The emergence of AI-generated deepfakes as a new tool for gender-based violence against women: A brief narrative review of evidence and the implications of the techno-feminist perspective

Mst Safia Akter* and Pavel Ahmed**

Abstract

Technology facilitates crime. Perpetrators use technology to commit new crimes or old crimes in new ways. The advancement of technology has spawned several cybersexual crimes that affect women disproportionately. The emergence of deepfakes has brought a new dimension to women's cyber sexual victimization. There is little empirical research on deepfakes and women's sexual abuse. Therefore, for this comment piece we reviewed existing peer-reviewed articles and data from websites to show that deepfakes have become a new tool for gender-based violence against women. We use a techno-feminist perspective to argue that deepfake technology is an addition to the tools that are used to form a patriarchal-capitalist society. Like other cybercrimes, cybercrimes using deepfakes affect women disproportionately, and deepfakes have become a tool to control and subjugate women. Also, we contend that techno-feminism has ignored the masculine aspects of new technologies. There is a need for more research on the role of deepfake technology in women's sexual abuse to prevent gender-based violence against women.

Keywords: Artificial Intelligence, deepfake, sexual abuse, techno-feminism, violence against women

* BSc in Criminology and Police Science, Mawlana Bhashani Science and Technology University, Tangail, Bangladesh. Email: cp19025@mbstu.ac.bd.

** Graduate Student, Criminal Justice Sciences, Illinois State University, Normal, IL, USA.

Introduction

In this era of technology and digitalization, cybercrime has become a matter of concern. Cybercrime differs from other crimes in where it takes place. Cybercrime is crime or criminal activity that occurs through the internet using information and communication technology (Jaishankar, 2018; Leukfeldt et al., 2020; Hall et al., 2021). Different scholars have tried to define cybercrime and there is presently no consensus about what constitutes cybercrime (Phillips et al., 2022; Holt & Bossler, 2014). In general, it is used as an umbrella term for a broad spectrum of digital crime (Sabillon et al., 2016). Government, industry and the general public all use the umbrella word "cybercrime" to describe a range of illegal practices and unlawful activities with the use of computers, the internet, or various technological devices (Wall, 2007). It is widely accepted that the word refers to both existing crimes that are made easier or more severe by using technologies, in addition to emerging crimes that have arisen due to the use of the same (Ho & Luong, 2022). According to psychosocial and socio-economic categories, there are five types of cyber-crime: cyberbullying, online harassment, online fraud, revenge porn, and cyberstalking (Ibrahim, 2016; Lazarus, 2019). Perpetrators generally commit this type of crime for economic and/or psychological gain (Ibrahim, 2016). According to the Tripartite Cybercrime Framework (TCF) developed by Lazarus (2019), cybercrime can be divided into three broad categirues based on motivation. These are socioeconomic, psychological, and geopolitical cybercrime.

A large number of studies on cybercrime are concerned with harassment in cyberspace rather than attacks on devices. Cyber harassment can range from cyberstalking to cyberbullying, and cyber hatred (see Wall, 2007; Halder & Jaishankar, 2008; Hinduja & Patchin, 2010) and affect teenagers and women disproportionately (Bocij, 2004; Halder & Jaishankar, 2008). Cyberbullying is the most widely used term in the cybercrime literature (Bailey, 2014; Todd, 2014). It is the intentional and malicious use of technology to harm and defame others by publishing fabricated texts, videos, images, or profiles (Safety Net Canada, 2013).

Much of the existing literature on cybercrime focuses on traditional ways of committing cybercrime (see Wall, 2007; Halder & Jaishankar, 2008; Hinduja & Patchin, 2010; Ibrahim, 2016; Lazarus, 2019). However, the emergence of AI-generated deepfakes has added a new dimension to cybercrime and defaming people. Some existing literature shows that AI-generated deepfakes affect women particularly (see Citron & Chesney, 2019; Westerlund, 2019; Dunn, 2020; Hao, 2020). Despite this, a dearth of information exists on the use of AI-generated deepfakes as tools for gender-based violence against women. This article aims to fill this void. To this end, we employ a techno-feminist perspective to explain that AI-generated deepfakes are used to subjugate women. The paper is divided into three sections. Firstly, we reviewed relevant literature and data to show that cybercrimes are gender-based. Secondly, we accumulated literature to argue that AI-generated deepfakes facilitate violence against women. Finally, we use the techno-feminist perspective to provide an understanding of how AI-generated deepfakes are used to demean women. Furthermore, we present the case for using techno-feminism to explore the gendered aspect of AI-generated deepfakes. Overall, we argue that AI-generated deepfakes are the result of the masculine urge to control, abuse, and subjugate women.

