, such as the right to know about sexual and reproductive health and rights.

APC has developed a set of Feminist Principles of the Internet[2] with 15 principles that assert feminist views on positions related to internet and communication rights. For example, Principle

12 provides: “It is our inalienable right to choose, express, and experiment with our diverse sexualities on the internet. Anonymity enables this”. The Feminist Principles cover issues such as privacy and surveillance, diverse and inclusive participation in decision-making, open source technology, regulation of sexual content and online pornography.

These examples, the freedom to share, the right to receive information and women’s rights online, highlight that Member States must ensure protection of all forms of expression and the full range of diverse rights holders seeking to express themselves.

Sources:

[1] Association for Progressive Communications, Internet Rights Charter, https://www.apc.org/en/node/5677/

[2] Feminist Principles of the Internet, available at: http://www.genderit.org/articles/feminist-principles-internet

2. What mechanisms can develop policies and common standards for open-licensed educational resources and scientific repositories, and for the long-term preservation of digital heritage?

3. How can greater progress be made as regards inclusive strategies for women and girls as well as marginalized and disabled people?

An inclusive approach to infrastructure and development is critical for women and girls. Internet development remains male dominated, which means that women’s needs are not fully considered and integrated into online spaces. A massive push to teach women and girls to code, help women and girls to train for development careers and change the culture of tech companies can solve this problem.

Additionally, online violence must be recognised as violence. As such, it violates women’s human rights, including their rights to freedom of expression, access to culture and technology, etc. Concerns about freedom of expression rarely take into account women’s freedom of expression, which is restricted by technology-related violence. Offline violence also plays a major role in women’s limited access to the internet, as women need safe spaces to go online and anonymity and privacy to express themselves online or find the information they need without an abusive partner or relative finding out. Programs that understand the connection between online and offline gender-based violence and women’s access are necessary.

We have made some suggestions in relation to those marginalised on the grounds of race or ethnic or national origins below under question 10.

4. How can accessibility be facilitated through increases in locally produced and relevant content in different languages?

The value of ICT devices and of the internet to vulnerable and minority communities depend on their accessibility and on the ability of those in vulnerable and minority communities to access content which is relevant to them. Women's voices remain underrepresented on the internet. Initiatives to increase accessibility must include equality in women's access to ICTs, in all of its forms, by taking into account the differences in levels of access, opportunity and participation of women and men and addressing the disadvantages and barriers that women and girls experience in the knowledge.

Accessibility requires support and resources that meet the needs and lived realities of those speaking languages not well represented on the internet. Training and support to produce local content on websites such Wikipedia are important to develop a web of knowledge that is inclusive and accessible to all people. Locally produced and relevant content must also draw from those individuals that do not currently have access to the internet. Community radio is an important tool for reaching groups that do not participate in online knowledge-sharing.

5. What can be done to institutionalize Media and Information Literacy (MIL) effectively in national educational systems?

6. What are the current and emerging challenges relevant to freedom of expression online?

+Surveillance

The knowledge, or even the perception, of being surveilled can have a chilling effect. Online surveillance, security and privacy are concerns that have been central to human rights activists for years – but with the recent revelations by former National Security Agency (NSA) contractor Edward Snowden of United States (US) government spying on citizens, the issues have reached global attention.

APC's 2014 edition of Global Information Society Watch (GISWatch)[1] tracks the state of communications surveillance in 57 countries across the world – countries as diverse as Hungary, India, Argentina, the Gambia, Lebanon and the United Kingdom. Each country report approaches the issue from a different perspective. Some analyse legal frameworks that allow surveillance, others the role of businesses in collecting data (including marketing data on children), the potential of biometrics to violate rights, or the privacy challenges when implementing a centralised universal health system. The perspectives from long-time internet activists on surveillance are also recorded.

Using the 13 International Principles on the Application of Human Rights to Communications Surveillance[2] as a starting point, eight thematic reports frame the key issues at stake. These include discussions on what we mean by digital surveillance, the implications for a human rights agenda on surveillance, the "Five Eyes" inter-government surveillance network led by the US, cyber security, and the role of intermediaries.

These reports indicate how rampant government surveillance is across the world, and how business is often complicit in this. They suggest action steps that civil society can take to push for a human rights framework for internet governance – and to expose what until now has remained hidden.

