Accelerating efforts to tackle online and technology-facilitated violence against women and girls

Committee: CSW

Student Officer: Elle Chassin & Daan de Klein

Forum: Commission on the Status of Women (CSW)

Issue: Accelerating efforts to tackle online and technology-facilitated violence against women and girls

Name: Elle Chassin & Daan de Klein

Position: Head Chair & Deputy Chair

Introduction

Every day, the internet becomes a bigger part of our daily lives. 64% of the world's population uses the internet, making them both aware and unaware consumers of constant advertising, cookies, and much more. Prior to the year 2000, when "The Year 2000" software problem or the millennium bug first surfaced, the majority of people did not particularly notice any security risks associated with using the internet. Even while the issue was not as serious as initially predicted, it did cause people to question the internet's actual level of safety. It became clear that cyberspace and software could be easily manipulated and misused. Cyberviolence has become an even bigger concern around the world, especially since the Covid-19 pandemic. This violence frequently targets women and girls and is gender-based. The full realization of gender equality is hampered by cyber violence, which also infringes on women's rights. Through many, many platforms, predators, violent individuals, and human traffickers can influence and get their hands on both young girls and women. Violence against women including in an online environment can take many forms: cyber harassment, revenge porn, threats of rape, and can go as far as sexual assault or murder. "Violence and abuse online may limit women's right to express themselves equally, freely, and without fear. Cyberviolence affects women disproportionately, causing them psychological harm and suffering and deterring them from digital participation in political, social, and cultural life." (Council of Europe) The internet is a huge place and exists ubiquitously throughout the world. Because of this, the Commission on the Status of Women must find a solution for this problem in every member state to protect and help innocent women and girls.

Definition of Key Terms

Algorithm

An algorithm is a set of rules and signals that automatically ranks content on a social platform based on how likely each individual social media user is to like it and interact with it

CSAM

Child sexual abuse material. This material is widely found online, and in 2021, there were over 29 million reports of it. It is often found in the form of child pornography, and other forms of child abuse.

Cyberviolence

Cyber violence is defined as; “The use of computer systems to cause, facilitate, or threaten violence against individuals, that results in (or is likely to result in) physical, sexual, psychological or economic harm or suffering and may include the exploitation of the individual's circumstance, characteristics or vulnerabilities." (COE)

Grooming

Grooming is the attempt to become close to a child or young person with the goal of sexually assaulting them or persuading them to commit a crime, such as buying or selling drugs or joining a terrorist group.

ICT

ICT means “information and communication technology” and includes all forms of media, platforms, and applications accessed by digital means, such as the Internet and digital telecommunications. (UN Women)

ICT VAWG

ICT VAWG refers to acts of violence against women and girls (VAWG) committed in part or fully through ICT.

Online harassment of women/Cybersexism

These terms are used interchangeably and refer to online participation in sexism. Although cyber sexism is sexism in general, the majority of the time this sexism is against women and girls.

Perpetrators

Online violence towards women is often done by individual persons, who could be partners or ex-partners, colleagues, schoolmates, or, as is often the case, anonymous individuals.

Trafficking

Human trafficking includes recruiting, transporting or receiving and housing human beings through the use of force, for the purpose of exploiting them. (Dutch Government)

General Overview

Hate Speech

There is no set legal definition for hate speech. This implies that each social media site has a distinct definition of online. However, hate speech is often defined as language or imagery that disparages, insults, targets, or threatens a person or group of people because of their identity, including gender, race, color, religion, national origin, sexual orientation, handicap, or other characteristics. Hate speech typically uses words, actions, and the use of imagery to intentionally disgrace, annoy, terrify, embarrass, humiliate, disparage, or threaten another person. It typically has specific, discriminating harms that have historical roots. The majority of legal definitions of harassment take the harasser's purpose into account. The use of the Internet, electronic devices, and mobile applications for these goals as cyber harassment, however, prevents this from translating in a constructive way. In the instance of harassment

and abuse made possible by technology, the intent might be challenging to establish and decipher. For instance, the majority of laws do not currently define harassment as communications with a third party. Therefore, while sending someone a threatening message for extortion purposes is allowed, the non-consensual sharing of sexual photos with someone who is not the subject of the photograph is not considered to be legal or hateful.

