SERIES ON DIGITAL RIGHTS AND INTERNET FREEDOM

Topic 7: Safety and Security Online

Greater Internet Freedom

The Centre for Intellectual Property and Information Technology Law (CIPIT), Strathmore University

August 2023

Safety and Security Online

Author: The Centre for Intellectual Property and Information Technology Law (CIPIT).

Acknowledgements: We would like to express our gratitude to the Centre for Intellectual Property and Information Technology Law (CIPIT) acknowledging, Florence Ogonjo, Joshua Kitili, Lilian Olivia Orero, Doreen Aoko Abiero, Josephine Kaaniru, and Dan Allan Kipkoech who prepared this learning material. The CIPIT team authored this material in close consultation with the Greater Internet Freedom team at Internews, including Sigi Waigumo Mwanzia, Digital Rights Advisor, and Olga Kyryliuk, Technical Advisor on Internet Governance and Digital Rights.

Copy-Edited by: Internews.

Design & Layout by: CIPIT.

Strathmore University
Centre for Intellectual Property and Information Technology Law

Internews

About CIPIT	About GIF
The Centre for Intellectual Property and Information Technology Law (CIPIT) is an evidence-based research and training Centre based at Strathmore University, Nairobi, Kenya. CIPIT was established in 2012 and focuses on studying, creating, and sharing knowledge on the development of intellectual property and information technology utilizing diverse methodological approaches to inform debates on ICT applications and regulation.	**The Greater Internet Freedom Project (GIF) is a three-year, consortium-based, global program implemented by Internews and the GIF consortium across 39 countries. GIF places regional and local organizations at the forefront of the fight to preserve an open, reliable, secure, and interoperable Internet – and, by extension, protects the citizens, civic actors, journalists, and human rights defenders who rely on it to realize fundamental freedoms.**

Table of Contents

Safety Online

The CIPIT and the GIF have developed exploratory material relevant to pertinent digital rights and internet freedom topics. The 'Safety and Security Online' topic examines safety online, security online and women's rights. It briefly explores safety online challenges, including cyber-stalking and child safety online, security online, including cyber-security and identity theft, and women's rights online, including online gender-based violence, amongst others.

Advancements in ICT connectivity and internet penetration specifically present safety and security challenges for various groups online at a global level. These challenges are largely a reflection of challenges faced in the offline realm, that have been transposed to the digital realm, albeit at an accelerated pace of transmission. It is imperative to ***recall that online safety and security issues overlap with mental health and online safety***. Pressingly, these issues negatively impact internet users' mental health, giving rise to a range of mental challenges including anxiety, depression, and suicidal thoughts, amongst others.[1]

- This material explores safety and security issues online, with a narrowed focus on their impact on women's rights online.

Cyber Stalking[2]

Cyber stalking refers to the use of information and communications technology (ICT) to perpetrate more than one incident intended to repeatedly harass, annoy, attack, threaten, frighten, and/or verbally abuse individuals.[3] It is an extension of offline stalking and involves repetitive, threatening, unwanted and harassing behaviors.[4] Examples of cyber stalking including monitoring or tracking a person's location and/or activities using GPS trackers, spyware, cameras and microphones,

and location-based dating apps, checking email, call or message histories, as well as monitoring a person's social media profiles.[5]

Cyber stalkers are often motivated by control or destruction to cause an individual to feel helpless and distressed.[6] The internet has created an environment where victims and offenders meet without any barriers, leading to a spike in the number of cybercrimes observed online.[7] Conversely, in this environment of power and control, cyber attackers deployed a range of creative, calculating and evolving approaches to attack their victims, leveraging new and emerging technologies, an driven by 'sadism, narcissism, general psychopathy, sexual aggression' amongst other personality traits.[8]

The emergence of new technologies, such as artificial intelligence, has also accelerated the pace at which stalkers can monitor and track their victims online, thereby entrenching the relationship between cyberstalking and digital advancements.

Important Note

"As a surveillance tool, AI could enable offenders to track and monitor their victims with greater ease and precision than ever before. AI-powered algorithms could, for example, analyze and predict a person's movements by gathering data from an array of sources: social media posts, geotagged photos, etc., to approximate or even anticipate a victim's location."

Source: C.A Goldberg.