+Real name policies for social media

In 2014, the social network created by Mark Zuckerberg suspended the profiles of drag queens whose pages were under their stage names. The performers suddenly found themselves blocked from their accounts and were sent messages with instructions on how to replace their stage names with their legal names, according to Facebook's "real name" policy. The right to anonymity has to be equally protected to create a safe online space for not only whistle blowers but any individual. Moreover, the gender perspective of anonymity has to be equally considered during every debate around surveillance and/or anonymity as it is largely women who feel watched over. From being unable to explore their sexuality to searching for something private on Google, they often feel watched, with the fear that their searches will be published without consent. Anonymity should be the default and identification a choice, as Robert Bodle from Internet Rights and Principles Coalition says. It is necessary in order to ensure the right to freedom of expression. [3]

+blocking of websites/content

Of those who are able to connect, the OpenNet Initiative estimates that nearly half of them

access a 'filtered' or censored internet of some kind, ranging from the filtering of illegal content

(such as child pornography) to restrictions on political speech, which is protected by the principles

of the Universal Declaration of Human Rights. By 2010, the OpenNet Initiative calculated that a

staggering half a billion internet users (or about 32%) experienced some form of national-level

restriction. As of 2011, more than forty-five states had placed restrictions on online content.

There is also evidence that governments are restricting access, or censoring content, from users

outside their countries using what is known as geolocational IP blocking.[4]

APC member organization VOICE, has noted that citizens are afraid to express themselves freely online because of the pervasive surveillance, filtering of content and criminalisation of free speech by the authorities.[5] In Pakistan, where Google has not yet developed a country-specific version of YouTube, the government responded to protests by blocking all access to the video sharing platform. In a statement on their blog, APC member Bytes for All Pakistan pointed out the dangers of using censorship as a tool to combat hateful online content: "'Innocence of Muslims' is not the first example of anti-Islam or anti-religious online content, and it won't be the last. It is impossible to filter and censor out millions of such opinions that may eventually result

in banning of all communication technologies and/or cripple critical infrastructure. In addition, such desperate attempts to ban disagreeable content only serves to draw attention towards it." Not only does censorship fail to deter acts of hateful expression online, it may in fact encourage further hatred and marginalisation.[6]

+Lack of infrastructure/affordable access

Ensuring continued extension of access for all to ICTs, particularly access to broadband,

especially in developing countries, and among marginalised communities in all countries, is critical for enabling freedom of expression globally. Yet millions of people still lack affordable and reliable

access to the necessary tools (e.g. smart phones or computers) and connectivity (internet infrastructure with sufficient and affordable bandwidth to enable them to make full use of the power of networks).

In many countries internet users are faced with slow broadband speeds, especially in areas outside

major cities, traffic caps may limit the amount of data that can be exchanged, and complex tariff

packages restrict competition or the user's ability to manage costs. Lack of choice of technologies and providers, along with limited public investment in infrastructure for remote and rural areas are the main causes of this. For those that cannot afford their own equipment and connectivity, public access facilities (e.g. in in public libraries) offer the only alternative, however, public investment in libraries, post offices, telecentres, and multi-purpose community centres is often limited.

At the industry level, internet providers often lack access to sufficient spectrum or competitively priced telecom infrastructure. In addition ISP licensing and content control may be too onerous for small or new market entrants, and interconnection regulations usually favour the dominant providers. A variety of indirect factors may also serve to limit internet accessibility; grid power may be unavailable, and high import duties may be levied on ICT equipment, which, along with luxury taxes on internet and voice services, further reduce their affordability.

+Cyberbullying/online violence against women

We see ongoing tension around balancing the sometimes competing rights of freedom of expression and women's empowerment. In particular we consider violence against women online as both a violation of women's rights and a barrier to women's freedom of expression.

The Internet has created a space for the expression of diverse experiences, needs and priorities by democratising information production, dissemination and journalism and overcoming the traditional gatekeeping role of the media and public institutions. In this respect, the internet plays a key role in countering negative stereotypes that perpetuate prejudice and discrimination. However violence against women and girls online - such as cyberstalking, cyberbullying, harassment and misogynist speech - limits their ability to take advantage of the opportunities

that ICTs provide for the full realisation of women's human rights, including freedom of expression. Just as violence is used to silence, control and keep women out of public spaces offline, women and girls' experiences online reflect the same pattern. Women human rights defenders face particular threats online including cyberstalking, violation of privacy, censorship and hacking of e-mail accounts, mobile phones and other electronic devices, with a view to discrediting them and/or inciting other violations and abuses against them.

As a consequence, women and girls self-censor, reduce participation or withdraw from platforms and technology they are using all together. In addition the normalisation of violent behaviour and the culture that tolerates violence against women that social media perpetuates and facilitates at rapid speed, works to reinforce sexist and violent attitudes, and contribute to norms and behaviour that makes online spaces hostile towards women.

