ADVANCE SOCIAL SCIENCE ARCHIVE JOURNAL
Available Online: https://assajournal.com
Vol. 05 No. 01. Jan-March 2026.Page#.303-321
Print ISSN: 3006-2497 Online ISSN: 3006-2500
Platform & Workflow by: Open Journal Systems
https://doi.org/10.5281/zenodo.18296456

Vulnerability to Empowerment: Digital Literacy as A Shield for Women Against Cyber Harassment

Rehana Anjum
Assistant Professor
Institute of Law, University of Sindh, Jamshoro, Pakistan.
rehana.anjum@usindh.edu.pk
Contact No: +923332624934
Postal Address: Institute of Law, Mitharam Hostel Building, Opposite G.P.O Saddar, Hyderabad
Arun Barkat
Assistant Professor
Institute of Law, University of Sindh, Jamshoro, Pakistan.
arun.barkat@hotmail.com
Contact No: +923452461619
Postal Address: Institute of Law, Mitharam Hostel Building, Opposite G.P.O Saddar, Hyderabad
Rubab Kanwal Shaikh
Student of LLM (Final)
Institute of Law, University of Sindh, Jamshoro, Pakistan.
rubabkanwal117@gmail.com
Contact No: +923103862656
Postal Address: Hala New, District Matiari.

Abstract
Digital literacy encompasses knowledge, skills, and viewpoints that equip individuals to navigate safely and confidently in a progressively digital environment. In today's digital era, women face various cyber threats like harassment, stalking, identity theft, and unauthorized sharing of personal information. These Challenges hinder their online engagement, thereby limiting their access to educational, professional, and personal growth opportunities. Digital literacy is the crucial yet unexplored mechanism in overcoming these challenges, empowering women to navigate the internet securely, protect their digital identities, and uphold their rights. In Pakistan, cybercrimes are dealt with in the Prevention of Electronic Crimes Act (PECA) 2016 which incorporates various provisions to protect women against cyber threats like offenses against the dignity of a natural person, cyber-stalking, unauthorized use of identity information, unauthorized access to intimate images, etc. however, the effectiveness of these legal safeguards is constrained by a deficiency in awareness, accessibility and implementation. This research has employed qualitative doctrinal methodology. Firstly, it aimed to develop a clear understanding of cyber threats encountered by women. Secondly, the study investigated the multi-faceted role of digital literacy in empowering women against cyber threats. Thirdly, this research examined the relationship between digital literacy and Pakistan's legal framework with special reference to the principal provisions of PECA. Fourthly, instant Research formulated strategies to bridge the gap through targeted digital literacy programs, enhanced legal education, and policy reforms. Finally,

the research concluded with recommendations to promote gender-responsive policies ensuring women's empowerment.
Key Words: *Digital-literacy, Cyber-threats, PECA, Policy-reforms, Cyber harassment.*

1) Introduction

The increasing digitalization of society has provided individuals with unparalleled access to information, communication, and economic prospects. Nevertheless, it has simultaneously subjected women to various cyber threats, such as online harassment, cyberstalking, identity theft, and the unauthorized dissemination of personal data. These types of cyber harassment not only infringe upon privacy rights but also impede women's full engagement in digital environments, thereby limiting their social, educational, and professional development.

Digital skills and competencies have transitioned from being optional to becoming essential. In today's societies characterized by pervasive technology, the capacity to effectively utilize digital tools is increasingly vital for an individual's overall well-being, paralleling the importance of numeracy and literacy. Lacking the ability to manage technology may lead individuals to be dominated by it or to experience disconnection from local, national, and global communities. In response to this reality, educational systems are striving to provide equitable, inclusive, and high-quality education and training in digital skills. The urgency of these initiatives is heightened by the fact that digital competencies facilitate access to further learning and skill enhancement. Indeed, it is challenging to identify two more significant catalysts for lifelong learning than the abilities to read and write, alongside the capability to leverage digital technology and navigate the internet. The situation regarding digital skills education is concerning and pervasive: women and girls are increasingly marginalized. Worldwide, the disparities in digital skills between genders are widening, despite more than ten years of concerted national and international initiatives aimed at bridging these gaps.[1]

The notion of digital literacy has gained significant prominence in the 21st century. The escalating requirements from the labor market for individuals to possess digital competencies have led to focused initiatives and innovations within the educational sphere aimed at equipping the future workforce with essential digital skills. Nevertheless, despite these endeavors, the digital skills gap continues to be evident on a global scale.[2] The advancement of technology and its application in the realm of digitalization has catalyzed a growing demand for digital education. As dependence on digital technology escalates, it is imperative to carefully examine the ways in which individuals engage with digital tools, the nature of their online interactions, and the competencies they possess to effectively navigate the tasks linked to digitalization.

2) Background of the Study

The rapid advancement of digital technology has rendered online environments crucial for personal, educational, and professional interactions. However, this growing reliance on digital platforms has simultaneously subjected women to a range of cyber threats, such as harassment, stalking, identity theft, and the unauthorized dissemination of personal information. These dangers not only jeopardize women's privacy and safety but also discourage their full engagement in digital arenas. Although legal frameworks like Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 exist, persistent deficiencies in awareness, accessibility, and enforcement continue to leave women exposed to cybercrimes. Digital literacy emerges as a vital

[1] West, M., Kraut, R., & Ei Chew, H. (2019). I'd blush if I could: closing gender divides in digital skills through education.

[2] Reddy, P., Chaudhary, K., & Hussein, S. (2023). A digital literacy model to narrow the digital literacy skills gap. *Heliyon*, *9*(4).

yet often overlooked resource that can empower women with the essential knowledge and skills needed to effectively navigate these online dangers. By promoting awareness and improving digital skills, digital literacy acts as a protective barrier, enabling women to defend their identities, report instances of cyber harassment, and assert their rights within the digital landscape. The continuous rise in digital technologies and services has resulted in a dichotomy of digital inclusion and exclusion among individuals. Those who lack digital literacy are more likely to encounter difficulties in managing various aspects of their lives, which in turn increase the risk of facing challenges in engaging with and adapting to the digital landscape.[3]

Digital literacy emerges as important yet often overlooked resource in empowering women to effectively navigate these online dangers. By improving their comprehension of cyber-security, privacy safeguards, and available legal remedies, digital literacy can equip women to protect their digital identities and take proactive measures against cyber harassment. In Pakistan, the Prevention of Electronic Crimes Act (PECA) 2016 offers legal safeguards against cyber offenses. However, challenges such as limited awareness, accessibility issues, and inadequate enforcement mechanisms undermine the law's capacity to ensure women's digital safety.

3) Research Problem

In Pakistan, women come across through various increasing threats in digital spaces but many of them lack necessary digital literacy to protect themselves against cyber harassment. However, in Pakistan, legal frameworks like PECA 2016 exist, their effectiveness is hindered by limited awareness, enforcement challenges, and the digital gender discrimination. Without adequate digital literacy, women remain susceptible to cyber threats that hinder their participation in online education, employment, and social engagement. This research seeks to explore the role of digital literacy in empowering women against cyber harassment and to assess the existing legal framework's ability to provide adequate protection.