Cybercrime and Gender-Based Cyber Violence

Cybercrime has aroused growing concern around the world due to its high destructiveness and widespread influence. In 2017, the WannaCry ransomware attack affected more than 230,000 computers across 150 countries, resulting in economic losses of more than 4 billion dollars and posing a serious danger to the global education, government, finance, and healthcare sectors (Mohurle & Patil, 2017; Castillo & Falzon, 2018; Ghafur et al., 2019). According to certain criminological theories, such as routine activity (Cohen & Felson, 1979), general strain (Agnew, 1992) and general theory of crime (Gottfredson & Hirschi, 1990), cybercrime is a sophisticated phenomenon that is shaped by the interplay of underpinning economic and social factors. The development of cybercrime agglomerations is significantly influenced by human and societal variables (Watters et al., 2012; Waldrop, 2016; Leukfeldt & Holt, 2019).

In recent years, a growing body of sociological and psychological research has focused on the human elements underlying cybercrime and examined phishing attacks, the spread of malware, identity theft, fraudulent activities on the web, harassment through the internet, cyberbullying, and other forms of cybercrime (Bergmann et al., 2018; Mikkola et al., 2020). Although males are more likely to be the victims of certain types of cybercrime, such as piracy, fraud and identity theft (Näsi et al., 2015), women tend to be the victims of romance scams (Whitty & Buchanan, 2012) and sexual harassment (Näsi et al., 2015) more than males. The world's biggest-ever survey by the European Union Agency for Fundamental Rights (FRA) revealed that 73 percent of women surveyed experienced internet-based sexual violence at least once (EU FRA, 2014).

Cyber violence against women can take many forms: cyberstalking, harassment, bullying, gender-based hate speech, and non-consensual intimate image abuse (EIGE, 2022). Studies show that women and girls are at greater risk of being the victims of cyber violence, enduring recurrent and extreme kinds of abuse, from physical to psychological and emotional, and incurring negative outcomes (GREVIO, 2021). UN research (2015) shows that 73 percent of women who use modern communication technology have faced some cyber abuse, such as sexual violence. In a study of almost 9000 Germans, a noticeable gender disparity was found among users of the internet aged 10 to 50: females compared to males were considerably more likely to have experienced the effects of online stalking and the trauma of this kind of violence was greater among women victims (Staude-Müller et al., 2012). Similarly, a Pakistani study showed that females are the primary victims of cybercrime, primarily cybersexual crime (Anjum, 2020). The scenario is the same in Indonesia (see National Commission on Violence Against Women, 2019). Women between the ages of 18 and 24 are particularly vulnerable to all forms of cyber-VAGW. According to Amnesty International's 2017 research, a quarter of the 4,000 women polled in European countries, even those from highly affluent nations like the United Kingdom, Spain, and Italy, had at least sometimes encountered online violence or harassment on the internet. Eighteen percent of women in EU countries—or roughly 9 million women—have been victims of significant online assault since the age of 15, according to this study. Online VAWG comes in the form of obscenely graphic and threatening electronic texts, pictures, and video contents. Dating websites and social networking sites, as well as chat rooms and