Legal, Policy and Regulatory Framework on Cyber-Stalking

Protecting victims of cyber-stalking requires the enactment and operationalization of efficient and operational legal, policy and regulatory frameworks capable of providing both redress to victims and imposing strict penalties that deter this behavior by perpetrators. Across GIF regions, countries have enacted laws that criminalize cyber stalking; in the Philippines, the Anti-Cybercrime Law and Cyberbullying Law, Republic No. 10175 classifies cyber stalking as an offence,

providing stiff penalties for those convicted. This law was enacted to tackle the growing prevalence of cyber stalking and cyber bullying, leading victims to "suffer from depression, anxiety, and suicidal thoughts."[9]

Problematically, enforcing cyber stalking laws across GIF regions, where these exist, is difficult, largely due to the fact that law enforcement officers trivialize these incidents due to a lack of understanding of the compounded effect of these issues, including identity theft, job loss, mental trauma or suicidal thinking. Further, locating perpetrators of cyber stalking incidents is also challenging, owing to digital anonymity protections.

Generally, across GIF regions, cyber stalking and harassment policies, actions, laws, and practices need to be amended to reflect the realities of modern day challenges and keep abreast with technological advancements. Further, law enforcement officers urgently require continuous training and up skilling to be able to provide tailored assistance to cyber stalking victims.

Child Safety Online

Resource: WHO's Report - What works to prevent violence against children online?

The World Health Organization observes that "cyberstalking is particularly common among young people of dating age, with girls victimized somewhat more than boys. One in four (24%) females and one in five (19%) males first experienced stalking when they were 17 or younger, according to one of the most comprehensive surveys of stalking conducted by the US Centers for Disease Control. Of these victims of stalking, 56% of females and 61% of males experienced their stalking via social media, such as unwanted texts and photos (39). In another national survey from the USA, victims said 61% of their cyber stalkers were intimate partners, friends or acquaintances, 28% were of unknown identity, and 10% were persons met online (95)."

Source: WHO.

The internet can be extremely beneficial for children; they can use it to learn, communicate, develop, create and explore the world around them. However, too often, it also leaves them vulnerable to risks and exposes them to experiences

which they find upsetting. These online risks are not always fully understood but it is essential for children's safety that they are addressed. For many children there is often no distinction between their online and offline lives.[10]

Online sexual abuse refers to the use of 'technology to manipulate, exploit, coerce or intimidate a child to (but not limited to): engage in sexual activity; produce sexual material/content; force a child to look at or watch sexual activities; encourage a child to behave in sexually inappropriate ways; or groom a child in preparation for sexual abuse (either online or offline). It also entails coordinating or directing others people to abuse children online.'[11]

As with other forms of sexual abuse, online abuse can be misunderstood by the child and others as being consensual, occurring without the child's immediate recognition or understanding of abusive or exploitative conduct. In addition, another influencing factor may be fear from the child if they fail to comply.[12] It is worth noting that no child can consent to being exploited or abused. Financial gain can be a feature of online child sexual abuse, it can involve serious organized crime and it can be carried out by either adults or peers.

Important Note

'Online safety is a community challenge and an opportunity for industry, government and civil society to work together to establish safety principles and practices. Industry can offer an array of technical approaches, tools and services for parents and children.

- **Age-Verification Systems:** these control systems are required to ensure that children are consuming content and services that are appropriate.
- **Highest Privacy Standards:** should be adopted by companies while processing children's data. This is because children may lack the maturity to appreciate the wider social and personal consequences of revealing or agreeing to share their personal information online, or to the use of their personal information for commercial purposes.
- **Risk Assessment and Mitigation:** all services directed at or likely to attract a main audience of children must consider the risks posed to them by access to, or collection and use of, personal information (including location information), and ensure those risks are properly addressed.'

Source: Sonia Livingstone.

Legal Framework Governing Child Online Safety

The *Convention on the Rights of the Child* is the most widely ratified international human rights treaty that sets out the civil, political, economic, social, and cultural rights of children.[13] The Convention protects children from all forms of violence, exploitation, abuse and discrimination of any kind and ensures that the child's best interest should be the primary consideration in any matters affecting them.[14]

Security Online

Cyber Security: Policies and SecurityAwareness

Cyber security is defined as the "*practice of defending computers, servers, mobile devices, electronic systems, networks, and data from malicious attacks. It's also known as information technology security or electronic information security.*"[15] With cyber threats on the rise, it is important for governments, organizations and businesses to have a comprehensive set of laws, policies and regulations in place. These need to be regularly updated with the latest technology trends and applicable laws.