1) Significance of the Study

This research holds significance as it highlights the vital role of digital literacy in mitigating cyber threats against women, thereby contributing to their empowerment in the digital age. This research provides actionable recommendations for policymakers, educators, and law enforcement agencies by highlighting gaps in legal protections and digital education. The findings can acquaint with initiatives aimed at bridging the digital gender divide, strengthening cyber-security measures, and promoting gender-inclusive legal reforms. Eventually, the study aims to encourage a safer digital environment for women, enabling their full participation in online spaces without fear of harassment or exploitation.

2) Research Objectives

This research aims to attain the following objectives;

- To identify the prevalent cyber threats faced by women in Pakistan.
- To examine the role of digital literacy in protecting women from cyber harassment.
- To evaluate the effectiveness of Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 in addressing cyber threats against women.
- To explore strategies for integrating digital literacy and legal awareness into women's empowerment initiatives.
- To recommend policy reforms and educational interventions to enhance women's digital safety and inclusion.

[3] Reddy, P., Sharma, B., & Chaudhary, K. (2020). Digital literacy: A review of literature. *International Journal of Technoethics (IJT)*, *11*(2), 65.

3) Research Questions

This research aims to answer following questions;

- What are the most common forms of cyber harassment experienced by women in Pakistan?
- How does digital literacy contribute to women's ability to protect themselves from online threats?
- To what extent does PECA 2016 provide legal safeguards against cyber harassment?
- What challenges hinder the implementation of digital literacy programs for women?
- What measures can be adopted to improve women's digital literacy and access to legal protections against cyber threats?

4) Understanding Cyber Harassment Against Women

7.1 Defining Cyber Harassment

Cyber harassment represents a significant risk associated with the utilization of digital technologies. This form of harassment can occur across various platforms, including social media, messaging applications, and mobile devices. Characterized by its repetitive nature, it seeks to intimidate, instill fear, humiliate, and suppress the voices of its victims.[4] Cyber harassment encompasses the utilization of digital platforms, including social media, email, messaging applications, and online discussion forums, to threaten, intimidate, or demean individuals. This form of online abuse manifests in various ways, such as cyberstalking, issuing online threats, doxxing (the unauthorized disclosure of personal information), and disseminating false or damaging information.

In contrast to conventional harassment, cyber harassment enables offenders to maintain anonymity while targeting victims remotely, complicating efforts to identify and intervene against them. Women are particularly vulnerable to gender-based cyber harassment, which may include misogynistic remarks, the non-consensual distribution of private images, and various forms of online sexual harassment.

The repercussions of cyber harassment can be profoundly detrimental, resulting in significant psychological, emotional, and social challenges for victims, including heightened anxiety, depression, and potential withdrawal from digital interactions. It is imperative to recognize and address this phenomenon to foster safer online environments for all individuals.

7.2 Common Cyber Threats Faced by Women

In today's digital landscape, women are increasingly confronted with a myriad of cyber threats that jeopardize their privacy, security, and mental health. The pervasive nature of social media, online communication tools, and digital financial transactions has facilitated the exploitation, intimidation, and abuse of women by cybercriminals and harassers. Unlike conventional forms of harassment, cyber threats often enable offenders to operate anonymously, complicating efforts to hold them accountable for their actions.

Women face distinct risks ranging from cyberstalking and online harassment to doxxing and the non-consensual sharing of images, all of which can lead to significant emotional, psychological, and even physical repercussions. These threats not only infringe upon personal privacy but also hinder women's ability to express themselves freely and engage fully in online communities. Recognizing these cyber threats is essential for fostering awareness, improving digital safety, and advocating for more robust legal protections. By understanding the risks and adopting proactive security strategies, women can enhance their defenses against online abuse and contribute to creating a safer digital environment for everyone.

[4] Cyber-Harrasment: Self-Protection. (n.d). Retrieved on dated 14 February 2025 from Cyber-harassment: self-protection tips | Investigative Team to Promote Accountability for Crimes Committed by Da'esh/ISIL (UNITAD)

The rise in Internet usage has led to an escalating threat of online dangers, such as cyber stalking and cyber harassment. Nevertheless, there exists a paucity of research examining the effects of these online harms on the well-being of adults.[5]

Women are frequently subjected to a range of cyber threats that are disproportionately influenced by gender-based discrimination and online misogyny. Among the prevalent cyber threats encountered by women are:

a) Cyberstalking

Cyberstalking is defined as the act of utilizing the internet and various technological means to intimidate or pursue an individual in a digital environment.[6] Previous studies have categorized cyberstalking into four primary types that include vindictive, composed, intimate, and collective. Vindictive cyberstalking is characterized by threats directed at the victim, while composed cyberstalking is marked by persistent annoyance and harassment. Intimate cyberstalking typically involves former partners or individuals who have developed an obsession with the victim. Lastly, collective cyberstalking occurs when a victim is targeted by a group of individuals.[7] Cyberstalking represents relatively a new issue that has not been extensively studied within the empirical research framework. As a result, the prevalence rates associated with this crime are often inconsistent and subject to significant fluctuations. The underreporting of cyberstalking incidents is likely attributable to a general lack of awareness within the community regarding the specific behaviors that define this form of harassment. Various factors inherent to the nature of cyberstalking may influence both the likelihood of reporting the crime and the degree to which accountability is assigned to either the perpetrator or the victim.[8] The pervasive use of technology-driven communication platforms, particularly social media, has garnered academic attention due to the escalating occurrences of cyberstalking. Although there has been a notable increase in research addressing cyberstalking in the last ten years, efforts to develop a thorough and integrative understanding of this phenomenon from an academic standpoint remain scarce.[9]

b) Online Harassment and Trolling

Women often encounter hate speech, derogatory comments, and personal assaults on social media platforms. This phenomenon encompasses abusive remarks, threats, and coordinated harassment efforts designed to silence or intimidate them. Trolling constitutes a collective manifestation of harassment, characterized by the intent to maliciously provoke another individual online.[10] A recent examination of studies concerning gender-based and sexualized online harassment indicates that the limited research involving adults consistently reveals that sexual harassment disproportionately impacts women, both in terms of prevalence and consequences, with young women being especially vulnerable.[11] Research has indicated that

[5] Stevens, F., Nurse, J. R., & Arief, B. (2021). Cyber stalking, cyber harassment, and adult mental health: A systematic review. *Cyberpsychology, Behavior, and Social Networking*, *24*(6), 367.

[6] Gorden, S. (2024). How to Protect Yourself From Cyber-Stalking: When Online Creeping Goes Too Far. Retrieved on dated 14 February 2025 from Cyberstalking: Definition, Signs, Examples, and Prevention .

[7] MacFarlane, L., & Bocij, P. (2003). An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers. *First monday*, *8*(9).

[8] Ahlgrim, B., & Terrance, C. (2021). Perceptions of cyberstalking: Impact of perpetrator gender and cyberstalker/victim relationship. *Journal of interpersonal violence*, *36*(7-8), NP4074-NP4093.

[9] Kaur, P., Dhir, A., Tandon, A., Alzeiby, E. A., & Abohassan, A. A. (2021). A systematic literature review on cyberstalking. An analysis of past achievements and future promises. *Technological Forecasting and Social Change*, *163*, 120426.

