



INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Human Rights and the Internet

Mami Talukdar

Ex- Assistant Professor, Deptt. Of Assamese, B. H. College, Howly

Abstract:

The internet has given citizens across the world enhanced opportunities to communicate in the public domain, breaking down commercial, social and geographical boundaries to communication. Outlining human rights is controversial enough in the physical world; on the Internet, defining rights is even more of an ambiguous task. Issues of human rights on the Internet are extremely nebulous given the size, scope, and borderless nature of the Internet world, which has no pre-set guardians, laws, or norms -a virtual no man's land. In India, according to the 2011 census, 6.3 percent of the total population had access to computers or laptops within the household. Half of those with computers or laptops had internet access, and many more citizens had access to the internet through cyber cafes and mobile telephones. The main purpose of this paper is to explore key trends and challenges to the right of all individuals to seek, receive and impart information and ideas through the Internet.

Keywords: Internet, Communication, Cyber, Computer.

Introduction

The internet offers enormous opportunity for people around the world to exercise their rights to free expression and free association, but access to the Internet must become truly universal. By greatly enhancing the possibilities for inexpensive and global communication, the internet allows for networking, organizing and information sharing on a scale never before possible. The internet also interacts with traditional media, becoming a forum for retransmitting communication, often through third parties (mirroring). In many countries, the internet can be used to overcome press censorship.¹

The internet is particularly important for human rights work. Human rights activists were among the first to make use of the internet to coordinate actions, make contacts and communicate privately, to post and domain information, to expose and publicize human rights violence, and to solicit action to address specific issues.

The internet has profound implication for governments to restrict freedom of expression and related human rights. Civil society organization can become more potent domestically, advancing rights and demanding accountability and transparency, and they will be linked to a global network of similar organizations.

Technology and the Human right

Related to this is debate over whether human rights should be interpreted extensively to include specific technologies (such as telecommunications or the internet). Generally speaking, human rights in the international instruments are expressed in broad conceptual terms which are not susceptible to change over time (e.g. fair trial, freedom from torture, freedom of conscience, education). The technologies which are most suitable for exercising and enforcing these generic rights change over time. In the case of freedom of expression, for example, print, radio, television, telephony and the internet have played varyingly significant roles at different times (and do today in different countries). Access to telecommunications has not usually been considered a ‘human right’ but universal access to telecommunications has been mandated by many governments through legislation and economic regulation. A recent article by the internet pioneer Vint Cerf,⁶ in which he argued that the internet should be regarded as a constitutional right and an enabler of rights (a term also used by the UN Special Reporters) rather than as a human right per se, provoked considerable debate.⁷ One aspect of this is whether human rights should be considered fixed or mutable. As the technologies that enable rights vary over time, the explicit inclusion of those technologies in the text of human rights instruments would imply that the instruments themselves would also need to change over time – though extensive interpretations that treat technologies as necessary enablers of rights would not require this.

Access to the Internet and the necessary infrastructure

The Internet, as a medium by which the right to freedom of expression can be exercised, can only serve its purpose if States assume their commitment to develop effective policies to attain universal access to the Internet. Without concrete policies and plans of action, the Internet will become a technological tool that is accessible only to a certain elite while perpetrating the “digital divide”.

The term “digital divide” refers to the gap between people with effective access to digital and information technologies, in particular the Internet, and those with very limited or no access at all. In contrast to 71.6 Internet users per 100 inhabitants in developed States, there are only 21.1 Internet users per

100 inhabitants in developing States³. This disparity is starker in the African region, with only 9.6 users per 100 inhabitants. In addition, digital divides also exist along wealth, gender, geographical and social lines within States. Indeed, with wealth being one of the significant factors in determining who can access information communication technologies, Internet access is likely to be concentrated among socioeconomic elites, particularly in countries where Internet penetration is low. In addition, people in rural areas are often confronted with obstacles to Internet access, such as lack of technological availability, slower Internet connection, and/or higher costs.

Restriction of content on the Internet

A restriction on the right of individuals to express themselves through the Internet can take various forms, from technical measures to prevent access to certain content, such as blocking and filtering, to inadequate guarantees of the right to privacy and protection of personal data, which inhibit the dissemination of opinions and information.

- 1. Arbitrary blocking or filtering of content:** Blocking refers to measures taken to prevent certain content from reaching an end-user. This includes preventing users from accessing specific websites, Internet Protocol (IP) addresses, domain name extensions, the taking down of websites from the web server where they are hosted, or using filtering technologies to exclude pages containing keywords or other specific content from appearing. For example, several countries continue to block access to YouTube, a video-sharing website on which users can upload, share and view videos.
- 2. Criminalization of legitimate expression:** The types of action taken by States to limit the dissemination of content online not only include measures to prevent information from reaching the end-user, but also direct targeting of those who seek, receive and impart politically sensitive information via the Internet. Physically silencing criticism or dissent through arbitrary arrests and detention, enforced disappearance, harassment and intimidation is an old phenomenon, and also applies to Internet users

One clear example of criminalizing legitimate expression is the imprisonment of bloggers around the world. According to Reporters without Borders, in 2010, 109 bloggers were in prison on charges related to the content of their online expression.⁶ Seventy-two individuals were imprisoned in China alone, followed by Viet Nam and Iran, with 17 and 13 persons respectively.⁵

- 3. Imposition of intermediary liability:** One of the unique features of the Internet is that the way in which information is transmitted largely depends on intermediaries, or private corporations which provide services and platforms that facilitate online communication or transactions between third parties, including giving access to, hosting, transmitting and indexing content.⁵ Intermediaries thus range from Internet service providers (ISPs) to search engines, and from blogging services to online community platforms. With the advent of Web 2.0 services,⁸ individuals can now publish information

without the centralized gateway of editorial review common in traditional publication formats. The range of services offered by intermediaries has flourished over the past decade, mainly due to the legal protection that they have enjoyed from liability for third-party content that Internet users send via their services.