The term ''policy'' is used in a variety of areas related to cyber security, and refers to information distribution rules and regulations, private sector goals for data conservation, system operations strategies for technology control.[16] For example, national cyber security strategies and policies are geared at creating a secure and resilient digital ecosystem that safeguards a nation's interests, fosters economic growth, and protects citizens and critical infrastructure from the ever-evolving landscape of cyber threats.[17] On the other hand, corporate cyber security policies apply to employees and the policies regulate their conduct while working in the company. In companies, it is common to have a centralized security unit that is responsible for cyber security policy and related standards and solutions.[18]

Security awareness training is a formal process for educating relevant parties, including government employees, corporate or NGO employees and third-party stakeholders on how to protect an organization's computer systems, along with its data, people and other assets, from internet-based threats or criminals.[19] In crafting a good security awareness training program, entities should **emphasize the criticality of protecting the organization** and provide ***an overview of the***

corresponding corporate or governmental policies and procedures that cover how to work securely and who to contact if they discover a potential threat.[20]

Identity Theft

Identity theft is defined as "*the crime of obtaining the personal or financial information of another person to use their identity to commit fraud, such as making unauthorized transactions or purchases. Identity theft is committed in many different ways and its victims are typically left with damage to their credit, finances, and reputation.*"[21] Identity theft affects all ranges of targets including individual consumers, businesses, and government institutions.

Due to the rapid adoption of technology in all facets of life, identity theft is a crime that does not discriminate and is one of the fastest-growing cybercrimes.[22] Notably, this cybercrime poses a significant risk to digital rights and internet freedoms in GIF regions, by exposing individuals' confidential information and creating a risk of recurring harm and a loss of control over one's identity.

The growing technology adoption of devices like smart phones and connective media such as social networking sites (Instagram, Twitter, and Facebook) and instant messaging greatly accelerates the growth of identity theft and creates a field ripe with opportunity for criminals. With such robust membership and enthusiastic participation in social media, these sites represent a vast repository of personal information about people, making them a prime target for those seeking to commit identity theft.[23]

Further, recent technology changes for the sake of convenience exacerbate this issue. Many websites have taken to using **Facebook as a central login and validation source** to reduce a person's number of credentials and the number of times that customers must negotiate the sign-on process.[24] Most account profiles

gather basic identifying information such as name, address, and contact information. However, entertainment, retail, and ecommerce sites are likely to have payment and financial information as well. More tangentially, many password security questions involve items such a favorite movie or color, so even the more innocent-appearing sites could provide information to enable identity theft.[25]

Women's Rights Online

Digital inequality is both a consequence, and a cause, of broader inequalities. Women's equal access to new technologies and their meaningful participation on and through the internet is a critical component of women's rights and equality in a digital world.[26] Access to the internet, in particular, has greatly enabled women to have a voice in spaces where this was previously denied, challenging gender norms, using information, participating in political and associational networks, and increasing their economic independence.[27]

Legal, Policy and Regulatory Framework on Women Rights Online

Gender mainstreaming is the process of assessing the implications for women and men of any planned action, including legislation, policies or programs, in all areas and at all levels. It is a strategy for making women's as well as men's concerns and experiences an integral dimension of the design, implementation, monitoring and evaluation of policies and programs in all political, economic and societal spheres so that women and men benefit equally and inequality is not perpetuated. The ultimate goal is to achieve equality between men and women.

Gender mainstreaming as a strategy and methodology does not in theory mean an emphasis on women's experiences. However, given the socially constructed differences and relations between males and females in most of the world's societies, in practice it often results in a specific focus on women because they are mostly adversely affected by existing gender inequalities.

Legal frameworks can either support or hinder gender equality and women's empowerment.[28] By incorporating gender equality within formal laws, countries

support women's economic empowerment, political voice and widen their opportunities for development overall.[29] Conversely, discriminatory laws promote the subordination of women and girls and support attitudes and harmful practices that limit their opportunities and potential. Discrimination in legal frameworks contributes significantly to persistent gender gaps in women's economic, social and political empowerment. The Convention on the Elimination of All Forms of Discrimination against Women (CEDAW) (1979) is one of the foremost international instruments on women's rights and gender equality.[30] Exclusively devoted to gender equality, CEDAW defines sex-based discrimination and its root causes, outlines legal obligations for States parties in regard to the fulfilment of substantive equality between women and men, and provides a framework for monitoring its implementation by the CEDAW Committee.[31]

In Africa, the Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa ("The Maputo Protocol") (2003), outlines a range of women's rights including economic, social, civil and political as well as cultural and environmental rights. The Maputo Protocol was devised to complement and strengthen the commitments to women's rights made in the African Charter on Human and Peoples' Rights ("The Banjul Charter") (1981).[32] Article 18 of the Banjul Charter specifically calls on states to eliminate discrimination against women and to protect women's rights in alignment with international declarations and conventions.