[10] Ortiz, S. M. (2020). Trolling as a collective form of harassment: An inductive study of how online users understand trolling. *Social Media+ Society*, *6*(2), 2056305120928512.

[11] Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, violence, & abuse*, *19*(2), 195.

while the overall gender differences in experiences of online harassment may be minimal, the types of harassment encountered by men and women differ significantly. Specifically, men are more frequently subjected to name-calling and physical threats, whereas women are more often targeted with sexual harassment.[12] There is an increasing focus on gender-based online harassment, evident in both academic research and public discourse. A multitude of documented instances strongly suggests that women are especially susceptible to becoming targets of such harassment.[13]

c) Doxxing (Exposure of Personal Information)

The term "doxxing" is an abbreviation for "dropping documents", referring to the act of publicly disclosing documents containing personal information about an individual on the internet. This practice is employed by hackers as a means to expose the identities of individuals who were previously anonymous, to reveal their physical locations, and to undermine the credibility of those individuals.[14] Doxxing constitutes a type of cyber harassment wherein an individual's private information such as their residential address, telephone number, employment details, or financial data is disclosed publicly on the internet without their permission. This act is typically executed with harmful intentions, seeking to intimidate, harass, or jeopardize the safety of the victim. Women, particularly those in prominent positions or engaged in activism, are often the primary targets of doxxing, as it serves as a tactic to silence or threaten them. The repercussions can be grave, encompassing online harassment, identity theft, and tangible threats such as stalking or physical violence. Offenders may acquire this sensitive information through methods such as hacking, social engineering, or by compiling data from publicly accessible resources. To safeguard against doxxing, individuals are advised to restrict the personal information they disclose online, implement robust privacy settings, and consistently review their digital presence. In the event of being doxxed, it is crucial to report the situation to relevant platforms, law enforcement agencies, or cybersecurity experts to help alleviate potential risks.

d) Non-Consensual Image Sharing (Revenge Porn)

The unauthorized dissemination of private images (NDII) occurs when an individual captures or shares an intimate photograph or video of another person without their consent. This act is also referred to as image-based sexual abuse, nonconsensual pornography, or revenge porn.[15] Non-consensual image sharing, frequently referred to as revenge porn, involves the dissemination of private or explicit photographs or videos without the consent of the individual portrayed. This act is typically motivated by a desire to shame, humiliate, or extort the victim. Often, these images were initially shared in a private context, such as between intimate partners, and subsequently exploited as a means of retribution following a separation or dispute. Additionally, there are cases where hackers or cybercriminals unlawfully access and distribute such material.

e) Phishing and Online Scams

Phishing constitutes a form of social engineering cyber threat in which malicious actors masquerade as reputable entities to deceive individuals into disclosing confidential information,

[12] Aardal, B., Bergh, J., & Karlsen, R. (2013). Hvorfor stemmer velgerne som de gjør?. *Valg og velgere. En studie av stortingsvalget*.

[13] Nadim, M., & Fladmoe, A. (2021). Silencing women? Gender and online harassment. *Social Science Computer Review*, *39*(2), 245

[14] Eckert, S., & Metzger-Riftkin, J. (2020). Doxxing, privacy and gendered harassment. The shock and normalization of veillance cultures. *M&K Medien & Kommunikationswissenschaft*, *68*(3), 273.

[15] Nonconsensual Distribution of Intimate Images: What To Know. (2024). Retrieved on dated 13 February 2025 from https://consumer.ftc.gov/articles/nonconsensual-distribution-intimate-images-what-know

such as passwords, credit card details, or personally identifiable information.[16] Phishing represents a fraudulent cyber assault in which perpetrators masquerade as credible entities, including financial institutions, social networking sites, or e-commerce platforms, with the intent of deceiving individuals into disclosing confidential information. These schemes typically manifest as emails, text messages, or counterfeit websites aimed at appropriating personal data, such as passwords, credit card information, and social security numbers. Women are often disproportionately affected by phishing schemes, particularly through communications that manipulate emotional responses, such as counterfeit employment opportunities, romantic deceptions, or alarming notifications regarding account deactivation. Phishing scams have experienced significant growth in recent years, driven by advantageous economic and technological factors. The necessary technical tools for conducting phishing attacks are easily accessible from both public and private channels. Furthermore, certain technical resources have been optimized and automated, enabling individuals without technical expertise to engage in such criminal activities. Consequently, phishing has become both economically and technically feasible for a broader demographic of less experienced offenders.[17]

Online fraudsters employ various strategies, including fraudulent investment opportunities, lottery scams, and impersonation schemes, to deceive women into transferring funds or granting access to their accounts. Additionally, cybercriminals may compromise social media accounts to disseminate phishing links to the victim's contacts, thereby amplifying the reach of the scam. To safeguard against phishing and online fraud, it is essential to authenticate the legitimacy of communications, refrain from engaging with dubious links, and activate two-factor authentication on accounts. Vigilance and awareness are paramount in protecting oneself from these digital dangers

f) Sextortion

Sextortion constitutes a type of sexual exploitation wherein offenders coerce victims, frequently minors, by threatening to disseminate intimate images. This manipulation aims to compel the victims into compliance, which may include actions such as transferring money, providing gift cards, or sharing additional sexual photographs and videos.[18] “Sextortion not only causes great individual harm, but, like other forms of corruption, has far-reaching implications for gender equity, democratic governance, economic development, and peace and stability”.[19] Sextortion represents a type of cyber-enabled extortion in which offenders threaten to disseminate explicit photographs, videos, or communications of a victim unless their demands are met. Such demands can encompass monetary payments, further explicit material, or personal services. The process of sextortion frequently initiates with cybercriminals gaining unauthorized access to a victim’s devices, employing deep fake technology to alter private images, or pressuring individuals into providing intimate content under deceptive circumstances. This crime predominantly targets women, particularly young girls, social media influencers, and professionals.

5) The Role of Digital Literacy In Women’s Empowerment

[16] Stouffer, C. (2024). What Is Phishing? Retrieved on dated 13 February 2025 from https://us.norton.com/blog/online-scams/what-is-phishing

[17] Milletary, J., & Center, C. C. (2005). Technical trends in phishing attacks. *Retrieved December*, *1*(2007), 1.

[18] Barrett, S. (2024, November 26). Sextortion: Laws, penalties, and help for victims. UC Law San Francisco. Retrieved on dated 14 February 2025 from https://www.criminaldefenselawyer.com/resources/sextortion-laws-penalties-and-help-for-victims.html

[19] Hendry, N. H. (2021). Sextortion. *The Fourth Industrial Revolution and Its Impact on Ethics: Solving the Challenges of the Agenda 2030*, 315-320.