messaging apps, make up the majority of the sender channels. Experiencing this type of abuse is more prevalent among women and girls of all ages than their male counterparts (Davis & Schmidt, 2016; Reyns et al., 2011). Women in Ghana experience internet harassment through rude remarks and pornographic photographs and videos (Armiwulan, 2021). A similar scenario has been seen in Bangladesh. A 2022 study by ActionAid Bangladesh showed that approximately 64 percent of women reported being victims of cyber violence, compared to around 50 percent in the previous year. The type of online violence they faced were sexual comments, receiving explicit images, proposals to have sex, discrimination, creation of fake IDs, stalking, threats of sexual assault, having private photos posted without consent, and having photos edited and posted on pornography sites (Dhaka Tribune, 2022). Not only women generally, but also women activists are subject to cyber violence. For instance, there have been recorded cases of internet stalking and sexual assault against women activists in Colombia (Lyons & Blanchard, 2016). Females face online sexual abuse and sexist remarks despite being public figures. This can be seen in the case of UK Labor MP Jess Phillips, who received over 600 threats of rape in a single night and sexist comments on her social media accounts (Rawlinson, 2018).

Since these forms of internet-based sexual violence disproportionately affect women, this violence can therefore be called gender-based violence, which the UNHCR defines as violence against someone because of his/her sex or gender. This new type of gender-based violence is called gender-based cyber violence which is made possible by the continual connectivity and greater usage of new digital technologies (EIGE, 2022). Previous studies indicate that the nature of cybercrime, especially cyber-sexual violence, is similar across borders. Women and girls are the primary targets of these crimes, which makes them gender specific. We argue that men find women and girls as the most vulnerable and suitable targets. Women become susceptible to internet-based sexual violence with their increasing use of digital technology. On the other hand, the availability of digital technology opens new avenues for men who exploit women for their gratification. One such technology is Artificial Intelligence (AI). Using AI, men create deepfakes of women to abuse them and harm their image (Dunn, 2020). The addition of AI-generated deepfakes within the tools for abusing women adds a new dimension and facilitates the commission of gender-based sexual violence.

Artificial Intelligence (AI)-Generated Deepfakes: A New Tool for Violence against Women

AI has a considerably longer history than is typically thought, going all the way back to ancient Greece (Dennehy, 2020). However, Alan Turing is credited for its present form (see Turing, 1950), and John McCarthy formally defined the phrase "artificial intelligence" as "the science and engineering of creating intelligent machines" at a conference held at Dartmouth College in 1956 (McCorduck & Cfe, 2019). According to McCarthy (1988):

> AI is concerned with methods of achieving goals in situations in which the information available has a certain complex character. The methods that have to be used are related to the problem presented by the situation and are similar whether the problem solver is human, a Martian, or a computer program.

However, cybercriminals have not just discovered a unique means of leveraging their illegal actions through the utilization of AI technology, but also new chances to plan and carry out attacks upon governments, businesses, and individuals. Although there is little proof that criminal organizations possess the technological knowledge necessary to effectively manage and use machine learning and AI systems for illicit objectives, it is undeniable that these organizations have recognized the enormous opportunity of these systems for illicit and destructive activities (Khanna & Khanna, 2020). Data and the present situation indicate that hackers are increasingly using the internet to create and disseminate malware and launch ransomware assaults, which are greatly facilitated by AI technology (Velasco, 2022).

AI-created deepfakes are a further harassing trend pervasive in numerous sectors. Deepfakes are based on AI deep learning algorithms, an area of machine learning that applies neural net simulation to massive data sets to create fake videos of real people. These are trained algorithms that allow the recognition of data patterns, as well as human facial movements and expressions, and can match voices to imitate the real voice and gestures of an individual (European Parliamentary Research