+Sanctions on technologies

Sanctions regulating the export of technologies, such as U.S. sanctions on Cuba, Iran, and Sudan, represent considerable barriers to freedom of expression in these countries. Human rights defenders, journalists and activists, in particular, do not have access to specialised ICTs and new media tools. For example in Sudan, under United States sanctions on digital technology imposed in 1997, Sudanese cannot buy original software, nor can they have access training and courses online. This situation exposes civil society to serious security threats.[7]

+Other challenges relevant to freedom of expression online include attacks on websites, defamation laws, and right to be forgotten.

Sources:

[1] Global Information Society Watch 2014: Communications Surveillance in a Digital Age, http://giswatch.org/2014-communications-surveillance-digital-age

[2] 13 International Principles on the Application of Human Rights to Communications Surveillance, https://necessaryandproportionate.org/

[3] Facebook: The king laid bare and the drag queens, http://www.genderit.org/es/node/4173

[4] OpenNet Initiative, “Global Internet filtering in 2012 at a glance”, opennet.net/blog/2012/04/global-internet-filtering-2012-glance.

[5] Freedom of expression under threat in Bangladesh, https://www.apc.org/en/blog/freedom-expression-under-threat-bangladesh

[6] Policing expression online: hate speech, internet culture and online security, https://www.apc.org/en/blog/policing-expression-online-hate-speech-internet-cu

[7] Global Information Society Watch 2014, Sudan: Systematic violations of digital rights, http://giswatch.org/sites/default/files/systematic_violations_of_digital_rights.pdf

7. **How can legislation in a diverse range of fields which impacts on the Internet respect freedom of expression in line with international standards?**

An area of increasing tension relates to Member States' different approaches to application of international standards. On the one hand, human rights and freedoms are universal, inalienable, and indivisible. On the other hand, restrictions on freedom of expression vary widely among Member States. In an internet era, these variations are thrown into sharp relief and are causing frustration for rights holders. For example, individual rights holders increasingly connect as friends and family members and community participants in multiple countries and are frustrated that material which may be available to them in one country is not available in another. These different approaches often have the effect of driving circumvention.

We recommend that Member States:

+Stop the escalation of penalties for offences related to intellectual property, particularly for individual users.

+Develop and share best practice in using the rights based approach to balancing conflicting or competing rights.

8. **Is there a need for specific protections for freedom of expression for the Internet?**

In his 2011 annual report, UN Special Rapporteur, Frank La Rue, wrote "Unlike any other medium, the Internet enables individuals to seek, receive and impart information and ideas of all kinds instantaneously and inexpensively across national borders". The Internet uniquely enables the sharing of information across a diverse set of networks. For this reason, we see a need for specific protection of an open internet, one which ensures the free flow of information and which can be used to uphold all human rights, including freedom of expression.

9. **To what extent do laws protect digitally interfaced journalism and journalistic sources?**

10. **What are the optimum ways to deal with online hate speech? How can Media and Information Literacy empower users to understand and exercise freedom of expression on the Internet?**

In his 2014 annual report, the United Nations Special Rapporteur on contemporary forms of racism, racial discrimination, xenophobia, and related intolerance, Mutuma Ruteere, examined new information technologies, including the internet, for disseminating racist ideas, hate messages and inciting racial hatred and violence.[1] The report highlights the importance of affordable access to the internet and promotion of local content, particularly for those groups who are most often the targets of racial discrimination, in order to reduce information asymmetry and misperceptions that feed racist and xenophobic sentiment. It also highlights the fundamental role of education and media literacy, especially for young people. Recognising the

importance of strong movements to counter racism and intolerance online, the Special Rapporteur suggests: “Community ownership of infrastructure, training in network and content management, and alternative software use, including free and open software, can help to bridge existing gaps in knowledge and access.”

APC member Bytes for All, Pakistan, has conducted research on hate speech online in the country[2], based on a survey of internet users and content analysis of published information. The research found that hate speech on top Facebook and Twitter accounts that could fall under criminal offence based on the study’s definitions was negligible (less than 1%), suggesting that a solution to the problem does not lie in greater state action in catching and prosecuting individuals/groups, or through bans, but through alternate means.

One alternative is encouraging ISPs and platforms to adopt human rights-based approaches and have clear definitions of hate speech and what will not be tolerated in their terms of service and community guidelines. APC's End VAW research shows that ISPs and social media platforms currently deal ineffectively with gender-based hate speech and harassment and do not have clear policies around these issues.

[1] Access to the internet, community-owned infrastructure and open source software linked to combating racism, UN report says, https://www.apc.org/en/news/access-internet-community-owned-infrastructure-and

[2] https://content.bytesforall.pk/node/134

11. What are the optimum systems for independent self-regulation by journalistic actors and intermediaries in cyberspace?