Digital literacy is essential for empowering women, equipping them with the necessary knowledge and skills to navigate the digital landscape both safely and effectively. In the contemporary technology-oriented society, access to digital resources, online learning, and career opportunities can greatly contribute to the personal and economic advancement of women. Digital literacy skills for women extend beyond mere reading and writing capabilities facilitated by digital technologies; they also encompass fundamental skills and attitudes or perspectives regarding technology. Digital literacy is not limited to the proficiency in using software or operating digital devices; rather, it includes a range of intricate cognitive, motor, sociological, and emotional competencies that are essential for individuals to navigate and thrive in the digital landscape.[20] Digital Literacy plays a vital role in empowering women in the following ways;

a) Bridging the Digital Divide

The digital divide denotes the disparity between individuals who possess access to digital technologies and the internet and those who lack such access. This issue is particularly pronounced for women, especially in rural and marginalized regions, where cultural, economic, and infrastructural obstacles hinder their ability to utilize digital tools and acquire necessary skills. Addressing this divide is crucial for promoting gender equality in areas such as education, employment, and social engagement.

A significant contributor to the digital divide is the absence of affordable internet connectivity and digital devices. Numerous women in developing nations face financial constraints that prevent them from purchasing smartphones, computers, or internet services, thereby impeding their ability to engage with online educational resources, job prospects, or vital digital services. Furthermore, prevailing societal norms and gender biases frequently limit women's access to technology, thereby restricting their opportunities to develop digital competencies or enter technology-oriented professions.

b) Enhancing Economic Opportunities

Digital literacy is essential for enhancing economic prospects for women, as it grants them access to online employment markets, entrepreneurial resources, and financial tools. By acquiring digital skills, women can engage in remote work, freelancing, and online business ventures, thereby overcoming conventional obstacles that hinder their professional advancement. Various platforms, including e-commerce sites, social media marketing, and digital banking, empower women to establish and operate their own businesses with relatively low initial investment. Digital literacy has the potential to significantly increase women's involvement in socio-economic activities. It offers them platforms for self-expression and fosters social transformation as they acquire access to a wealth of global knowledge.[21]

c) Promoting Online Safety and Security

Ensuring the safety and security of women in the online realm is paramount for fostering their confidence and enabling them to navigate the digital landscape without apprehension. The increasing prevalence of cyber threats, including cyberstalking, identity theft, hacking, and online harassment, underscores the importance of digital literacy in safeguarding personal information and preserving privacy. It is imperative that women are encouraged to adopt robust passwords, activate two-factor authentication, and exercise caution when disclosing personal information online. Developing an awareness of how to identify phishing attempts, fraudulent activities, and

[20] Hufad, A., Purnomo, N. S., & Rahmat, A. (2019). Digital literacy of women as the cadres of community empowerment in rural areas. *International Journal of Innovation, Creativity and Change*, *9*(7), 277.

[21] Anzak, S., & Sultana, A. (2020). Social and economic empowerment of women in the age of digital literacy: A case study of Pakistan, Islamabad-Rawalpindi. *Global Social Sciences Review*, *1*, 104.

harmful links is essential in mitigating the risk of cybercrimes. Furthermore, a comprehensive understanding of privacy settings on social media platforms and the ability to report abusive conduct are critical components in establishing a safer online environment. It is also essential for governments, organizations, and technology companies to enforce stringent policies and security protocols to address digital abuse effectively. By advocating for online safety and empowering women with cybersecurity knowledge, we can cultivate an inclusive digital ecosystem that allows them to express themselves freely, seize opportunities, and engage in the digital economy without fear.

d) Access to Education and Information

Digital literacy plays a crucial role in improving women's access to education and information, effectively dismantling conventional obstacles to learning. The emergence of online educational platforms allows women to engage in academic studies, vocational training, and skill enhancement from virtually any location globally. This is particularly advantageous for those residing in remote regions, where educational facilities may be scarce. Digital resources, including e-books, virtual classrooms, and online research databases, equip women with essential knowledge, thereby broadening their expertise and enhancing their career opportunities. Enhancing women's digital literacy has resulted in substantial beneficial effects on both their individual lives and the broader community.[22] Furthermore, access to information enables women to remain informed about their rights, health matters, financial prospects, and societal issues. By utilizing digital tools, women are empowered to make educated choices, participate in dialogues, and advocate for social change. Ultimately, digital literacy redefines education as a more accessible and inclusive domain, promoting lifelong learning and empowerment for women from diverse backgrounds.

e) Strengthening Social and Political Participation

Digital literacy plays a crucial role in enhancing women's economic prospects, educational achievements, access to healthcare, and engagement in political processes, thus facilitating progress towards the Sustainable Development Goals.[23] Digital literacy enables women to participate meaningfully in social and political discourse, thereby enhancing their influence in decision-making arenas. By utilizing social media, online discussion platforms, and digital advocacy campaigns, women can champion issues related to gender equality, human rights, and legislative reforms that affect their daily lives. These digital environments create opportunities for women to network with others who share similar values, engage in collective movements, and take part in online activism, thereby amplifying their concerns to a broader audience.

6) Digital Literacy and Pakistan's Legal Framework

Digital literacy is vital for empowering women to comprehend and maneuver through Pakistan's legal landscape related to cyber threats. In an era characterized by increasing incidents of cyber harassment, online fraud, and data breaches, awareness of legal protections is imperative for the preservation of women's rights and their online safety. The Prevention of Electronic Crimes Act (PECA) 2016 stands as the principal legislative framework in Pakistan that tackles cybercrimes, providing legal recourse for victims of online harassment, cyberstalking, identity theft, and the unauthorized distribution of images. Digital platforms and social media have facilitated access to information, educational resources, and opportunities for skill

[22] Debbarma, A., & Chinnadurai, A. S. (2023). Empowering women through digital literacy and access to ICT in Tripura. *Research Journal of Advanced Engineering and Science*, *9*(1), 5.

[23] Aslam, A., Abidi, S. N. M., & Rizvi, S. S. A. (2024). Digital Literacy and Women's Empowerment: Bridging the Gender Gap in Technology for Achieving Sustainable Development Goals (SDGs). *Pakistan Journal of Gender Studies*, *24*(2), 93.

enhancement. Women have leveraged these digital tools to pursue entrepreneurship and achieve economic empowerment.[24]

9.1 Understanding PECA 2016: Legal Protections Against Cyber Threats

On August 11, 2016, Pakistan enacted the Prevention of Electronic Crimes Act (PECA) to mitigate radical online content, hate speech, and harassment. The PECA encompasses various provisions aimed at addressing online harassment and safeguarding women's rights. Specifically, Sections 18, 19, and 21 focus on cybercrimes that infringe upon women's dignity and privacy. However, these provisions lack precise definitions of the offenses, leading to ambiguity that hampers the effective enforcement of the law. While the act establishes a framework intended to combat crimes against women, it is essential to explore the broader implications of the PECA and the factors contributing to its ineffectiveness, as it has not succeeded in protecting women in the digital realm. Furthermore, it is vital to examine the deficiencies in its enforcement and the consequent effects on women's freedom of expression in the online environment. The institutional shortcomings of the PECA are rooted in its vague provisions and inconsistent enforcement. Section 18, while not specifically aimed at addressing online harassment of women, pertains to certain forms of reputational harm associated with harassment and violations of women's dignity. This section presents challenges in the context of human rights law, particularly due to the inclusion of criminal defamation. Likewise, Article 19 addresses the unauthorized use of images for sexually explicit purposes, stipulating that any individual who intentionally and publicly displays or disseminates information without the consent of the individual involved may face a penalty of up to seven years in prison, a fine of up to five million Rupees, or both.