Service, 2021). They substitute the resemblance of one person for another, giving the target person the appearance that they are speaking or acting in the same way as the source person (Albahar & Almalki, 2019). Although deepfakes can be made with the agreement of the people portrayed, they are frequently made without their knowledge. Recent innovations have made it possible to create complex deepfake films from a single image, making it possible to construct any computerized human record and endangering privacy (Naitali et al., 2023). Deepfakes are employed for illegal activities including extortion, emotional abuse, fraud, and prejudice against women and adolescents (Hao, 2020). It is a special tool for technology-based abuse and assault against women (Citron & Chesney, 2019). Although deepfake technology is being employed for a variety of beneficial purposes, it has also been used to torture, degrade, and humiliate women (Westerlund, 2019). Deepfakes provide a fresh method of exercising dominance and control (Eaton & McGlynn, 2020). This is a new method of image-based sexual abuse which is different from traditional sexual abuse and has various consequential impacts on victims, affecting mental and physical health, reputation, and relationships (Henry et al., 2020). Deepfakes are frequently used as abusive tools to undermine a woman's identity, harm her image, frighten her, and coerce her into submission (Dunn, 2020). Deepfakes propagate and perpetuate an online environment where women's pictures are fabricated for general amusement by utilizing a woman's physical appearance as an online resource without her consent. The widespread use of deepfakes further assumes, breeds and strengthens an online space in which women's images are fabricated for consumption by men who occupy these digital worlds by using a woman's face and body as a digital resource without her consent (Van Der Nagel, 2020).

Sensity, a cybersecurity company, claims that deepfakes are expanding fast and doubling in number every six months (Compton, 2021). Ninety percent of the 85,000 deepfake videos circulating online feature women in non-voluntary pornographic content. Regarding the developers, a simple glance at the top 30 on one website finds deepfakers everywhere, including in the United States, Canada, Guatemala, and India (Compton, 2021). Adam Dodge, the founder of EndTAB, a nonprofit organization that educates individuals about technology-facilitated abuse, claims that this is violence against women (Hao, 2021).

Deepfakes and Gender-Based Violence: From a Techno-Feminist Perspective

Gender dynamics in the usage of technology can be understood from a techno-feminist perspective. Techno-feminism, first used by Cynthia Cockburn (1983) and developed by Judy Wajcman (2004), is a theoretical approach concerned with the study of the intersection of gender and technology (Sikka, 2017). This approach examines the implication of gender with technologies that are thought to be symbols of masculinity (Wajcman, 2004). Also, this approach shows how gender and technology shape each other (Sikka, 2017) and facilitates the study of women's interaction and usage of various technologies (Chan, 2018).

Digitalization is a new revolution aimed at enhancing people's lives and well-being. However, women have failed to get equal benefits as men from this revolution (Wajcman et al., 2020). It has been found that a gender gap persists in almost every country (Sey et al., 2018). Research shows that gender intersects with different factors, such as race, class, sexuality, ethnicity and other aspects of difference within the present form of technological society. These intersections create diverse challenges for women, and women from minority groups face the most disastrous effects of technology (Buolamwini & Gebru, 2018). Despite attempts to make algorithms and data-driven decision-making processes objective, unbiased, and equitable, technological biases exist, and AI intensifies them, as a result of the exclusion of women and marginalised people from leadership positions in the field (Wajcman & Young, 2023).

The central idea of techno-feminist theory, which points out that technology and gender shape each other, considers technology as a root and a result of patriarchy (Wajcman, 2004). By proposing technology as "both a source and consequence of gender relations", Wajcman (2006: 15) argues that technology and gender are mutually constituted. Particularly, men shape technology and exclude women from the technological sphere (Wajcman, 2010). Indeed, data show that women are largely excluded from the technology workforce, AI workforce, and AI research (see (Wajcman & Young, 2023).

However, we suggest that the scope of techno-feminism should be broadened out, by not only focusing on women's underrepresentation within the technological sphere but also examining women's subjugation as they experience gender-based violence within the new waves of technology, such as deepfakes. This is because subjugating women by gender-based violence has potentially more severe impacts than excluding them from the technological workforce. Existing evidence shows that cybercrime works as a means of controlling, intimidating or harming those who are subjugated. Technology facilitates these crimes and provides offenders with a means of committing them. They can hurt others anonymously and inflict psychological pain. Technology encourages them and makes harming others easier (Al-Nemrat et al., 2010) and women are the primary easy targets of abusive technology-made content (Jane, 2016). Along with other uses of deepfake technology, it has been used to make content to facilitate image-based sexual abuse of women, to humiliate and abuse them (Westerlund, 2019). Perpetrators use deepfake technology to dominate women (Eaton & McGlynn, 2020) and make them submissive (Dunn, 2020). These dominating and controlling effects of deepfakes are overlooked in the public sphere (Eaton & McGlynn, 2020; Jane, 2016). Considering these, we argue that exercising control over women and demeaning them using deepfake technology is a patriarchal-capitalist process that harms women and halts their advancement. The digital world mirrors and exacerbates the traditional patriarchal society that harms women in the offline world. Women are more likely than men to become the victims of technology-facilitated crimes, and deepfake technology harms women disproportionately. The available evidence on women's sexual abuse by AI-generated deepfakes shows how women are subjugated. The male perpetrators use AI-generated deepfakes for domination and to control and demean women. AI and masculinity thus combine to form a more patriarchal society.