Women's Political Participation and Representation

The definition of political participation has been drawn from the literature review. Consequently, it is important to note that there are many different activities and behaviors that are considered "political".[33] "Participation" in these includes on the one hand involvement in formal political activities (voting, standing for election

etc.) but also non-party political activism, advocacy, and public debate. Barriers to women's involvement and advancement in formal representative politics includes: The prevalence of the 'masculine model' of political life and of elected government bodies, women's relative lack of material resources to support their move into politics; women's additional work burden which denies them the time necessary to engage in politics and cultural values which enshrine male behaviors and norms in political cultures.[34] Media representations of male and female politicians are found to play a substantial role in men and women's 'socialization' through which women are excluded from political, public discourse.[35]

Women's Economic Empowerment

Women's economic empowerment is the process of achieving women's equal access to and control over economic resources, and ensuring they can use them to exert increased control over other areas of their lives.[36] Women's empowerment is a process of personal and social change, taking place over interlinked and mutually reinforcing psychological, political, social and economic domains, and through which women individually and collectively gain power, meaningful choices and control over their lives. It is not a linear, uncontested process but instead a journey characterized by negotiation and compromise, and uncertain outcomes.[37]

The internet, with its great potential for economic opportunity and social empowerment, has long been celebrated as a force for greater equality-breaking down barriers for those previously held back by their geography, wealth, race, class and gender. But while digital connectivity has improved life for billions of people, it is falling short on its promise to beat back inequality. Despite recent legal reforms toward gender parity, legal impediments continue to exist in many countries.[38]Addressing the gender inequality in the workforce has the potential to unlock needed resources (especially for developing countries) and support

economic development. It would also help reduce global poverty, since women are more likely to be illiterate and poor. Furthermore, reducing gender inequality could help mitigate the negative effects of a shrinking workforce in developed countries.[39]

It is widely accepted that women have no inherent limitations to assuming the same roles as men. However, history, dominant belief systems, and cultural norms have often subjected them to formal and informal constraints that have become enshrined in countries' legal frameworks to varying degrees.[40] Since laws can incentivize changes in behavior, legal reforms supportive of gender equality can help change cultural biases against women and promote gender equality.[41]

Eliminating gender bias and discrimination in the law is only the first step, but this alone is not enough. In addition, legal reform should also incentivize women to participate in the economy and encourage employers to hire women in traditionally male dominated roles.[42] This includes implementing laws which protect women from discrimination in the workplace due to pregnancy and childbirth, and which promote higher presence of women in leadership roles. In addition, resources should be allocated via policy reforms that make it easier for women to enter and stay in the workforce, such as parental leave, lactation facilities, etc.

Ultimately, gender mainstreaming and gender budgeting on all levels would transform gender relations and reform existing structures that cause discrimination.[43] Providing women with equal economic opportunities requires an integrated set of laws and policies, which are relevant across every domain of women's economic empowerment.[44] Conversely, restrictive environments significantly constrain women's economic choices.[45]

Gender and Technology Design Biases in Algorithmic Decision-Making

Bias refers to any form of preference. An algorithm is a formalized abstract description of a computational procedure.[46] Algorithmic-related bias connotes repeatable errors in a computer system that lead to outputs that are unfair and favor one group over the other. Selection of training data sets is pivotal in building algorithms. Yet, the output will only be as good as the software developers, coders and data scientists behind it.[47] The crux of the matter is that human beings have inherent assumptions and biases stemming from conscious or unconscious prejudices. This will in turn influence the accuracy, reliability and universality of the data sets used leading to a system discriminating unfairly against women.[48]

The growth of algorithmic decision-making in various domains of everyday life has the power to simplify and accelerate a plethora of ordinary tasks, thus playing an important role in facilitating daily activity.[49] However, algorithmic decision-making systems and their data-driven automation processes have revealed discriminatory behavior in many cases. One important dimension of this discrimination is related to gender.[50] Various examples of machine-learned automated decision-making systems (ML-ADM) that resulted in gender bias, some of which developed even by companies that are considered technological giants, have been reported in the past.[51]

The design of ML-ADM systems is usually based on predictive models that are trained using historical data. Unfortunately, these data may encode gender and other social stereotypes.[52] This persistent underrepresentation of women in science and engineering may have negative implications on gender fairness in automated recruitment processes.[53]

Online Gender-Based Violence

The definition of online violence against women extends to any act of gender-based violence against women that is committed, assisted or aggravated in part or fully by the use of ICT, such as mobile phones and smartphones, the Internet, social media platforms or email, against a woman because she is a woman, or affects women disproportionately.[54] Online gender-based violence has been recognized as a challenge to achieve gender equality for women.