This section exhibits several shortcomings, particularly due to the absence of explicit criteria defining what is meant by "sexually explicit". The Prevention of Electronic Crimes Act (PECA), initially praised for its role in criminalizing online harassment and various forms of cybercrime, has now become a refuge for such offenses, particularly when they are perpetrated to protect the interests of the state or government.[25] Additionally, it fails to address other significant factors that may contribute to the distress of women. Under Section 21 of the PECA, cyberstalking is defined as an offense committed by an individual who utilizes cyberspace "with the intent to coerce or intimidate or harass any person", such individuals are subject to penalties. However, similar to other provisions, the characterization of cyberstalking in this section remains unclear, potentially criminalizing behaviors that may not universally be regarded as criminal. Consequently, the provisions of the act that pertain to the privacy and dignity of women in the digital realm lack precision. The interpretations of these sections are largely speculative, which undermines the effectiveness and enforcement of the PECA. The structural inefficacy of enforcement agencies, including the Federal Investigation Agency (FIA), the judiciary, the Pakistan Telecommunication Authority (PTA), and service providers, has resulted in numerous obstacles for female victims of online crimes. In October 2018, the FIA observed a significant surge in cybercrimes within Pakistan. During this period, it undertook 2,295 inquiries, filed 225 cases, and executed 209 arrests, marking the highest numbers recorded since the implementation of the Prevention of Electronic Crimes Act (PECA).[26]

---

[24] Akmal, Z., & Usmani, S. A. A. (2024). Digital Rights and Women's Empowerment in Pakistan: An Analysis of Contemporary Islamic Legal Perspectives in the Age of Social Media. *MILRev: Metro Islamic Law Review*, *3*(1), 95.

[25] Shahid, K. K. (2020, May 9). Five years of PECA: The law that tried to silence Pakistan. Pakistan | Gender and Sexual Diversity. Retrieved on dated 14 February 2025 from Five years of PECA: The law that tried to silence Pakistan - IFEX

[26] Riaz, K. (2021, March 26). Does PECA Law Empower Women. Retrieved on dated 14 February 2025 from https://cscr.pk/explore/themes/social-issues/does-peca-law-empower-women/

The lives of women have been significantly affected by the inadequate implementation mechanisms of the Prevention of Electronic Crimes Act (PECA). Cybercrimes targeting women have not only restricted their freedom of expression but have also fostered a sense of cyber timidity among them. These offenses have intensified the fear of online harassment among women and girls, discouraging them from engaging with social media platforms. A psychologist from Peshawar has identified a strong correlation between cyber violence and mental health challenges faced by women. Consequently, it is imperative that the PECA incorporates specific provisions addressing cyber harassment against women.

Despite the existing shortcomings of the Act, there is potential for enhancement through proactive measures. The sections of the PECA pertaining to women, which currently lack clarity and precision, should be revised to delineate offenses against women in a more specific and comprehensible manner. Furthermore, the effectiveness of this legislation hinges on the implementation process; thus, it is essential to bolster the enforcement agencies responsible for the PECA to effectively combat online violence against women and promote cybersecurity and women's empowerment. Additionally, a system of checks and balances should be established to oversee the actions of these enforcement agencies. Should the current law prove unamendable, the introduction of a new cybercrime statute specifically for women could be pursued through legislative discourse, thereby creating a safer online environment for women in Pakistan.

In short, the PECA has largely been ineffective to date due to its inherent flaws and inadequate mechanisms. However, as the significance of cyberspace continues to grow, it is crucial to address the deficiencies within the PECA and its institutional framework. Such initiatives will facilitate the inclusion of women in the digital landscape by safeguarding their online rights and enhancing their participation in the virtual sphere.

7) Bridging The Gap: Digital Literacy and Legal Reforms

The digital revolution has fundamentally altered various dimensions of our existence, influencing areas such as communication, commerce, education, and healthcare. Nevertheless, this change has not been uniform, resulting in substantial portions of the population being excluded due to insufficient access to the necessary tools and skills for full engagement in the digital landscape. This gap, referred to as the digital divide, represents a considerable challenge to social and economic inclusion, intensifying pre-existing inequalities and obstructing both individual and community advancement.[27] In light of the growing dependence on digital platforms, a significant number of women in Pakistan continue to face heightened risks from cyber threats, primarily due to insufficient digital literacy and a lack of awareness regarding legal protections. To mitigate this issue, it is crucial to implement targeted digital literacy initiatives alongside necessary policy reforms. These efforts should aim to empower women with the skills required to safely navigate the digital landscape, while also ensuring that legal instruments, such as the Prevention of Electronic Crimes Act (PECA) 2016, are effectively enforced and made accessible. Enhancing legal education, increasing cybersecurity awareness, and advocating for gender-sensitive policies can contribute to fostering a safer online environment for women.

In today's digital landscape, the protection of women's safety online necessitates robust initiatives in digital literacy alongside comprehensive legal reforms. Numerous women encounter various cyber threats, including harassment, identity theft, and online exploitation, yet many remain unaware of the legal protections available to them. Addressing this knowledge gap is crucial for empowering women to safely engage in digital environments and pursue legal

[27] Mahmood, K., & Liu, Y. (2023). Bridging the digital divide: Strategies for inclusive access to technology. University of Engineering and Technology (UET) & Tsinghua University.

remedies when necessary. Enhancing digital education, refining legal structures, and promoting collaboration among relevant stakeholders are vital measures in this endeavor.

Following are certain strategies to bridge the divide between digital literacy and legal reforms.

a) Enhancing Digital Literacy Program

Enhancing digital literacy among women is essential for closing the gender gap in technology access and enabling them to effectively navigate the digital environment with confidence. In Pakistan, there is a notable digital gender disparity, as only 26% of women have access to the internet, in contrast to 47% of men.[28] The existing inequality constrains women's access to education, job prospects, and participation in social activities. In the contemporary digital landscape, it is imperative for women to possess the necessary knowledge and skills to safely traverse online environments. The enhancement of digital literacy initiatives is essential for informing women about cybersecurity, online privacy, and prudent internet usage. Such programs ought to encompass subjects including the identification of phishing schemes, the protection of personal data, the creation of robust passwords, and the recognition of cyber threats, including harassment and identity theft.

b) Improving Awareness of Legal Rights

Raising awareness of legal rights is crucial for empowering women to defend themselves against cyber threats and pursue justice in cases of online harassment. A significant number of women lack knowledge regarding the legal protections available to them, such as the Prevention of Electronic Crimes Act (PECA) 2016 in Pakistan, which addresses offenses like cyberstalking, identity theft, and the unauthorized distribution of private images. Enhancing awareness through digital literacy initiatives, workshops, and online outreach can inform women about their rights, available legal recourse, and the appropriate procedures for reporting cybercrimes. Furthermore, partnerships among government entities, educational institutions, and civil society organizations can facilitate the accessibility, simplification, and widespread distribution of legal information. Establishing legal helplines, online resources, and awareness campaigns can also help close the gap between law enforcement and victims, thereby empowering women to take decisive action against cyber offenders.