While techno-feminists are mostly concerned with women's underrepresentation in science and technology, we argue that the focus should be extended to also viewing how technology breeds gendered oppression. Empirical studies should also focus more on emerging technologies, such as AI and deepfake technologies, and their impacts on women.

Conclusion

Technology reflects and reproduces traditional gender relations in our societies, including the cultures and practices of sexual violence against women (Powell & Henry, 2017). Although AI has become an essential part of digital services and governments around the world are willing to use AI to combat crime (Velasco, 2022), AI-generated deepfakes are becoming a matter of concern for both political and personal life (Westerlund, 2019). This technology has become a tool for violence against women (Hao, 2021). However, AI-generated deepfakes and their potential as a tool for dominating women have been overlooked in techno-feminist literature. With this article, we call for new avenues of research within techno-feminism, emphasizing deepfakes as a new tool for reproducing traditional patriarchal power dynamics.

We also call for strategies to combat this image-based sexual violence. Although numerous strategic partnerships and international instruments have been formed to combat AI-based cybercrimes (see Velasco, 2022), there is no strategy or regulation focused on regulating violence against women by deepfake technologies. However, there are ways to combat deepfakes (Westerlund, 2019). Significant recent research has concentrated on deepfake technologies. This research should focus more on deepfakes' effect on women, especially the sexual abuse of women, and on identifying methods to prevent perpetrators from using deepfakes to commit sexual violence against women. More attention should be given to the development of anti-deepfake technology. Overall, governments should develop strategies to combat this transnational cyber sexual violence against women.

References

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. *Criminology*, 30(1), 47–88.

Albahar, M. & Almalki, J. (2019). Deepfakes: Threats and countermeasures systematic review. *Journal of Theoretical and Applied Information Technology*, 97(22), 3242–3250.

Al-Nemrat, A., Jahankhani, H. & Preston, D.S. (2010). Cybercrime victimisation/criminalisation and punishment. In: Tenreiro de Magalhães, S., Jahankhani, H. & Hessami, A.G. (eds) *Global Security, Safety, and Sustainability*. Cham: Springer.

Amnesty International. (2017). *Amnesty Reveals Alarming Impact of Online Abuse against Women*. Available at: https://www.amnestyusa.org/press-releases/amnesty-reveals-alarming-impact-of-online-abuse-against-women/

Anjum, U. (2020). Cyber crime in Pakistan; Detection and punishment mechanism. *STED Journal*, 2(2), 29-55.

Armiwulan, H. (2021). Gender-based cyber violence: A challenge to gender equality in Indonesia. *International Journal of Cyber Criminology*, 15(2), 102-111.

Bailey, J. (2014). "Sexualized online bullying" through an equality lens: Missed opportunity in *AB v. Bragg*? *McGill Law Journal*, 59(3), 709–737.

Bergmann, M.C., Dreißigacker, A., von Skarczinski, B. & Wollinger, G.R. (2018). Cyber-dependent crime victimization: The same risk for everyone? *Cyberpsychology, Behaviour and Social Networking*, 21(2), 84–90.

Bocij, P. (2004). *Cyberstalking: Harassment in the Internet Age and How to Protect your Family*. Westport, CT: Praeger Publishers.

Buolamwini, J. & Gebru, T. (2018). Gender shades: Intersectional accuracy disparities in commercial gender classification. *Proceedings of the 1st Conference on Fairness, Accountability and Transparency*, 77–91.