In the past few decades, information and communication technologies (ICT) have provided society with many new communication opportunities. For example, people can communicate in real-time with others in different countries using various technologies such as Voice over Internet Protocol (VoIP), instant messaging or social networking websites like Twitter, Instagram, and Facebook.[55] These technologies have transformed self-expression, interactions, and relationships, and even provided somewhat direct access to social, private, non-government, and government sectors.[56]The Association for Progressive Communications (APC) defines online gender-based violence as acts of violence that are committed, abetted or aggravated, in part or fully, by the use of information and communication technologies (ICTs), such as mobile phones, the internet, social media platforms, and email. It includes, but is not limited to, verbal and graphic threats, abusive comments and harassments, sexual assault, and rape photos and videos.[57]Online gender-based violence can manifest itself as cyber-stalking, hacking, non-consensual intimate image violence, cyber-bullying, defamation, online sexual harassment, surveillance/ tracking, hate speech, exploitation or impersonation among others.[58]

Technology-facilitated GBV is action by one or more people that harms others based on their sexual or gender identity or by enforcing harmful gender norms.[59]

This action is carried out using the internet and/or mobile technology and includes stalking, bullying, sexual harassment, defamation, hate speech and exploitation. The perpetrator's motivation refers to the emotional, psychological, functional or ideological driver(s) behind the perpetrator's behavior. Motivations can be political or ideological in nature or driven by revenge.[60] From motivation comes intent, or the determination of the perpetrator to harm someone.

Like motivation, intent varies by type of behavior and can include psychological or physical harm, enforcement of gender norms or extortion.[61] The behavior is the perpetrator's actions or strategy and can include stalking, defamation, bullying, sexual harassment, exploitation and hate speech.[62] Each behavior may be repeated with varying frequency and can be conducted using one or more forms of technology (modes), such as social networking. sites or entertainment platforms. Perpetrators use a variety of technology-facilitated tactics — such as hacking and communicating threats — to carry out specific technology facilitated behaviors.[63]

TFGBV is "*carried out through text, images and unwanted digitally-enabled or enhanced surveillance and monitoring, using a variety of devices and platforms from basic digital tools, such as texting, email and social media, to more advanced technologies such as artificial intelligence (AI), GPS tracking and drones*."[64] Gender-based violence against women has been defined as "any act that results in, or is likely to result in physical, sexual, or psychological harm or suffering to women, including threats of such acts, coercion or arbitrary deprivation of liberty, whether occurring in public or private life."[65] This definition, which emerged from the 1995 United Nations Conference on Women in Beijing, represents an international consensus on how to conceptualize the dynamics of gender-based violence and encompasses child sexual abuse, coercive sex, rape, stalking, and intimate partner violence.

The term “gender-based” is used because such violence is shaped by gender roles and status in society. Gender-based violence against women does not encompass every violent act a woman may happen to experience (being threatened by a weapon during a robbery, for example). A complex mix of gender-related cultural values, beliefs, norms, and social institutions implicitly and even explicitly have supported intimate partner violence and provided little recourse for its victims. In particular, gender roles and expectations, male entitlement, sexual objectification, and discrepancies in power and status have legitimized, rendered invisible, sexualized, and helped to perpetuate violence against women. One of the ways that gender has differentially shaped the meaning of violent acts by women and men is by differentially conferring legitimacy on male violence against women.

Sharing Non-Consensual Intimate Images

Sharing non-consensual intimate images is one of the most prevalent forms of online gender-based violence. It describes the case in which sexually explicit images are shared online without the woman’s consent.[66] It is irrelevant whether the images were taken with or without consent, as the women did not consent to their public distribution. The perpetrators can be those who took the images (whether with or without consent) or hackers who somehow gained access to these intimate images. ***Calling it “revenge porn” is a misnomer: intimate images are not pornography, and revenge is only one possible motive.*** NCII is used to stalk, threaten, blackmail or extort victims. Deeply entrenched patriarchal notions add shame, stigma, and even victim-blaming on top of the online gender-based violence.[67]

Sexualized Threats and Violence

Any unwanted, sexual, online, message is online sexual harassment. It can be a private or public text message, photo, or video. Harassment makes victims feel

threatened, exploited or humiliated and especially when it is repeated, can impact victims' mental health. Online sexual harassment is used to silence women and uphold patriarchal structures.[68]

Cyber Dating Violence

Cyber-dating violence (also termed digital dating abuse, cyber dating abuse, online dating abuse, or cyber partner abuse) is conceptualized as behaviors intended to control, monitor, coerce, harass, and/or stalk a dating partner through the use of digital technology and online partner surveillance occurring out of attachment anxiety, clinginess, anger, jealousy, and other negative emotions.[69] Examples of cyber-dating behaviors consist of, but are not limited to, sending threatening messages, stalking partners online, imposing various forms of surveillance, such as constantly checking on a partner's account, demanding passwords to an online account/phone, and monitoring a partner's online interactions.