c) Strengthening Law Enforcement Training

Effective law enforcement plays a vital role in combating cybercrimes targeting women; however, a significant number of officers lack the necessary specialized training to address these digital offenses with the required sensitivity and efficiency. Enhancing law enforcement training is essential, as it involves providing officers with the technical expertise needed to investigate cyber threats, utilize digital forensic tools, and comprehend relevant cyber legislation, such as the Prevention of Electronic Crimes Act (PECA) 2016. Furthermore, incorporating gender-sensitive training is critical to ensure that officers can respond appropriately to victims of online harassment, cyberstalking, and digital extortion. The reluctance of many women to report cybercrimes stems from fears of being dismissed or blamed, underscoring the importance of adopting a victim-centered approach. Collaborating with digital experts, non-governmental organizations, and legal professionals can facilitate the development of comprehensive training programs and workshops for law enforcement agencies. By enhancing the capabilities of law enforcement, victims will be more likely to trust the legal system, resulting in improved reporting, investigations, and prosecution of cybercriminals.

d) Integrating Digital and Legal Education

[28] Irfan, A. (2023). The Digital Gender Gap, a major obstacle to the fight for equality for women in Pakistan. Retrieved on dated 14 February 2025 from The digital gender gap, a major obstacle to the fight for equality for women in Pakistan | International | EL PAÍS English.

The integration of digital literacy into legal education is crucial for empowering women with the necessary knowledge and resources to navigate online environments securely while comprehending their legal entitlements. Numerous women in Pakistan and globally encounter cyber threats, including online harassment, cyberstalking, and identity theft, yet they frequently lack awareness of the legal safeguards that exist to protect them. By embedding digital safety education and legal awareness initiatives within educational institutions and community organizations, women can acquire the competencies required to identify cyber threats, protect their personal data, and pursue legal recourse when needed.

It is imperative for educational bodies and governmental programs to collaborate in the development of curricula that encompass subjects such as cybersecurity, responsible digital citizenship, and the Prevention of Electronic Crimes Act (PECA) 2016. Furthermore, training initiatives aimed at law enforcement, legal practitioners, and policymakers should prioritize the effective handling of gender-based cybercrimes. By closing the divide between digital literacy and legal understanding, women can be empowered to assert their rights and foster a safer digital landscape.

e) Making Legal Support More Accessible

One of the primary obstacles that women encounter in addressing cyber threats is the insufficient availability of effective legal support. Numerous victims of online harassment, cyberstalking, and digital fraud either lack awareness of their legal entitlements or find it challenging to navigate the intricate procedures involved in filing complaints. To address this issue, governments, and legal institutions must create specialized cybercrime helplines, online complaint systems, and legal aid centers that are sensitive to the needs of women, thereby facilitating prompt action against offenders. Awareness initiatives addressing cyber harassment should be implemented for women across various professions and social demographics.[29] Furthermore, incorporating legal awareness initiatives into digital literacy programs can equip women with essential knowledge regarding their rights, particularly under legislation such as the Prevention of Electronic Crimes Act (PECA) 2016 in Pakistan. Collaborating with non-governmental organizations (NGOs), legal professionals, and technology platforms can further improve accessibility by providing free legal advice, assistance with reporting processes, and support services for victims. By streamlining legal procedures and ensuring the effective enforcement of cyber laws, a greater number of women will be able to pursue justice and safeguard themselves against online harassment.

f) Reforming Cybercrime Laws

As digital threats continue to advance, there is an increasing necessity to revise cybercrime legislation to effectively tackle issues such as online harassment, identity theft, and various other cyber-related offenses. In Pakistan, the Prevention of Electronic Crimes Act (PECA) 2016 functions as the main legal structure for addressing cybercrimes. Nonetheless, critics contend that the law needs modifications to bolster protections for women, simplify reporting processes, and enhance enforcement mechanisms. Numerous victims of cyber harassment encounter significant obstacles in obtaining justice, stemming from a lack of awareness, protracted legal processes, and insufficient training for law enforcement personnel. Enhancing legal provisions, implementing more stringent penalties for offenders, and integrating gender-sensitive strategies into cyber legislation could contribute to establishing a safer digital landscape for women. Furthermore, adopting international best practices, such as those outlined in the Budapest

[29] Qureshi, S. F., Abbasi, M., & Shahzad, M. (2020). Cyber harassment and women of Pakistan: analysis of female victimization. *Journal of Business and Social Review in Emerging Economies*, *6*(2), 503.

Convention on Cybercrime, could provide valuable guidance for Pakistan in refining its legislative framework and enforcement approaches.

g) Collaboration Between Government and Tech Companies

Collaboration between governmental entities and technology firms is crucial for fostering a safer online environment for women. Governments are instrumental in formulating and enforcing cyber legislation, while technology companies manage the platforms that facilitate the majority of online interactions. Through cooperative efforts, these stakeholders can create more robust policies aimed at addressing issues such as cyber harassment, misinformation, and data security breaches. Governments can establish regulatory frameworks that mandate technology companies to adopt more rigorous content moderation practices, enhance user privacy controls, and respond swiftly to incidents of online abuse. Conversely, social media platforms and digital service providers can deploy AI-based monitoring systems, refine reporting processes, and offer digital literacy initiatives to their users. Collaborative initiatives may also encompass public awareness campaigns, support hotlines, and cybersecurity training programs designed to empower women in the digital landscape. By reinforcing this partnership, it is possible to ensure that legal protections are effectively enforced, thereby enhancing the safety and accountability of digital platforms.

h) Promoting Gender-Inclusive Policies

Gender-inclusive policies are crucial for guaranteeing that women have equitable access to digital environments, legal safeguards, and avenues for empowerment. In the realm of cybersecurity and digital literacy, these policies must confront the specific obstacles that women encounter online, such as cyber harassment, online abuse, and the digital gender gap. It is imperative for governments to establish legal frameworks that explicitly acknowledge gender-based cybercrimes and to ensure that law enforcement personnel are adequately trained to address these issues with sensitivity. Moreover, digital platforms should implement more stringent measures to combat online harassment and create safer spaces for women.

Education is also a vital component in fostering gender inclusion. By incorporating digital literacy and legal knowledge into educational curricula, young girls can be equipped with the necessary skills to navigate the internet securely. Additionally, initiatives aimed at providing affordable internet access, women-centric technology training programs, and opportunities for digital entrepreneurship can help close the digital divide and advance gender equality within the digital economy. Through a gender-responsive lens, policymakers can not only protect women from cyber threats but also empower them to engage fully in the digital landscape.

8) Conclusion

The rapid advancement of digital technology has fundamentally altered the ways in which individuals connect, engage in work, and access various opportunities. Nonetheless, this transformation has also brought forth new vulnerabilities, particularly for women, who encounter a spectrum of cyber threats such as online harassment, cyberstalking, identity theft, and the unauthorized dissemination of personal information. Although digital literacy is a crucial asset for addressing these challenges, its potential remains largely unexploited in Pakistan due to deficiencies in education, awareness, and the enforcement of legal measures. The Prevention of Electronic Crimes Act (PECA) 2016 stands as the principal legislative framework for combating cybercrimes in Pakistan; however, its efficacy has been compromised by vague legal definitions, insufficient enforcement mechanisms, and a general lack of public understanding regarding digital rights and protections.