Many States have adopted laws which impose liability upon intermediaries if they do not filter, remove or block content generated by users which is deemed illegal. For example, in Turkey, Law 5651 on the Prevention of Crime Committed in the Information Technology Domain, which was enacted in 2007, imposes new obligations on content providers, ISPs and website hosts.⁴

- 4. Disconnecting users from Internet access, including on the basis of violations of intellectual property rights law:** While blocking and filtering measures deny access to certain content on the Internet, States have also taken measures to cut off access to the Internet entirely. This includes legislation based on the concept of “graduated response”, which imposes a series of penalties on copyright infringers that could lead to suspension of Internet service, such as the so-called “three strikes-law” in France⁸ and the Digital Economy Act 2010 of the United Kingdom.⁹ Beyond the national level, the Anti-Counterfeiting Trade Agreement (ACTA) has been proposed as a multilateral agreement to establish international standards on intellectual property rights enforcement.
- 5. Cyber-attacks:** Cyber-attacks, or attempts to undermine or compromise the function of a computer based system, include measures such as hacking into accounts or computer networks, and often take the form of distributed denial of service (DDoS) attacks. During such attacks, a group of computers is used to inundate a web server where the targeted website is hosted with requests, and as a result, the targeted website crashes and becomes inaccessible for a certain period of time.¹⁰ As with timed blocking, such attacks are sometimes undertaken during key political moments. When a cyber-attack can be attributed to the State, it clearly constitutes inter alia a violation of its obligation to respect the right to freedom of opinion and expression. Although determining the origin of cyber-attacks and the identity of the perpetrator is often technically difficult, it should be noted that States have an obligation to protect individuals against interference by third parties that undermines the enjoyment of the right to freedom of opinion and expression.¹²
- 6. Inadequate protection of the right to privacy and data protection:** The right to privacy is essential for individuals to express themselves freely. Indeed, throughout history, people’s willingness to engage in debate on controversial subjects in the public sphere has always been linked to possibilities for doing so anonymously.¹¹ The Internet allows individuals to access information and to engage in public debate without having to reveal their real identities, for example through the use of pseudonyms on message boards and chat forums. Yet, at the same time, the Internet also presents new tools and mechanisms through which both State and private actors can monitor and collect information about individuals’ communications and activities on the Internet. Such practices can constitute a violation of the Internet

users' right to privacy, and, by undermining people's confidence and security on the Internet, impede the free flow of information and ideas online.¹³

Conclusion

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. By vastly expanding the capacity of individuals to enjoy their right to freedom of opinion and expression, which is an "enabler" of other human rights, the Internet boosts economic, social and political development, and contributes to the progress of humankind as a whole.

This is particularly important as the medium becomes the dominant mode of communication, exchange of thought, and commerce. Internet as a human right serves as a tool, an instrument with which people can work and fight to achieve their other economic, social, cultural, civil, and political rights. It deserves the respect accorded to other human rights and other media.

References:

1. Internet Society. "A Brief History of the Internet". <http://www.internetsociety.org/internet/whatinternet/history-internet/brief-history-nternet>.
2. Internet Encyclopedia of Philosophy, The Golden Rule, 2010 <http://www.iep.utm.edu/goldrule/> (Access December 2013).
3. UN Doc. Doc. A/HRC/20/L.13. Human Rights Council, "The promotion, protection and enjoyment of human rights on the Internet", 29 June 2012, para.1.
4. Office of the High Commissioner for Human Rights. "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue." Report for the Human Rights Council 17th Session. May 16, 2011. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf.
5. "Four in five regard Internet access as a fundamental right: global poll," BBC News, 8 March 2010. Available from: http://news.bbc.co.uk/1/shared/bsp/hi/pdfs/08_03_10_BBC_internet_poll.pdf.
6. Access denied: the practice and policy of global internet filtering 276 (ronald deibert et al., eds. 2008) [hereafter access denied].
7. UN Administrative Committee on Coordination. 1997. ACC Statement on Universal Access to Basic Communication and Information. <http://www.unites.org/html/resource/acc1997.htm>.
8. Jeff Jarvis 'A Bill of Rights in Cyberspace', 27 March 2010, <http://buzzmachine.com/2010/03/27/a-bill-of-rights-in-cyberspace/> (Access December 2013).
9. Michael Fromkin 'Habermas@Discourse. Net: Toward a Critical Theory of Cyberspace' (2003) 116 Harvard Law Review, 749-873.

10. Internet Governance Forum, <http://www.intgovforum.org/> (Access December 2013).
11. John Arquilla and David Ronfeldt, 'Cyberwar is Coming!' (1993) 12 Comparative Strategy, 141-165.
12. Irina Netchaeva 'E-Government and E-Democracy. A Comparison of Opportunities in the North and South'(2002) 64 The International Journal for Communications Studies 467-477.
13. UN Doc. A/C.3/68/L.45. General Assembly, 'The right to privacy in the digital age', 1 November 2013.