Like cyber-bullying, cyber-dating violence is not bounded by place or time. Inability to witness facial expression and body language increases the potential for misinterpretation of online written communication and minimization of its impact; thereby reducing bullies' capacity to develop feelings of remorse.[70] A burgeoning body of literature reports the co-occurrence between cyber dating violence and offline physical and/or psychological dating violence. Existing evidence postulates that endorsement of stereotypical gender beliefs and internalizing rigid gender scripts that depict women as permissive sexual objects and revere men as the primary aggressors are inherent risks for cyber dating abuse.[71] Further, witnessing perpetration (e.g., domestic violence) and subjecting to peer norms/pressure increase propensities for dating violence in part through acknowledging violence as a legitimate way to express anger, monitor behaviors, and resolve conflicts in dating relationships.[72] Cyber dating violence may co-occur with a constellation of

problematic behaviors, such as substance use/abuse, high-risk sexual behaviors, poor physical health, and bullying (both victimization and perpetration and is empirically linked to various negative emotions, such as depression, anger, hostility, and loneliness.[73]

The rise of online dating (also known as "cyber romance") as the latest dating trend in the new millennium following the diminished social stigma attached to dating online and the emergence of various free or low cost dating apps (e.g., *Match, Tinder, OkCupid, Coffee meets Bagel, Bumble, Badoo, Hinge, PlentyOf Fish, Zoosk, Elite Singles, eharmony, Grindr, Happn*) reinforces the belief that online dating is an efficient way to meet potential dates or spouses.[74]

Unlike other types of online forums and social-networking sites, online interactions are typically initiated with the anticipation of face-to-face meetings. Utilizing the World Wide Web or mobile platforms, users can use location-based features to identify potential dates within close proximity, or target users with special interests or from different social groups (e.g., sexual minorities) 24/7 without the fear of rejection. With just one click or swipe, some dating sites also use matching based on personality tests and mathematical algorithms to help users find their best match, and provide access to dating through social media accounts, simplifying the login process and avoiding the concern of identity theft.[75]

To make their dating profile appealing for potential dates, users can select the type of photographs and information they wish to share online such as their interests, mate selection preferences, hobbies, physical attributes (e.g., height, body shape), religion, number of children, desire for having children, pet ownership, and location Empirical evidence suggests that users with attractive profiles are seen more favorably (more competent, intelligent, desirable) and viewed more frequently.[76]

To facilitate communication, online dating sites provide interactive built-in features that offer live chats, instant messages, or emotion icons, allowing users to convey their interests prior to their face-to-face meeting.[77] Exchanging computer-mediated or text messages that are carefully constructed (in lieu of a face-to-face meeting right away) grants users the opportunities to enhance self-presentation, conceal imperfection, and make a positive impression. Nonetheless, the tendency to self-represent in an idealized way by maximizing desired traits and minimizing undesired qualities can lead to the creation of personas that do not represent their offline selves.[78]

Online dating sites may be preferred by people who have limited opportunities to meet potential dates in their immediate surroundings. However, dating apps have also been used to facilitate sexual encounters that may or may not necessarily lead to any romantic relationships.[79] Despite the fact that hooking up with underage youths are legally prohibited and most dating apps have specification that teenagers under the age of 18 are not permitted to use hookup or dating apps, many lucrative dating sites have yet taken initiatives to protect the safety of their customers by mandating a background check on new members.[80] Dangers of online dating may also include being deceived, “catfished,” “friended” into sex trafficking, being cyber-bullied, discriminated, harassed, harmed, and bombarded with rude comments or offensive pictures.[81]

Supplementary Resources

Legislation (International, Regional, National)

African Charter on Human and Peoples' Rights (ACHPR), 1986.

American Convention on Human Rights (1969).

American Declaration of the Rights and Duties of Man (1948).

Association of Southeast Asian Nations (ASEAN) Human Rights Declaration, 2009.

Charter of Fundamental Rights of the European Union, 2009.

Convention on the Elimination of All Forms of Discrimination against Women (CEDAW), 1979.

Convention for the Protection of Human Rights and Fundamental Freedoms (European Convention on Human Rights, or ECHR), 1953.

Declaration of Principles on Freedom of Expression in Africa, revised in 2019.

Guidelines on Freedom of Association and Assembly in Africa, 2017.

Inter-American Democratic Charter (2001).

International Covenant on Civil and Political Rights (ICCPR), 1996.

Protocol to the African Charter on Human and Peoples' Rights on the Rights of Women in Africa (The Maputo Protocol), 2003.

Universal Declaration of Human Rights (UDHR), 1948.

Journals

Berry, M. J., & Bainbridge, S. L. *Manchester's Cyberstalked 18- 30s: Factors affecting cyberstalking*. (2017) Advances in Social Sciences Research Journal, 4(18).

