Unit 7: Rights in Cyberspace

Welcome to Week 7.

This week's learning explores human rights in the context of the cyberspace. You will investigate issues concerning the tension between competing interests, and the need to find a balance between rights such as the right to privacy and the right of freedom of expression. You will critically consider whether these rights have any meaning in a digital landscape, and whether when we put something 'out there' do we lose ownership of it. Finally, you will investigate the effects and efficiency of the Data Protection legislation in ensuring compliance (The GDPR will be discussed in the relevant lecturecast).

On completion of this unit you will be able to:

- Explore issues concerning breaches of rights.
- Assess the extent the criminal justice system can reach a balance between competing rights.
- Practice research skills.
- Apply critical assessment.

Human Rights in Cyber Space:

Protection of human rights in cyberspace is a new area of law that is mostly uncharted. In accordance with Article 19(2) of the International Covenant on Civil and Political Rights, the United Nations Human Rights Council (UNHRC) has said that people have the right to receive and share information, ideas, and opinions over the internet as part of their freedom of expression and information rights (ICCPR) (UNITED NATIONS, 1966).

The International Covenant on Civil and Political Rights (ICCPR) says in Article that: The actual use of the right given in paragraph 2 of this article comes with a unique set of duties and responsibilities for each person. As a result, it may be subject to several restrictions, but those restrictions should only be those that are required by law:

a) Out of respect for other people's property rights and good names
b) To protect national security, public order, public health and morals, or public health and morals (UNITED NATIONS, 1966).

A Human Rights Commission (HRC) statement says that people's rights in the real world must also be protected online (mentioning freedom of expression) (Team, 2015).

1. **Public Privacy**
   Freedom of speech and access to information online are two sides of the same coin known as "public privacy," which also includes safeguarding individuals' private data online. The ability to use the internet as a personal service tool without worrying that third parties would get access to and use one's data in a variety of

ways without one's permission is what is meant by "privacy" in the context of the internet and cyberspace (*Mihr, A., 2013)*.

The right to freedom, which includes the right to free speech, is protected by a number of international agreements. This freedom involves the unrestricted expression of one's opinions and the open flow of information and ideas. It also includes the liberty to say what one wants; however, one wants to say it, which includes the freedom to share one's thoughts and opinions through the many online mediums available today. The right to engage in political conversation is protected by Right, particularly when doing so brings up issues of paramount public importance (*Mihr, A., 2013)*.

Most democracies have embraced the Internet for commercial and communication reasons, and this has resulted in a degree of protection for political expression online. There are countries that have strict regulations in place to ensure that their citizens' personal information online is safe. The potential for private information to be misused and exploited because of these international accords has serious implications for a variety of basic freedoms and rights. Governments must find a middle ground between business as usual and laws that protect people's privacy and personal liberties (*Mihr, A., 2013)*.

2. Governance in cyberspace

According to German political scientist Anja Mihr, despite the lack of a central authority, legislative bodies, law enforcement, or any other type of constitution, cyberspace is home to more people than any other nation in the world. Without these safeguards, it will be harder for citizens to exercise their rights. The United Nations (UN), Organization of American States (OAS), African Union (AU), and European Union (EU), among others, are IGOs with the stated goal of establishing international standards for the use of cyberspace and the Internet, to be enforced by national governments. It's an issue that the state's power and the methods it uses to enforce its laws are limited to inside its boundaries.

Cyberspace lacks boundaries, hence appropriate legislation has yet to be established. Problems arise because of the lack of clarity about online jurisdiction, which makes it simpler for criminals to move across national borders (Fanchiotti. *Et. al., 2012)*. It's likely that if a governing regime were to be developed, it would include a wide range of national, international, commercial, and individual interests and players, including those that represent enterprises, social networks, NGOs, and people.

3. Liability of Internet service providers

When people's most fundamental political and civil liberties are threatened, it's time to be concerned. Should the first infringer face all responsibility, or should the ISP also be held liable if their service was used to commit an infringement? This is an essential question to consider since it pertains to striking a balance between free expression and the right not to be slandered (Mansell, 2004). Individuals and their

reputations are more at risk due to the Internet's rising speed and its potentially endless audience.