To address these issues, it is essential to implement a comprehensive strategy that not only improves women's digital competencies but also fortifies legal frameworks and law enforcement

responses to cyber threats. By incorporating digital literacy into educational curricula and community initiatives, women can be empowered with essential knowledge about cybersecurity, online privacy, and legal safeguards, thus enabling them to navigate digital environments with greater safety and assurance. Furthermore, extensive policy reforms are necessary to guarantee the effective application of laws such as PECA, which should include precise definitions of offenses and streamlined processes for reporting cybercrimes.

Countries such as India, the United Kingdom, Australia, and the United States have made significant strides in developing gender-sensitive cyber policies, enhancing law enforcement training, and establishing public-private partnerships to address online harassment and cyber threats.[30] Pakistan can benefit from these exemplary practices by promoting stronger collaborations among government entities, technology firms, civil society organizations, and educational institutions. By ensuring that digital platforms are held accountable for the removal of harmful content, improving access to legal support, and facilitating prompt action against offenders, Pakistan can foster a safer digital environment for women.

Moreover, gender-responsive policymaking should be integral to Pakistan's strategy for digital inclusion. The persistent gender digital divide restricts women's access to technology, rendering them more susceptible to cyber threats and depriving them of the advantages offered by the digital economy. Targeted initiatives such as digital literacy programs, legal awareness campaigns, and the creation of economic opportunities within the digital sector can help mitigate these disparities, thereby enhancing women's empowerment and social mobility.

Ultimately, the intersection of digital literacy and legal reforms transcends mere protection; it embodies empowerment. Women should not only feel secure in online spaces but also be motivated to engage as leaders, entrepreneurs, activists, and professionals within the digital realm. To realize this vision, Pakistan must implement a comprehensive strategy that integrates education, legal reforms, law enforcement training, and technology-driven solutions. Only through a concerted and ongoing effort can Pakistan ensure that women are not only safeguarded against cyber threats but also fully empowered to excel in the digital landscape.

9) Recommendations

To promote the safety and empowerment of women in the digital era, Pakistan must undertake comprehensive measures to close the divide between digital literacy and legal safeguards. Although the Prevention of Electronic Crimes Act (PECA) 2016 establishes a legal framework to address cyber threats, its efficacy is compromised by insufficient awareness, inadequate enforcement, and the absence of gender-sensitive policies. Women continue to encounter online harassment, cyberstalking, identity theft, and digital exploitation, which impede their full engagement in the digital sphere.

To tackle these issues, a holistic strategy is essential, integrating digital literacy programs, legal reforms, and enhanced enforcement mechanisms. By drawing insights from successful international practices, Pakistan can cultivate a more inclusive and secure digital environment for women. Following are certain recommendations to address these challenges;

Firstly, Digital literacy initiatives should be embedded within the national education framework to guarantee that young girls develop an understanding of cybersecurity and online safety from a young age. Educational institutions, including schools and universities, ought to include curricula focused on privacy protection, cyber hygiene, and responsible digital practices. The success of India's Digital Saksharta Abhiyan (DISHA) in executing these programs serves as a valuable reference for Pakistan. The initiative was inaugurated on July 1, 2015, to facilitate access

[30] Yadav, V. (2023). Tackling Non-Consensual Dissemination of Intimate Images in India's Contemporary Legal Framework. *International Annals of Criminology*, *61*(3-4), 355.

to government services through electronic means. This was to be achieved by enhancing online infrastructure, expanding internet connectivity, and fostering a digitally empowered nation in the realm of technology.[31]

Secondly, Targeted digital literacy programs should be implemented specifically for women residing in rural and underserved communities. These initiatives can take the form of community-based workshops facilitated by non-governmental organizations and women's rights groups, focusing on educating participants about safe internet practices, identifying cyber threats, and the procedures for reporting online harassment. Evidence from the European Union's Safer Internet Program illustrates the success of these awareness campaigns in enhancing women's resilience against cyber threats. This initiative has been in operation since 1999, intending to provide parents and educators with the necessary knowledge and resources to promote safety on the Internet.[32]

Thirdly, the dissemination of knowledge regarding legal rights under the Prevention of Electronic Crimes Act (PECA) 2016 requires significant enhancement. A considerable number of women remain uninformed about the processes for reporting cybercrimes or pursuing legal remedies. It is imperative to implement nationwide initiatives utilizing social media, television, and community outreach programs to inform women about their rights and the legal safeguards at their disposal. The United Kingdom's Online Safety Bill has effectively bolstered public understanding of online protections and may provide a valuable framework for similar efforts in Pakistan.[33]

Fourthly, the implementation of the Prevention of Electronic Crimes Act (PECA) 2016 requires enhancement. It is essential to amend the legislation to establish more precise definitions of cyber harassment, violations of digital privacy, and online exploitation, thereby ensuring more robust legal safeguards for women. The creation of specialized cybercrime units within the Federal Investigation Agency (FIA) is necessary to effectively address gender-sensitive cases. The experience of the United States Cybercrime Task Forces illustrates the advantages of having dedicated investigative teams focused on online criminal activities.[34]

Fifthly, law enforcement personnel and judicial officials must undergo training to manage cyber harassment incidents with a gender-sensitive perspective. A significant number of women are reluctant to report cybercrimes due to concerns about victim-blaming or lack of action. Training initiatives for police and judicial staff should emphasize the identification of digital threats, support for victims, and the enforcement of stringent measures against offenders. Additionally, the establishment of fast-track courts is crucial to ensure the prompt adjudication of cyber harassment cases. The specialized cybercrime courts in the United States have enhanced the legal framework for addressing digital offenses, serving as a model for Pakistan.

Sixthly, it is vital to strengthen collaborations among the government, private sector, and civil society to improve digital safety efforts. Partnerships with technology firms and social media platforms should prioritize the implementation of stricter content moderation policies to combat cyber harassment. The e-Safety Commissioner in Australia has effectively collaborated with social media companies to regulate online environments and eliminate harmful content.[35]

[31] Tudu, I. (2024). Make in India Digital: A Review. *Management Journal for Advanced Research*, *4*(1), 73.

[32] Eurobarometer, S. (2006). *Safer Internet*.

[33] Woods, L. (2024, August). Approaches beyond the EU–Misinformation, disinformation and the Online Safety Bill in the UK. In *Disinformation in Europe* (pp. 195-222). Nomos Verlagsgesellschaft mbH & Co. KG.

[34] Brunner, M. (2019). Challenges and opportunities in state and local cybercrime enforcement. *J. Nat'l Sec. L. & Pol'y*, *10*, 563.

[35] Regulatory Guidance. (n.d). https://www.esafety.gov.au/industry/regulatory-guidance?utm_source.

Pakistan could greatly benefit from a similar regulatory authority to oversee online safety initiatives.

Lastly, it is essential to implement gender-responsive policies that guarantee women equal access to digital resources and opportunities. Such policies should tackle obstacles including inadequate internet connectivity, insufficient digital skills, and the prevalence of online gender-based violence. Prioritizing initiatives that offer affordable internet access, technology training programs tailored for women, and opportunities for digital entrepreneurship is crucial. Sweden's Gender Equality in Digitalization Policy serves as a successful example, having effectively enhanced women's engagement in the digital realm through educational initiatives and legal safeguards, thus providing a potential framework for Pakistan.