Cava, M.-J., Tomás, I., Buelga, S.,& Carrascosa, L. (2020). *Loneliness, depressive mood and cyberbullying victimization in adolescent victims of cyber dating violence*. International Journal of Environmental Research and Public Health, 17(12), 4269.

Citron, K. D. and Norton, H. *Intermediaries and hate speech: Fostering digital citizenship for our information age.* (2011) Boston University Law Review, Vol. 91, pp. 1435–84.

De Maggio, M.C., Mastrapasqua, M., Tesei, M., Chittaro, A. and Setola, R. (2019). *How to improve the security awareness in complex organizations*. European Journal of Scientific Research, Vol. 4, pp. 33-49.

Duflo, E. '*Women empowerment and economic development'*, (2012) Journal of Economic Literature 50(4): 1051–79.

E. Kritzinger. Online safety in South Africa - A cause for growing concern, *2014 Information Security for South Africa*, Johannesburg, South Africa, 2014, pp. 1-7,.

Fereshteh Naseri, Davoud Taghvaei, Bahram Saleh Sedghpour, Gholam Ali Ahmadi. *A Comparative Study on the Opportunities and Threats of the Internet and Considering the Rights of Kids Online in Australia, Brazil, Iran, and South Africa*, (2021) Iranian Journal of Comparative Education.

Hille, P., Walsh, G., & Cleveland, M. (2015). Consumer fear of online identity theft: Scale development and validation. Journal of Interactive Marketing, 30, 1-19.

Kerr, Orin S. *Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes.* (2003) New York University Law Review, 78, no. 5: 1596-668.

Tokunaga, R.S., 8l, K.S., *Cyber-defense: a taxonomy of tactics for managing cyberstalking*. (2017) Interpers. Violenc. 32 (10), 1451–1475.

Policy Papers

Africa Portal. Exploring Data Anonymisation and Internet Safety in East Africa.

Hinduja S, Patchin J Electronic dating violence: A brief guide for educators and parents. Cyberbullying Research Center; 2011.

Reports

Borrajo, E., Gámez-Guadix, M., & Calvete, E. (2015). Cyber dating abuse: Prevalence, context, and relationship with offline dating aggression. *Psychological Reports*, 116(2), 565–585.

Logan, T. K., & Walker, R. Stalking: A Multidimensional Framework for Assessment and Safety Planning. Trauma, Violence, and Abuse, (2017) 18(2).

KICTANet. Online gender-based violence in times of COVID-19 (2020)

Hinson L et.al., Technology-facilitated gender-based violence: what is it and how do we measure it? (2018)

Javelin Research and Strategy. (2014). Identity fraud report: card data breaches and inadequate consumer password habits fuel disturbing fraud trends. Pleasanton, CA: Javelin Strategy and Research.

Alsop, R., Heinsohn, N. and Somma, A. '*Measuring empowerment: An analytic framework'*, (2005) in R. Alsop (ed.) Power, rights and poverty: Concepts and connections. Washington, DC: World Bank.

Cordes, J.J. (2011), "An overview of the economics of cybersecurity and cybersecurity policy", George Washington University, Cybersecurity Policy Research Institute Report, pp. 1-18.

Websites and Blogs

Cripps, J., Stermac, L., Cyber-sexual violence and negative emotional states among women in a Canadian university. (2018) Int. J. Cyber Criminol. 12 (1), 171–186.

Woodlock, D.,The abuse of technology in domestic violence and stalking. Violence Against Women (2017) 23 (5), 584–602..

H. L. Alford, “Gender Bias in IT Hiring Practices: An Ethical Analysis,” 2016.

Conference Papers

A. Asante and X. Feng, "Content-Based Technical Solution for Cyberstalking Detection," (2021) 3rd1 International Conference on Computer Communication and the Internet (ICCCI), Nagoya, Japan, 2021, pp. 89-95.