Platforms

Promoting violence

In order to draw users and keep them on their platforms for as long as possible, social media platforms use algorithms that prey on the weakest parts of human nature. The majority of platforms make their money primarily through advertising, therefore increasing user activity also means better earnings. Facebook leaker Frances Haugen claims that social media sites base their decisions about what content to show users in their newsfeeds on the kinds of stuff they have previously liked, shared, or remarked on. These measures favor the display of violent, inflammatory, and upsetting content, which is why it is more frequently shown than benign stuff. “Repeated exposure to violence in the media is widely known to have a desensitizing effect on children and youth. As the sight of violence becomes normalized, it becomes less upsetting, and a lack of empathy can develop.” (Social Media Victims Law Center)

Common platforms

The most common platforms for predators to use are Facebook, Instagram, online gaming sites, and other forum/messaging platforms. Instagram is the most common for grooming, while Facebook is very commonly used for trafficking. It is illegal under internet harassment legislation to use the internet to harass, threaten, stalk, intimidate, or otherwise distress a person. Internet harassment laws are in place to shield potential victims from the trauma of cyberstalking, cyberbullying, and other types of internet harassment. Legislation and enforcement differ from one jurisdiction to the next,

because there are different laws in each member state. States with less laws against internet harassment etc, generally have higher rates of it. However, more legislation against the issue can have two main effects. The first is that it goes down, as potential perpetrators are scared of the implications of their actions. The second is that perpetrators find ways around the laws, and ways to stay under the governmental eye.

Anonymity and Fake Accounts

Anonymity grants people the ability to take actions that aren't associated with their name, or identity. Since there is no real public accountability for their activities, they feel comfortable propagating their messages of abuse online. Because anyone can create a social presence online and there is nothing forcing the individual to fill out truthful, personal information when creating the account, many, many fake accounts are created. Sometimes, fake accounts can be harmless, but in other cases, they are used to catfish other unknowing victims. Catfishing can lead to financial fraud, sextortion, and predatory sexual behavior toward adults and minors.

Human Trafficking

Human trafficking is the exploitation of human beings for labor or sexual purposes. It is very often facilitated through social media. A $150 billion global industry, human trafficking denies freedom to 25 million individuals worldwide. Social media has been used by traffickers to recruit victims, expand their trafficking operations, and control victims online by limiting their access to social media, posing as the victim, or spreading rumors about them. Over half of all online recruiting occurs through Facebook. Facebook is aware of its role but has yet to take meaningful action. Facebook and other social media platforms are used because that is where lots of children are found.

"There is no typical case of human trafficking, which often overlaps with other closely related crimes, such as human smuggling, prostitution, intimate partner violence, and child abuse."

— Report of the Task Force on Trafficking Women and Girls

Risk Factors for Vulnerability to Trafficking - by the American Psychological Association

- Factors that undermine the ability to protect oneself or that disrupt connections to social and family support increase susceptibility to coercion.
- Variables that contribute to a person's vulnerability to being trafficked include membership in a marginalized group; prior victimization and trauma; disabilities; immigrant or refugee status; and family disruption. These may be magnified by globalization, poverty, political instability and war.

Scar trafficking victims can have

- Mental health problems can arise such as anxiety, depression, suicidal thoughts, addiction, PTSD, and many more.
- Physical symptoms include neurological issues, brain injuries, bodily issues, STIs, and many more.

Constitutions in Democratic Countries

As stated in the UDHR and the ICCPR, freedom of speech and expression in democratic nations is regarded as a fundamental human right and has a significant impact on society. However, democratic nations typically enforce regulations to prevent the exploitation of this privilege because it is particularly "sensitive" and can be construed quite subjectively. For instance, the constitution of the United States forbids the introduction of legislation that restricts freedom of speech and expression (see important parties concerned). Because many people view this subject as inappropriate, the Communications Decency Act (CDA) of 1996 made an effort to

regulate pornography on the Internet. Due to legal concerns about restrictions on free expression, this statute underwent numerous revisions. The Child Internet Protection Act (CIPA), among other laws, contains limitations on pornography today. This demonstrates that, despite fully supporting the human right to freedom of expression, democratic nations frequently employ filtering techniques to control the content that they believe to be abusing this right.

Algorithms and Extremism

In the last ten years, social media has developed from being a place where you interact with your friends and family and people you know in real life to a place where you are mostly recommended content from strangers. This shift in the way social media work started back in 2016 when the Chinese company Byte Dance adopted their Chinese app Douyin to the western market with the name Tik Tok. TikTok was fundamentally different from traditional social media. When you open the app for the first time, instead of choosing interest and following accounts you might like, you are immediately presented with an infinitely long feed of videos you might like. TikTok picks up on behavior like rewatching videos, liking videos, and a multitude of other factors to psychoanalyze the viewer and recommend more videos they could be interested in. It is a common belief that these algorithms know more about you than you know about yourself. For example, Tik Tok's algorithm probably knows if you are pregnant before you know it or knows whether you will break up with your partner.