APC has been working with members and project partners in the Africa region to examine intermediary liability and the different models in South Africa, Kenya, Senegal, Uganda and Nigeria.[1] Our findings suggest that models of self-regulation and mixed models (with self-regulation combined with some legal frameworks) vary widely[2], with negative impacts on freedom of expression and other rights and freedoms[3]. To address this, we have encouraged sharing of law drafting best practice among lawyers, journalists, government, private sector and civil society groups.

We supported the UNESCO research into intermediary liability and strongly recommend UNESCO develop clear guidance for Member States on principles for the policy in relation to intermediary liability.

[1] Intermediary Liability, http://www.apc.org/en/irhr/intermediary-liability/about

[2] Intermediary Liability in Africa: Baseline studies and summary report (2012), https://www.apc.org/en/node/15623/

[3] Alex Comninos, the liability of internet intermediaries in Nigeria, Kenya, South Africa and Uganda: An uncertain terrain (APC, 2012, available at: http://www.apc.org/en/node/15649/

12. What principles should ensure respect for the right to privacy?

In light of the 2014 report of the High Commissioner for Human Rights on the right to privacy in the digital age, we have taken questions in section C as a whole and make the following response.

The guiding framework for principles to ensure respect for privacy must be those found in core United Nations human rights standards. The High Commissioner reiterates that the right to privacy is a universal right[1], and interferences with the right conferring responsibilities on Member States regardless of the territory on which these interferences occur or the nationality of the person whose rights are infringed.

We note the recent General Assembly resolution on the right to privacy[2] and recommend that UNESCO:

(a) Support establishment of a dedicated special procedures mandate on the right to privacy, to ensure that the right to privacy is given meaning and practical application in the light of technological advancements.

(b) Issuance by the Human Rights Committee of a new General Comment on the right to privacy, to replace General Comment 16 (1988).

(c) Renewed protection for whistleblowers and human rights defenders who seek to uphold their human rights, including the right to privacy, in the context of digital communications.

Civil society groups have worked with legal experts and other stakeholders to developed a set of 13 principles to guide policy makers and law enforcement officers in the area of search, surveillance online. These principles simply reiterate the call for any intereference with the right to privacy to be necessary, proportionate and in accordance with the rule of law: www.necessaryandproportionate.org

[1] The right to privacy in the digital age Report of the Office of the United Nations High Commissioner for Human Rights, http://www.ohchr.org/Documents/Issues/DigitalAge/A-HRC-27-37_en.doc

[2] Resolution adopted by the General Assembly on 18 December 2013, http://www.un.org/en/ga/search/view_doc.asp?symbol=A/RES/68/167

13. What is the relationship between privacy, anonymity and encryption?

14. What is the importance of transparency around limitations of privacy?

15. What kinds of arrangements can help to safeguard the exercise of privacy in relation to other rights?

16. **How can openness and transparency of data be reconciled with privacy?**

17. **What may be the impact of issues relating to big data on respect for privacy?**

18. **How can security of personal data be enhanced?**

19. **How can Media and Information Literacy be developed to assist individuals to protect their privacy?**

20. **How can ethical principles based on international human rights advance accessibility, openness, and multi-stakeholder participation on the Internet?**

21. **What conceptual frameworks or processes of inquiry could serve to analyse, assess, and thereby inform the choices that confront stakeholders in the new social uses and applications of information and knowledge?**

22. **How does ethical consideration relate to gender dimensions of the Internet?**

23. **How can ethics, - i.e. the simultaneous affirmation of human rights, peace, equity, and justice - inform law and regulation about the Internet?**

24. **What international, regional and national frameworks, normative guidelines and accountability mechanisms exist of relevance to one or more fields of the study?**

25. **How do cross-jurisdictional issues operate with regard to freedom of expression and privacy?**

26. **What are the intersections between the fields of study: for example, between access and freedom of expression; ethics and privacy; privacy and freedom of expression; and between all four elements?**

27. What pertinent information materials exist that cut across or which are relevant to the four fields of the study?

28. What might be the options for role of UNESCO within the wider UN system in regard to the distinct issues of online Access to information and knowledge, Freedom of Expression, Privacy and Ethical dimensions of the information society?

+Continued leadership on these issues through the WSIS review

+Work more closely with OHCHR, the special procedures, and the HRC on these issues.

29. What might be options for the role of UNESCO in relation to stakeholders outside the UN system?

30. For each study field, what specific options might UNESCO Member States consider?