References

[1] WHO (2022). Mental Health; Sarah Fader (2018). Social media obsession and anxiety.
[2] The cyber bullying and online hate speech material is canvassed under Topic 2 on Freedom of Expression Online.
[3] UNODC (2020). Cyberstalking and cyberharassment.
[4] CIGI (2023). Supporting Safer Digital Spaces – Introducing CIGI's Special Report.
[5] Jenna Cripps & Lana Stermac (2018). Cyber-sexual violence and negative emotional states among women in a Canadian university.
[6] *Ibid.*
[7] Artem Oleshko (2017). 'Stranger danger' in the online and real world.
[8] Audre Asante and Xiaohua Feng (2021). Content-Based Technical Solution for Cyberstalking Detection; TK Logan and Robert Walker (2016). Stalking: A Multidimensional Framework for Assessment and Safety Planning. Trauma, Violence, and Abuse.
[9] Attorney of the Philippines (2018). Cyberbullying in the Philippines: How the Anti-Cybercrime Law Helps Combat Online Abuse.
[10] World Health Organization (2022). What works to prevent online violence against children.
[11] Sonia Livingstone et. al., (2014). Children's online risks and opportunities: comparative findings from EU Kids Online and Net Children Go Mobile.
[12] *Ibid.*
[13] The Convention on the Rights of the Child, 1989.
[14] Shamard Charles (2019). Social media linked to rise in mental health disorders in teens, survey finds.
[15] Kaspersky (2023). What is cyber security?
[16] Orin S. Kerr (2013). Cybercrime's Scope: Interpreting 'Access' and 'Authorization' in Computer Misuse Statutes.
[17] UNODC. The role of cybercrime law.
[18] Exabeam. The 12 Elements of an Information Security Policy
[19] Mary Pratt (2021). Security Awareness Training.
[20] *Ibid.*
[21] Ali Hussain (2022). What is Identity Theft? Definitions, Types and Examples.
[22] Javelin Research and Strategy (2014). Identity fraud report: card data breaches and inadequate consumer password habits fuel disturbing fraud trends.
[23] *Ibid*.
[24] *Ibid*.
[25] *Ibid.*
[26] Ruth Alsop & Nina Heinsohn (2005). Measuring empowerment: An analytic framework', (2005) in R. Alsop (ed.) Power, rights and poverty: Concepts and connections.
[27] *Ibid*.
[28] IDEA and Gender Links (2021). Women's Political Participation: Africa Barometer.
[29] *Ibid*.
[30] *Ibid, n. 26*.
[31] *Ibid*.

[32] *Ibid*.
[33] *Ibid*.
[34] Mayra Buvinic Rebecca Furst-Nichols (2014). Promoting women's economic empowerment: What works?
[35] *Ibid*.
[36] *Ibid*.
[37] Esther Duflo (2012). Women empowerment and economic development.
[38] *Ibid*.
[39] *Ibid*.
[40] Womankind (2015). Creating new spaces: Women's experiences of political participation in communities.
[41] *Ibid*.
[42] *Ibid*.
[43] *Ibid*.
[44] Robert T. Jensen (2010). Economic opportunities and gender differences in human capital: Experimental evidence for India.
[45] *Ibid*.
[46] Harmony L. Alford (2016). Gender Bias in IT Hiring Practices: An Ethical Analysis.
[47] *Ibid*.
[48] *Ibid*.
[49] Jeffrey Dustin (2018). Amazon scraps secret AI recruiting tool that showed bias against women.
[50] Clementine Collett & Sarah Dillon (2019). AI and Gender: Four Proposals for Future Research.
[51] *Ibid*.
[52] *Ibid*.
[53] *Ibid*.
[54] Statistics Canada (2018). Gender based violence and unwanted sexual behavior in Canada.
[55] *Ibid.*
[56] Delanie Woodlock (2017). The abuse of technology in domestic violence and stalking. Violence Against Women.
[57] KICTANet (2020). Online gender-based violence in times of COVID-19 (2020).
[58] Hinson L et.al., (2018). Technology-facilitated gender-based violence: what is it and how do we measure it?
[59] *Ibid*.
[60] *Supra* n.128.
[61] *Ibid*.
[62] *Supra* n.130.
[63] *Ibid*.
[64] Robert Tokunaga & Krysyna Aune (2017). Cyber-defense: a taxonomy of tactics for managing cyberstalking.
[65] *Ibid*.
[66] E. Borrajo et al. (2015). Cyber dating abuse: Prevalence, context, and relationship with offline dating aggression.
[67] *Ibid*.

[68]C ava, M.-J., et al. (2020). Loneliness, depressive mood and cyberbullying victimization in adolescent victims of cyber dating violence.
[69] *Ibid*.
[70] Galende N, Ozamiz-Etxebarria N, Jaureguizar J, Redondo I. (2020). *Cyber Dating Violence Prevention Programs in Universal Populations: A Systematic Review*.
[71] *Ibid*.
[72] *Ibid*.
[73] Cornelius TL, Resseguie N. (2007). Primary and secondary prevention programs for dating violence: A review of the literature.
[74] *Ibid*.
[75] *Ibid*.
[76] Hinduja S, Patchin J (2011). Electronic dating violence: A brief guide for educators and parents.
[77] *Ibid*.
[78] *Ibid*.
[79] Borrajo, E., Gámez-Guadix, M., & Calvete, E. (2015). Cyber dating abuse: Prevalence, context, and relationship with offline dating aggression.
[80] *Ibid*.
[81] *Ibid*.