Internet service providers (ISPs) may not be aware that their website hosts a defamatory comment because they lack the resources necessary to monitor the information published on their websites.

As shown in Cubby, Inc. v. CompuServe, Inc. (Smiley, 2017) the ISP is not responsible for the content of messages posted on its bulletin board since it is only serving as a distributor. In contrast, the New York Supreme Court decided in Stratton Oakmont, Inc. v. Prodigy Services Co. (Smiley, 2017) that Prodigy was responsible for the plaintiff's damages because it had functioned as a publisher with an editorial role. These occurrences shed light on the grey areas of ISP accountability.

Another issue that has to be addressed is whether or not ISPs will act as "moral guardians" in cyberspace. Overzealous Internet service providers (ISPs) might threaten online free speech if they began refusing to serve controversial websites. On the other hand, if ISP responsibility is unclear, it might mean that providers are willing to ignore the consequences of hosting bad information.

4. Cybersecurity

Sensitive private information should not be stored on the World Wide Web (WWW) because to the presence of hackers, viruses, and zero-day attacks (Nohe, 2018). While the Internet provides a platform on which people may express their right to freedom, it is not a guarantee that we will always be so (Mihr, A., 2013). About 2.5 billion people are now connected to the web. Since everyone these days leaves digital trail, it's crucial that the internet's safety be maintained.

More individuals than ever before feel the same way about protecting their privacy and the right to free speech, and as a result, they have similar views about how to do it (Mihr, A., 2013).

Most governments restrict Internet freedom, with certain nations being more restrictive than others, as seen by the 2013 Freedom in the Net Index (*Index.,* 2015). The countries are likely to use a wide variety of strategies. Take, as an example, the concept of cyber police. To prevent or limit someone's right to freedom, one may use any number of techniques.

Several filtering initiatives, such as NETprotect I and II, ICRAsafe, and the PRINCIP program, have been supported by the European Union *(Shaping Europe's digital future).* It has been argued that the largest danger to the liberties enjoyed by Internet users comes from the users' own reluctance to speak freely online. The combination of pervasive monitoring and the anticipation of having one's private conversations broadcast leads to an increase in self-censorship. People nowadays don't share their own ideas or thoughts through Google or social media. Because certain words may alert national security agencies, the Internet may be used as a tool for political manipulation.

Discriminatory behaviors and perspectives

1. **Cyber bullying**
   It is possible to see discriminating behaviors both offline and online. Cyberbullying refers to one of the behaviors. At least one out of ten students in Australia are victims of cyberbullying. The right to the greatest achievable quality of bodily and mental health; the right to work and fair working conditions; the right to freedom of speech and the right to hold ideas without interference; the right to leisure and recreation for children and young people. Cyberbullying may affect several human rights, including: (Moses, 2012).

2. **Cyber-racism**
   People may exhibit racism online by posting racist statements or by joining group websites that have been built for the express purpose of being racist. A Facebook page named "Aboriginal memes" served as an example that garnered considerable attention. It included many images of indigenous people and harsh comments. Facebook classed the page as "controversial comedy," as claimed (Moses, 2012).

3. **Hate speech**
   As stated in Article 20 of the International Covenant on Civil and Political Rights, any advocacy of national, racial, or religious hatred that constitutes incitement to discrimination, hostility, or violence shall be criminalized (ICCPR) (UNITED NATIONS, 1966b). Remarks made about a group of people based on their sexual orientation, nationality, color, or ethnicity that are derogatory might instigate acts of violence or prejudice against those members of the group. Cyberspace has also been used for harmful purposes in this way.

Future of human rights in the Digital Age

Future events concerning human rights in cyberspace will be determined by the evolution of the law and the way in which it is interpreted by national and international governing bodies. Jon Bing warns that it is very difficult to bring electronic rules and regulations via the judicial review process. According to Bing, we now live in a period where "technology is carrying out the law".