Social media apps exist not to entertain you, but first and foremost they exist to earn money. Social media apps mainly make money by advertising. Viewers are advertised by being shown paid content between posts. These advertisements can be pictures or videos. The app will earn more money if it shows you more advertisements. To do this it wants to keep you on the app for as long as possible, allowing it to show you more ads and earn more money. Algorithms for Tik Tok and the like are coded to hold your attention for as long as possible. These algorithms do this by exploiting your brain's reward system.

When we see something funny or interesting our brain releases dopamine, dopamine is a core part of the way humans feel pleasure. It allows us to think about and plan our actions and it allows us to find things interesting. Social media uses this reward system by showing us content that triggers this dopamine release. However, if we see only a continuous stream of videos that are constantly receiving dopamine, eventually our brain will become used to it, and we could close the app. To prevent this the algorithm will space out these good videos and fill the gaps with videos we may not like as much. This makes the viewer spend more time on the app as they are chasing their next hit of dopamine.

A way social media serves us content that will interest us and trigger our brain's reward system is by finding our interests and sending us into a rabbit hole about them. For example, some people might be sucked down into '*booktok*' because of their interests in books and others may be sucked down into DIY renovation videos; it sends us into a rabbit hole of what we are interested in. To keep us interested it will also make use of confirmation bias. Confirmation bias is a form of false optimism or wishful thinking. Confirmation bias is when we receive only evidence that supports our viewpoint and dismisses all other evidence denying it. This phenomenon can allow us to be sucked into an extremist community without us knowing.

Extremist groups know how to play into social media algorithms and use them to recruit new members for the organization. This content mainly focuses on showing strength and power in terrorist actions and diverting interested people to forums and chat rooms where they can be further influenced and radicalized. A UNESCO report outlined the strategy that terrorist organizations use to recruit new members (Alava et al. 19-22)**.** It detailed how the internet has allowed recruitment to become easier and more spread out around the world.

An example of algorithms promoting content that promotes violence against women is in 2022 when ex-kickboxer Andrew Tate started to dominate social media. He describes himself as "absolutely sexist" and "absolutely a misogynist." When he participated in the TV show Big Brother he was also removed from the show after six days as a video of him surfaced where he

was beating a woman with a belt. Both he and the woman say they are friends, and this was consensual. This is an example of how algorithms can promote potentially dangerous content that - left unmoderated - can change behavior in the online and offline world. Behavior change caused by content on the internet usually manifests itself by new morals and ideas being expressed on the internet, with these new ideas and morals slowly trickling into real life where they can be potentially more dangerous.

Timeline of Key Events

1946	United Nations Commission on the Status of Women was founded
1975	First World Conference on Women in Mexico City
1989	World wide web (WWW) is invented by Tim Berners-Lee
1996	Communications Decency Act
2000	Child Internet Protection Act
2001	Convention on Cybercrime
2006	The 'Great Firewall' in Peoples' Republic of China is first implemented
2008	UNODC launched the Blue Heart campaign combating human trafficking but also helping rehabilitate the victims
2012	UN Resolution (A/HRC/20/L.13) passes, recognizing Internet freedom as a basic human right

2012	World conference on International Telecommunications Union (ITR)
2015	Octopus Conference 2015 : Cooperation against Cybercrime

Major Parties Involved

United States of America (US/USA)

As stated in the First Amendment to the United States Constitution, “Congress shall make no law respecting an establishment of religion or prohibiting the free exercise thereof. or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble and petition the Government for a redress of grievances. This amendment forbids the adoption of legislation with the aim of restricting free speech and expression rights. Private Internet connections in the USA are uncensored in compliance with this amendment, as is the situation in many democracies with similar constitutions. The US and 55 other nations failed to ratify a treaty at the International Telecommunications Union (ITU) convention in Dubai in 2012, which would have finally guaranteed some level of worldwide Internet filtering. As a result, this treaty was terminated. Instead, the US decides to spread its own censorship-related laws. Furthermore, many large media companies are headquartered in the US, meaning that these various companies have to comply with the US laws and local laws in the countries they are operating in. Various companies include Meta (Facebook, Instagram, WhatsApp), Snapchat, and Twitter.