By embracing these strategies, Pakistan can make substantial progress toward establishing a safer and more inclusive digital landscape for women. Enhancing legal protections, advancing digital literacy, and promoting collaboration among various stakeholders will empower women to engage fully in the digital sphere without the threat of cyber violence.

References

- West, M., Kraut, R., & Ei Chew, H. (2019). I'd blush if I could: closing gender divides in digital skills through education.
- Reddy, P., Chaudhary, K., & Hussein, S. (2023). A digital literacy model to narrow the digital literacy skills gap. *Heliyon*, *9*(4).
- Reddy, P., Sharma, B., & Chaudhary, K. (2020). Digital literacy: A review of literature. *International Journal of Technoethics (IJT)*, *11*(2), 65.
- Cyber-Harrasment: Self-Protection. (n.d). Retrieved on dated 14 February 2025 from Cyber-harassment: self-protection tips | Investigative Team to Promote Accountability for Crimes Committed by Da'esh/ISIL (UNITAD)
- Stevens, F., Nurse, J. R., & Arief, B. (2021). Cyber stalking, cyber harassment, and adult mental health: A systematic review. *Cyberpsychology, Behavior, and Social Networking*, *24*(6), 367.
- Gorden, S. (2024). How to Protect Yourself From Cyber-Stalking: When Online Creeping Goes Too Far. Retrieved on dated 14 February 2025 from Cyberstalking: Definition, Signs, Examples, and Prevention .
- MacFarlane, L., & Bocij, P. (2003). An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers. *First monday*, *8*(9).
- Ahlgrim, B., & Terrance, C. (2021). Perceptions of cyberstalking: Impact of perpetrator gender and cyberstalker/victim relationship. *Journal of interpersonal violence*, *36*(7-8), NP4074-NP4093.
- Kaur, P., Dhir, A., Tandon, A., Alzeiby, E. A., & Abohassan, A. A. (2021). A systematic literature review on cyberstalking. An analysis of past achievements and future promises. *Technological Forecasting and Social Change*, *163*, 120426.
- Ortiz, S. M. (2020). Trolling as a collective form of harassment: An inductive study of how online users understand trolling. *Social Media+ Society*, *6*(2), 2056305120928512.
- Henry, N., & Powell, A. (2018). Technology-facilitated sexual violence: A literature review of empirical research. *Trauma, violence, & abuse*, *19*(2), 195.
- Aardal, B., Bergh, J., & Karlsen, R. (2013). Hvorfor stemmer velgerne som de gjør?. *Valg og velgere. En studie av stortingsvalget*.
- Nadim, M., & Fladmoe, A. (2021). Silencing women? Gender and online harassment. *Social Science Computer Review*, *39*(2), 245
- Eckert, S., & Metzger-Riftkin, J. (2020). Doxxing, privacy and gendered harassment. The shock and normalization of veillance cultures. *M&K Medien & Kommunikationswissenschaft*, *68*(3), 273.
- Nonconsensual Distribution of Intimate Images: What To Know. (2024). Retrieved on dated 13 February 2025 from https://consumer.ftc.gov/articles/nonconsensual-distribution-intimate-images-what-know
- Stouffer, C. (2024). What Is Phishing? Retrieved on dated 13 February 2025 from https://us.norton.com/blog/online-scams/what-is-phishing
- Milletary, J., & Center, C. C. (2005). Technical trends in phishing attacks. *Retrieved December*, *1*(2007), 1.
- Barrett, S. (2024, November 26). Sextortion: Laws, penalties, and help for victims. UC Law San Francisco. Retrieved on dated 14 February 2025 from https://www.criminaldefenselawyer.com/resources/sextortion-laws-penalties-and-help-for-victims.html

- Hendry, N. H. (2021). Sextortion. *The Fourth Industrial Revolution and Its Impact on Ethics: Solving the Challenges of the Agenda 2030*, 315-320.
- Hufad, A., Purnomo, N. S., & Rahmat, A. (2019). Digital literacy of women as the cadres of community empowerment in rural areas. *International Journal of Innovation, Creativity and Change*, *9*(7), 277.
- Anzak, S., & Sultana, A. (2020). Social and economic empowerment of women in the age of digital literacy: A case study of Pakistan, Islamabad-Rawalpindi. *Global Social Sciences Review*, *1*, 104.
- Debbarma, A., & Chinnadurai, A. S. (2023). Empowering women through digital literacy and access to ICT in Tripura. *Research Journal of Advanced Engineering and Science*, *9*(1), 5.
- Aslam, A., Abidi, S. N. M., & Rizvi, S. S. A. (2024). Digital Literacy and Women's Empowerment: Bridging the Gender Gap in Technology for Achieving Sustainable Development Goals (SDGs). *Pakistan Journal of Gender Studies*, *24*(2), 93.
- Akmal, Z., & Usmani, S. A. A. (2024). Digital Rights and Women's Empowerment in Pakistan: An Analysis of Contemporary Islamic Legal Perspectives in the Age of Social Media. *MILRev: Metro Islamic Law Review*, *3*(1), 95.
- Shahid, K. K. (2020, May 9). Five years of PECA: The law that tried to silence Pakistan. Pakistan | Gender and Sexual Diversity. Retrieved on dated 14 February 2025 from Five years of PECA: The law that tried to silence Pakistan - IFEX
- Riaz, K. (2021, March 26). Does PECA Law Empower Women. Retrieved on dated 14 February 2025 from https://cscr.pk/explore/themes/social-issues/does-peca-law-empower-women/
- Mahmood, K., & Liu, Y. (2023). Bridging the digital divide: Strategies for inclusive access to technology. University of Engineering and Technology (UET) & Tsinghua University.
- Irfan, A. (2023). The Digital Gender Gap, a major obstacle to the fight for equality for women in Pakistan. Retrieved on dated 14 February 2025 from The digital gender gap, a major obstacle to the fight for equality for women in Pakistan | International | EL PAÍS English.
- Qureshi, S. F., Abbasi, M., & Shahzad, M. (2020). Cyber harassment and women of Pakistan: analysis of female victimization. *Journal of Business and Social Review in Emerging Economies*, *6*(2), 503.
- Yadav, V. (2023). Tackling Non-Consensual Dissemination of Intimate Images in India's Contemporary Legal Framework. *International Annals of Criminology*, *61*(3-4), 355.
- Tudu, I. (2024). Make in India Digital: A Review. *Management Journal for Advanced Research*, *4*(1), 73.
- Eurobarometer, S. (2006). *Safer Internet*.
- Woods, L. (2024, August). Approaches beyond the EU–Misinformation, disinformation and the Online Safety Bill in the UK. In *Disinformation in Europe* (pp. 195-222). Nomos Verlagsgesellschaft mbH & Co. KG.
- Brunner, M. (2019). Challenges and opportunities in state and local cybercrime enforcement. *J. Nat'l Sec. L. & Pol'y*, *10*, 563.
- Regulatory Guidance. (n.d). https://www.esafety.gov.au/industry/regulatory-guidance?utm_source.