Castillo, D. & Falzon, J. (2018). An analysis of the impact of Wannacry cyberattack on cybersecurity stock returns. *Review of Economics and Finance*, 13, 93–100.

Chan, L.-S. (2018). Liberating or disciplining? A technofeminist analysis of the use of dating apps among women in urban China. *Communication Culture & Critique*, 11(2), 298–314.

Citron, D. & Chesney, R. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753-1820.

Cockburn, C. (1983). *Brothers: Male Dominance and Technological Change*. London: Pluto Press.

Cohen, L.E. & Felson, M. (1979). Social change and crime rate trends: A routine activity. *American Sociological Review,* 44(4), 588-608.

Compton, S. (2021). More and more women are facing the scary reality of deepfakes. *Vogue*, 16 March. Available at: https://vogue-int-rocket.prod.cni.digital/deepfakes-and-online-abuse-against-women

Davis, N. & Schmidt, C. (2016). Cyberbullying and cyber abuse intervention: The three-tiered model for schools. *Journal of Creativity in Mental Health*, 11(3-4), 366-367.

Dennehy, D. (2020). Ireland post-pandemic: Utilizing AI to kick-start economic recovery. *Cutter Business Technology Journal*, 33(11), 22-27.

Dhaka Tribune. (2022). *Study: 63.51% of women in Bangladesh face online violence*, 27 November. Available at: https://www.dhakatribune.com/bangladesh/299185/study-63.51%25-of-women-in-bangladesh-face-online

Dunn, S. (2020). *Technology-Facilitated Gender-Based Violence: An Overview*. Centre for International Governance Innovation: Supporting Safer Internet Paper No. 1., available at https://papers.ssrn.com/abstract=3772042

Eaton, A.A. & McGlynn, C. (2020). The psychology of nonconsensual porn: Understanding and addressing a growing form of sexual violence. *Policy Insights from the Behavioral and Brain Sciences*, 7(2), 190–197.

European Institute for Gender Equality (EIGE). (2022). *Cyber Violence against Women and Girls Key Terms and Concepts*. Available at:

https://eige.europa.eu/sites/default/files/cyber_violence_against_women_and_girls_key_terms_and_concepts.pdf

European Parliamentary Research Service. (2021). What if deepfakes made us doubt everything we see and hear? *Science and Technology Podcast*. Available at: https://epthinktank.eu/2021/09/08/what-if-deepfakes-made-us-doubt-everything-we-see-and-hear/

EU Fundamental Rights Agency (FRA). (2014). *Violence against Women: An EU-Wide Survey - Main Results*. Available at: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2014-vaw-survey-main-results-apr14_en.pdf

GREVIO. (2021). *GREVIO General Recommendation No. 1 on the Digital Dimension of Violence against Women*. Council of Europe. Available at: https://rm.coe.int/grevio-rec-no-on-digital-violence-against-women/1680a49147

Ghafur, S., Kristensen, S., Honeyford, K., Martin, G., Darzi, A. & Aylin, P. (2019). A retrospective impact analysis of the WannaCry cyberattack on the NHS. *NPJ Digit Med*, 2(1), 1–7.

Gottfredson, M.R. & Hirschi, T. (1990). *A General Theory of Crime*. Palo Alto: Stanford University Press.

Halder, D. & Jaishankar, K. (2008). Cyber crimes against women in India: Problems, perspectives and solutions. *TMC Academy Journal*, 3(1), 48–62.

Hall, T., Sanders, B., Bah, M., King, O. & Wigley, E. (2021). Economic geographies of the illegal: The multiscale production of cybercrime. *Trends in Organized Crime*, 24(2), 282–30.

Hao, K. (2020). A deepfake bot is being used to “undress” underage girls. *MIT Technology Review*, 12 October. Available at: https://bit.ly/3qj1qWx

Hao, K. (2021). Deepfake porn is ruining women’s lives. Now the law may finally ban it. *MIT Technology Review*, 12 February. Available at: https://www.technologyreview.com/2021/02/12/1018222/deepfake-revenge-porn-coming-ban/

Henry, N., McGlynn, C., Flynn, A., Johnson, K., Powell, A. & Scott, A. J. (2020). *Image-Based Sexual Abuse: A Study on the Causes and Consequences of Non-consensual Nude or Sexual Imagery*. Abingdon: Routledge.

Hinduja, S. & Patchin, J.W. (2010). Bullying, cyberbullying, and suicide. *Archives of Suicide Research*, 14(3), 206–221.

Ho, H.T.N. & Luong, H.T. (2022). Research trends in cybercrime victimization during 2010–2020: A bibliometric analysis. *Springer Nature Social Sciences*, 2(1), 1–32.

Holt, T.J. & Bossler, A.M. (2014). An assessment of the current state of cybercrime scholarship. *Deviant Behaviour*, 35(1), 20–40.

Ibrahim, S. (2016). Social and contextual taxonomy of cybercrime: Socioeconomic theory of Nigerian cybercriminals. *International Journal of Law, Crime and Justice*, 47, 44–45.

Jaishankar, K. (2018). Cyber criminology as an academic discipline: History, contribution and impact. *International Journal of Cyber Criminology*, 12(1), 1-8.

Jane, E.A. (2016). *Misogyny Online: A Short (and Brutish) History*. Los Angeles: SAGE.

Khanna, P. & Khanna, R. (2020). Artificial intelligence and cybercrime- A curate's egg. *Medium*, 14 June. Available at: https://medium.com/the-%C3%B3pinion/artificial-intelligence-and-cybercrime-a-curates-egg-2dbaee833be1

Lazarus, S. (2019). Just married: The synergy between feminist criminology and the tripartite cybercrime framework. *International Social Science Journal*, 69(231), 15–3.

Leukfeldt, R. & Holt, T.J. (2019). *The Human Factor of Cybercrime*. Abingdon:Routledge.

Leukfeldt, E.R., Notté, R.J. & Malsch, M. (2020). Exploring the needs of victims of cyber-dependent and cyber enabled crimes. *Victims & Offenders*, 15(1), 60–77.

Lyons, M. & Blanchard, A. (2016). "I could see, in the depth of his eyes, my own beauty reflected": Women's assortative preference for narcissistic, but not for Machiavellian or psychopathic male faces. *Personality and Individual Differences*, 97, 40-44.

McCarthy, J. (1988). Mathematical logic in artificial intelligence. *Daedalus*, 117(1), 297–311.

McCorduck, P. & Cfe, C. (2019). *Machines Who Think: A Personal Inquiry into the History and Prospects of Artificial Intelligence* (2nd ed.). New York: AK Peters/CRC Press.

Mikkola, M., Oksanen, A., Kaakinen, M., Miller, B.L., Savolainen, I., Sirola, A., Zych, I. & Paek H.-J. (2020). Situational and individual risk factors for cybercrime victimization in a cross-national context. *International Journal of Offender Theories of Comparative Criminology*, 68(5), 449-467.

Mohurle, S. & Patil, M. (2017). A brief study of Wannacry threat: Ransomware attack 2017. *International Journal of Advanced Research in Computer Science*, 8(5), 1938–1940.

Naitali, A., Ridouani, M., Salahdine, F. & Kaabouch, N. (2023). Deepfake attacks: Generation, detection, datasets, challenges, and research directions. *Computers*, 12(10), 216-242.

Näsi, M., Oksanen, A., Keipi, T. & Räsänen, P. (2015). Cybercrime victimization among young people: A multi-nation study. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, 16(2), 203-210.

National Commission on Violence against Women. (2019). *National Human Rights Institution Independent Report on 25 Years of Implementing the Beijing Platform for Action (BPfA+25) in Indonesia*. Available at: https://ngocsw.org/wp-content/uploads/2019/10/Komnas-Perempuan-Independent-Report-BPFA25.pdf

Phillips, K., Davidson, J.C., Farr, R.R., Burkhardt, C., Caneppele, S. & Aiken, M.P. (2022). Conceptualizing cybercrime: Definitions, typologies and taxonomies. *Forensic Science*, 2(2), 379-398.

Powell, A. & Henry, N. (2017). *Sexual Violence in a Digital Age*. London: Palgrave Macmillan.

Rawlinson, K. (2018). Pressure grows on PM over Brexit Cambridge Analytica scandal. *The Guardian*, 26 March. Available at:. https://www.theguardian.com/politics/2018/mar/26/pressure-grows-on-pm-over-brexit-cambridge-analytica-scandal-theresa-may

Reyns, B. W., Henson, B. & Fisher, B.S. (2011). Being pursued online: Applying cyber lifestyle–routine activities theory to cyberstalking victimization. *Criminal Justice and Behavior*, 38(11), 1149-1169.

Sabillon, R., Cavaller, V., Cano, J. & Serra-Ruiz, J. (2016). Cybercriminals, cyberattacks and cybercrime. *IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, 1-9.

Safety Net Canada. (2013). *Executive Summary: Canadian Legal Remedies for Technology-Enabled Violence against Women*. Office of the Privacy Commissioner of Canada.

Sey, A., Kang, J. & Junio, D. R. (2018). *Taking Stock - Data and Evidence on Gender Equality in Digital Access, Skill and Leadership: Preliminary Findings of a Review by the EQUALS Research Group*. United Nations University Institute on Computing and Society. Available at: https://collections.unu.edu/view/UNU:6645

Sikka, T. (2017). Technofeminism and ecofeminism. In D. A. Vakoch & S. Mickey (eds.), *Ecofeminism in Dialogue* (pp. 107–128). Lanham, MD: Lexington Books.

Staude-Müller, F., Hansen, B. & Voss, M. (2012). How stressful is online victimization? Effects of victim's personality and properties of the incident. *European Journal of Developmental Psychology*, 9(2), 260–274.

Todd, P. (2014). *Extreme Mean: Ending Cyberabuse at Work, School, and Home*. Toronto: Signal.

Turing, A.M. (1950). Computing machinery and intelligence. *Mind*, 59(236), 433–460.

Van Der Nagel, E. (2020). Verifying images: Deepfakes, control, and consent. *Porn Studies*, 7(4), 424–429.

Velasco, C. (2022). Cybercrime and artificial intelligence. An overview of the work of international organizations on criminal justice and the international applicable instruments. *ERA Forum*, 23(1), 109–126.

Wajcman, J. (2004). *Technofeminism*. Cambridge: Polity Press.

Wajcman, J. (2006). Technocapitalism meets Technofeminism: Women and technology in a wireless world. *Labour & Industry: A Journal of the Social and Economic Relations of Work,* 16(3), 7-20.

Wajcman, J. (2010). Feminist theories of technology. *Cambridge Journal of Economics*, 34(1), 143-152.

Wajcman, J. & Young, E. (2023). Feminism confronts AI: The gender relations of digitalisation. In J. Browne, S. Cave, E. Drage & K. McInerney (eds.), *Feminist AI: Critical Perspectives on Algorithms, Data, and Intelligent Machines* (p. 47-64). Oxford: Oxford University Press.

Wajcman, J., Young, E. & Fitzmaurice, A. (2020). *The Digital Revolution: Implications for Gender Equality and Women's Rights 25 Years after Beijing*. UN Women Discussion Paper. Available at: https://www.unwomen.org/sites/default/files/Headquarters/Attachments/Sections/Library/Publications/2020/The-digital-revolution-Implications-for-gender-equality-and-womens-rights-25-years-after-Beijing-en.pdf

Wall, D. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Cambridge: Polity Press.

Waldrop, M.M. (2016). How to hack the hackers: The human side of cybercrime. *Nature*, 533, 164-167.

Watters, P.A., McCombie, S., Layton, R. & Pieprzyk, J. (2012). Characterising and predicting cyber attacks using the Cyber Attacker Model Profile (CAMP). *Journal of Money Laundering Control*, 15(4), 430-441.

Whitty, M.T. & Buchanan, T. (2012). The online romance scam: A serious cybercrime. *Cyberpsychology Behaviour and Social Networking*, 15(3), 181–183.

Westerlund, M. (2019). The emergence of deepfake technology: A review. *Technology Innovation Management Review*, 9(11), 40–53.