People’s Republic of China (PRC)

China's Internet censorship is more comprehensive and sophisticated than any other country in the world. It is known colloquially as the ‘Great Firewall.’ There are 547 million active female internet users, and that number is growing by the year. “A growing nationalistic fervor is fueling a torrent of vitriol against anyone speaking out against the state, especially women’s rights activists” (The Guardian) False nude photos, threats, defamatory remarks, and

harassment of family members have been directed at some women who have used their public platforms to bring attention to human rights issues like the injustices in Xinjiang. As well as government representatives and state media, ordinary citizens have launched attacks online.

Freedom House

This NGO, which has its headquarters in the US, carries out research on matters pertaining to human rights, including the matter of freedom of expression. Additionally, it actively promotes freedom of speech and expression through collaboration and communication with groups, supporters of free expression, and the UN (UN).

National Coalition Against Censorship

The NCAC is an association of groups with the mission of defending free expression and opposing censorship. They achieve this by informing the public about censorship and by reporting on matters that are of current interest. Internet censorship is one of their areas of attention, among other forms of censorship.

Human Rights Watch (HRW)

The HRW is an international NGO, and freedom of expression is one of the primary concerns it addresses. In addition to writing numerous papers on the subject, it founded the International Freedom of Expression Exchange. They have published papers on the trafficking of women and girls all over the world, and appeal, suggest and help governments in their fights for human rights and the protection of individuals. The HRW relies on the definition that defines trafficking in the Protocol to Prevent, Suppress and Punish Trafficking in Persons, Especially Women and Children, Supplementing the United Nations Convention Against Transnational Organized Crime (Trafficking Protocol). The Trafficking Protocol provides states with a framework for protecting the victims' human rights, including providing them with medical and psychiatric care, suitable housing, legal aid, protection and safety, temporary residence, and safe repatriation.

Meta

Meta is the holding company that was previously known as Facebook, which now owns Facebook, Instagram, WhatsApp, and the new Horizon Worlds, also called the 'Metaverse.' As stated previously, Facebook and Instagram are the primary hubs for human trafficking, catfishing, and harassment. As of 2021, the dominant social media network claimed to have taken several actions to ensure the safety of women, including creating strict standards against bullying and harassment and implementing technological modifications to stop the distribution of indecent photographs on the platform without consent. However, it is unclear if any of these large statements have come into practice, as online protection is far from guaranteed.

Possible Solutions

Women's violence and cyberattacks are typically not taken seriously. States must use all the tools at their disposal to address cyberviolence against women on an equal footing with other forms of violence against women if they want to see a change. Online freedom of expression is in danger if states do nothing.

Law and Justice

Implementing laws and prosecuting offenders would be a very effective method, furthermore, states can use existing human rights frameworks to combat online gender-based violence. Mary Anne Franks, a professor at the University of Miami School of Law, points out that "laws prohibiting stalking, harassment, extortion, computer fraud, identity theft, and threats can be very effective against online harassment, but they are rarely used because law enforcement either does not know, does not care, or does not have the training and resources to use them."

The Digital Services Act of the European Union is a recent illustration of a significant legislative endeavor (DSA). According to the regulation, digital businesses must provide a means for customers to disable algorithms that utilize their personal data to customize content. Companies will also be required to compile an annual risk assessment report, have it reviewed

by an outside auditor, and make a summary of the results available to the public in order to promote transparency.

Previous attempts to solve this issue include the Lanzarote Convention on sexual abuse and exploitation against children, the Budapest Convention on cybercrime, and the landmark Istanbul Convention is the Council of Europe Convention on preventing and combating violence against women and domestic violence. On 12 March 2012, Turkey became the first country to ratify the convention, followed by 37 other countries from 2013 to 2022, which are Albania, Andorra, Austria, Belgium, Bosnia and Herzegovina, Croatia, Cyprus, Denmark, Estonia, Finland, France, Georgia, Germany, Greece, Iceland, Ireland, Italy, Liechtenstein, Luxembourg, Malta, Moldova, Monaco, Montenegro, the Netherlands, North Macedonia, Norway, Poland, Portugal, Romania, San Marino, Serbia, Slovenia, Spain, Sweden, Switzerland, Ukraine, United Kingdom. The treaty seeks to prevent violence, protect victims, and put an end to the impunity of offenders.

Balanced Regulation

It is becoming more and more obvious that computer platforms cannot be fully depended upon to monitor their users and filter material. As a result, governments all over the world are increasingly eager to control these platforms through legislation and sanctions. There is a conflict between, on the one hand, preventing or managing online harms like cyberbullying, misogyny, and hate, and, on the other, employing those controls to stifle dissent, restrict free speech, or undermine democratic principles.

The potential problem that comes from governments curbing tech companies' control over online platforms is that they could decide to use it for their own purposes and further infringe on users' rights. "The most promising legislation seeks to address online ills while bringing both corporate and state practices into compliance with international human rights principles such as necessity, transparency, oversight, and due process. But the danger posed by the worst

initiatives is immense: if placed in the hands of the state, the ability to censor, surveil, and manipulate people end masse can facilitate large-scale political corruption, subversion of the democratic process, and repression of political opponents and marginalized populations." (Freedom House)

Something that has to be avoided when censoring content is something that the social media giants call "viewpoint censorship." They claim that censorship is biased against conservative views. "Some proposed viewpoint laws do include exceptions for threats against people based on factors such as race, religion, or national origin. Gender is rarely if ever, included. This omission is quite common in laws banning hate, harassment, stalking, or other forms of violence." (CIGI)

Bibliography

Alava, Séraphin, et al. *Youth and violent extremism on social media: mapping the research*. UNESCO Publishing, 2017. *UNESCO Digital Library*, https://unesdoc.unesco.org/ark:/48223/pf0000260382. Accessed 4 January 2023.

Cristol, Hope, and Smitha Bhandari. "Dopamine: What It Is & What It Does." *WebMD*, 14 June 2021, https://www.webmd.com/mental-health/what-is-dopamine. Accessed 4 January 2023.

Hu, Charlotte. "Why TikTok's algorithm is so addictive." *Popular Science*, 7 December 2021, https://www.popsci.com/technology/tiktok-algorithm/. Accessed 4 January 2023.

Medium Contributers. “How TikTok Is Addictive. Psychological Impacts of TikTok’s… | by - | DataSeries.” *Medium*, 6 September 2020, https://medium.com/dataseries/how-tiktok-is-addictive-1e53dec10867.

Accessed 4 January 2023.

Wikipedia contributors. “Andrew Tate.” *Wikipedia*, Wikipedia, The Free Encyclopedia, https://en.wikipedia.org/w/index.php?title=Andrew_Tate&oldid=1131500100.

Accessed 03 January 2023.

American Psychological Association. “Facts about Trafficking of Women and Girls.” *Https://Www.apa.org*, 2017, www.apa.org/advocacy/interpersonal-violence/trafficking-women-girls.

Crelinsten, Ronald. “What Can We Do to Combat Online Gender-Based Violence?” *Centre for International Governance Innovation*, www.cigionline.org/articles/what-can-we-do-to-combat-online-gender-based-violence/.

“Cyberviolence against Women - Cyberviolence - Publi.coe.int.” *Cyberviolence*, www.coe.int/en/web/cyberviolence/cyberviolence-against-women#.

“Digital 2022: North Korea.” *DataReportal – Global Digital Insights*, datareportal.com/reports/digital-2022-north-korea.

“Global Knowledge Platform to End Violence against Women.” *Evaw.unwomen.org*, evaw.unwomen.org/en.

Maeve Duggan. “Men, Women Experience and View Online Harassment Differently.” *Pew Research Center*, Pew Research Center, 14 July 2017, www.pewresearch.org/fact-tank/2017/07/14/men-women-experience-and-view-online-harassment-differently/.

“Online Violence against Women in Asia.” *UN Women – Asia-Pacific*, asiapacific.unwomen.org/en/digital-library/publications/2020/12/online-violence-against-women-in-asia.

“Our Issues.” *Freedom House*, freedomhouse.org/issues.

Reichert, Corinne. “Facebook Emphasizes Women’s Safety on Social Media.” *CNET*, www.cnet.com/tech/mobile/facebook-emphasizes-womens-safety-on-social-media/. Accessed 4 Jan. 2023.

Shook, Natalie J., et al. “Sexism, Racism, and Nationalism: Factors Associated with the 2016 U.S. Presidential Election Results?” *PLOS ONE*, vol. 15, no. 3, 9 Mar. 2020, p. e0229432, 10.1371/journal.pone.0229432.

“Social Media Violence.” *Social Media Victims Law Center*, socialmediavictims.org/social-media-violence/.

The Problem with Anonymity on the Internet – RISKEYE. riskeye.com/the-problem-with-anonymity-on-the-internet/.

“U.S.: Efforts to Combat Human Trafficking and Slavery.” *Human Rights Watch*, 23 Sept. 2008, www.hrw.org/news/2004/07/06/us-efforts-combat-human-trafficking-and-slavery.