Roger Brownsword advocates adopting a utilitarian pragmatic attitude, a defense of human rights, and a "dignitarian coalition" in relation to challenges raised by biotechnology and human rights advancements in addition to those raised by digital technologies. Brownsword highlighted some of the concerns that have been raised by these changes in addition to those raised by digital technology. Brownsword asserts that the first two of the three perspectives are popular in the United Kingdom, claiming that technologies are being created that treat human beings as though they lacked autonomy and the ability to make independent decisions. Brownsword is alluding to the reality that

technologies are being created that treat human beings as though they lack the ability to make independent decisions.

What the future holds for cyberspace has been the subject of recent government discussions. In the month of April 2008, the Virtual Law Conference (Hoffman, 1998) was held in New York. At addition to Disney's Walt Disney Company, Microsoft and Sony also participated in the conference. The seminar was supposed to explore the enforcement of intellectual property rights, legal problems coming from virtual money, legal issues originating from virtual property, ethical considerations for lawyers and executives working in virtual worlds, and how to litigate a virtual case.

The purpose of the United States Congressional Hearing on Virtual Worlds was to inform the public and investigate the possibilities of virtual worlds. Among the topics on the agenda were consumer protection, intellectual property protection, and the protection of minors. This hearing, which occurred earlier today, was among the early legislative investigations into virtual worlds. It is now unclear which of these events, if any, will have any lasting impact on the sector, which continues to progress rapidly alongside new technical advances.

During a discussion on cybersecurity held on May 22, 2020, the United Nations Security Council stressed how crucial it is to recognize that cyberattacks constitute a human rights issue. The course of action suggested that operations such as Internet shutdowns by the government and hacking into the electronic devices of dissidents might result in serious breaches of human rights. At least a dozen more countries, including Estonia, Belgium, the Netherlands, Ecuador, Japan, and Switzerland, supported the idea (Brown, 2020).

References:

Brown, D. (2020, May 26). It’s Time to Treat Cybersecurity as a Human Rights Issue. Human Rights Watch. https://www.hrw.org/news/2020/05/26/its-time-treat-cybersecurity-human-rights-issue

Fanchiotti, Vittoriio; Pierini, Jean Paul (2012). "Impact of Cyberspace on Human Rights and Democracy":

Global Broadband and Mobile Performance Data Compiled by Ookla | Net Index. (2015, May 29). Web.archive.org. https://web.archive.org/web/20150529015231/http://www.netindex.com/

Hoffman, C. (1998). Christopher Hoffmann. Www.lawyer.com. https://www.lawyer.com/christopher-hoffmann-mo.html

Mansell, R. (2004). Human rights in the digital age (pp. 1–10). Glasshouse Books. http://eprints.lse.ac.uk/3707/1/Introduction%E2%80%93Human_Rights_and_Equity_in_Cyberspace_%28LSERO%29.pdf

Mihr, Anja (2013). "Public Privacy Human Rights in Cyberspace" (PDF).

Moses. (2012, August 8). Contents removed from racist Facebook page. The Sydney Morning Herald; The Sydney Morning Herald. https://www.smh.com.au/technology/contents-removed-from-racist-facebook--page-20120808-23tr1.html

Nohe, P. (2018, January 31). Cybercrime at Super Bowl LII - How not to get Hacked. Hashed out by the SSL StoreTM. https://www.thesslstore.com/blog/cybercrime-super-bowl-lii-not-get-hacked/

Shaping Europe's digital future | Shaping Europe's digital future. (n.d.). Digital-Strategy.ec.europa.eu. https://digital-strategy.ec.europa.eu/en

Smiley, S. (2017, September 8). Australians' financial information at risk in data breach of US company. ABC News. https://www.abc.net.au/news/2017-09-08/smiley-credit-check-australians-financial-information-at-risk/8887198

Team, O. (2015). ODS HOME PAGE. Documents-Dds-Ny.un.org. https://documents-dds-ny.un.org/doc/RESOLUTION/GEN/G12/153/25/PDF/G1215325.pdf

UNITED NATIONS. (1966, December 16). International Covenant on Civil and Political Rights. OHCHR. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights

UNITED NATIONS. (1966b, December 16). International Covenant on Civil and Political Rights. OHCHR. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights