Journal of Law & Social Studies (JLSS)
Volume 8, Issue 1, pp 147-164
www.advancelrf.org

Gender-Responsive AI Governance in Pakistan: Legal Gaps, Algorithmic Bias, and Democratic Rights

Ammara Kalsoom
CEO, Universum Consulting Pvt Ltd,
Government Liaison Advisor, Alliance for Equitable AI
Email: ammarakalsoom@yahoo.com

Abstract
Artificial intelligence (AI) increasingly influences political communication, digital governance, and democratic participation in Pakistan, yet its gendered consequences remain insufficiently addressed within existing legal and policy frameworks. This study examines how algorithmic systems, automated moderation, synthetic media, and data-driven political communication reinforce structural inequalities affecting women's participation in digital political spaces. Drawing upon doctrinal legal analysis, feminist legal theory, and comparative governance perspectives, the discussion evaluates constitutional protections, the Prevention of Electronic Crimes Act (PECA) 2016, and the Prevention of Electronic Crimes (Amendment) Act 2025 alongside international standards relating to ethical AI governance. The analysis explains that women politicians, journalists, parliamentarians, and activists experience disproportionate exposure to cyberstalking, coordinated harassment, deepfake manipulation, reputational attacks, and algorithmically amplified misogyny, all of which weaken democratic inclusion and discourage political engagement. Existing cyber governance mechanisms remain technologically limited because they primarily address conventional cybercrime while failing to regulate algorithmic discrimination, platform accountability, and AI-generated abuse. The study further highlights tensions between expanding state regulation of digital content and the protection of constitutional freedoms concerning equality, dignity, and political expression. It concludes that Pakistan requires transparent, rights-based, and gender-responsive AI governance capable of protecting women's digital participation while preserving democratic accountability within rapidly evolving technological environments. The research also emphasises stronger institutional oversight, accessible reporting mechanisms, algorithmic transparency obligations, and international cooperation to address technology-facilitated gender-based violence effectively across contemporary political platforms.

Keywords: Gendered AI Governance, Algorithmic Bias, Feminist AI, Technology-Facilitated Gender-Based Violence, Digital Democracy, Cyber Governance, PECA 2016, AI Ethics.

1. Introduction

AI increasingly shapes governmental decision-making, electoral campaigning, public administration, and political communication across both democratic and authoritarian systems. Machine-learning technologies now influence voter profiling, predictive policing, automated content moderation, and public service delivery. Governments increasingly rely upon algorithmic systems to regulate digital spaces, process large volumes of data, and monitor online behaviour, thereby transforming the relationship between citizens, political institutions, and technological intermediaries (Zuboff, 2023). The rapid integration of AI into governance structures raises complex concerns regarding accountability, transparency, and democratic participation. Digital platforms simultaneously function as principal arenas for political engagement and public deliberation. Electoral campaigns rely heavily upon algorithmically curated communication strategies designed to maximise engagement and shape political opinion. Political actors increasingly employ AI to micro-target voters, automate messaging, and disseminate political narratives through coordinated digital campaigns (Woolley & Howard, 2018). While these technologies enhance communication efficiency, they also intensify

misinformation, political manipulation, and democratic polarisation. Consequently, political participation within contemporary digital environments increasingly depends upon opaque systems controlled largely by private technology corporations.

1.1 The Rise of Artificial Intelligence in Governance and Politics

The global expansion of AI reflects a broader transition towards data-driven governance. Automated systems increasingly influence policymaking, surveillance practices, security operations, and administrative procedures. AI technologies have become central to digital governance strategies because they enable governments and corporations to process vast quantities of information with speed and precision. Nevertheless, technological efficiency does not necessarily correspond with democratic accountability. Existing literature demonstrates that algorithmic systems frequently reproduce structural inequalities embedded within social and institutional frameworks (Noble, 2018). AI also significantly shapes electoral politics and political communication. Political campaigns increasingly utilise automated technologies to analyse voter behaviour, predict political preferences, and target specific demographic groups with personalised content. Algorithmic amplification determines which political narratives receive visibility and which voices remain marginalised within digital spaces. The digital public sphere, therefore, operates through systems that are neither politically nor socially neutral. Platform algorithms privilege engagement-oriented content that frequently rewards sensationalism, hostility, and polarisation over informed democratic discourse. The transformation of digital communication further complicates democratic participation. Social media platforms increasingly function as quasi-public forums where political identities and ideological conflicts are negotiated. However, unequal access to technological visibility affects participation within these spaces. AI, therefore, possesses the capacity both to facilitate democratic engagement and to reinforce exclusionary structures that undermine political equality.

1.2 AI and Gendered Digital Spaces

Feminist literature on technology consistently demonstrates that digital systems often replicate patriarchal assumptions embedded within data collection, institutional design, and technological development. AI systems trained on historically biased datasets may therefore produce discriminatory outcomes affecting women's representation, participation, and visibility (Hart, 2025). Gendered algorithmic bias extends beyond technical malfunction and reflects broader inequalities shaping political and social institutions. Women participating in online political spaces frequently encounter targeted harassment, coordinated abuse, and reputational attacks. Technology-facilitated gender-based violence increasingly includes cyberstalking, non-consensual dissemination of intimate images, doxxing, and threats of sexual violence. The emergence of generative AI has intensified these harms through synthetic media, manipulated images, and deepfake pornography targeting women journalists, activists, and politicians (UNESCO, 2021). Such practices undermine women's security and discourage meaningful political participation within digital environments. Algorithmic invisibility further affects women's political engagement. Platform recommendation systems frequently privilege commercially profitable and sensationalist content while marginalising nuanced political engagement by women. Misogynistic narratives often receive greater algorithmic amplification than substantive political discourse, thereby reproducing patriarchal hierarchies within digital communication spaces. AI consequently functions not merely as a technological instrument but as a mechanism capable of reinforcing gendered exclusion within democratic participation (Jipguep-Akhtar, 2020).

1.3 Pakistan's Digital Landscape

Pakistan's expanding digital landscape reflects broader global transformations in political communication and civic participation. Increased smartphone penetration and rising social media usage have enabled wider participation in online political debate, electoral mobilisation, and public advocacy. Platforms such as X, Facebook, TikTok, and YouTube increasingly shape political narratives and influence public opinion, particularly among younger populations. Women parliamentarians, lawyers, journalists, and activists increasingly utilise these digital platforms to

advocate legislative reform, challenge discriminatory practices, and engage directly with constituents. Despite this expansion, Pakistan continues to experience a substantial digital gender divide. Women possess comparatively lower access to mobile technologies, internet connectivity, and digital literacy resources (GSMA, 2023). Social norms restricting women's public visibility further intensify exclusion from online political participation. Women entering digital political spaces frequently encounter gendered abuse intended to silence dissenting voices and discourage public engagement. Such harassment reflects broader structural inequalities embedded within Pakistani political culture and social relations. The PECA 2016 criminalises cyberstalking, unauthorised use of identity information, and offences against modesty and dignity (PECA, 2016, ss. 20, 21, & 24). Nevertheless, the legislation remains largely reactive and insufficiently adapted to emerging forms of AI-enabled harm. Existing legal provisions inadequately address algorithmic discrimination, synthetic media manipulation, automated disinformation campaigns, and AI-generated harassment targeting politically active women.

1.4 Problem Statement

Pakistan presently lacks a comprehensive regulatory framework addressing the gendered implications of AI within political and digital governance. Existing cybercrime legislation provides limited protection against AI-driven harms, particularly those affecting women participating in political discourse. The emergence of deepfakes, automated propaganda, and algorithmically amplified misinformation creates new vulnerabilities for women parliamentarians, journalists, and activists. Inadequate institutional safeguards consequently risk reinforcing political exclusion and weakening democratic participation.

1.5 Research Questions

This study addresses three principal questions. First, how does AI reinforce gendered exclusion within Pakistan's digital political sphere? Secondly, to what extent does the PECA 2016 adequately respond to AI-enabled harms affecting women? Thirdly, what policy and regulatory gaps persist within Pakistan's evolving framework of AI governance?

1.6 Objectives of the Study

The study critically examines gender-related risks associated with AI and digital governance in Pakistan. It analyses the adequacy of the PECA 2016 and associated policy frameworks in addressing AI-enabled harms. The study further assesses the implications of digital exclusion and online violence for women's political participation while proposing reforms capable of promoting gender-sensitive and rights-based AI governance.

1.7 Research Methodology

This study employs a doctrinal legal methodology centred upon critical interpretation of statutory provisions, constitutional principles, policy instruments, and international governance standards regulating digital technologies and AI. Doctrinal analysis remains particularly relevant because the regulation of algorithmic systems in Pakistan primarily emerges through legislative enactments, delegated regulations, and institutional policy frameworks rather than through an established body of judicial precedent (Hutchinson & Duncan, 2012). The methodology, therefore, facilitates examination of legal inconsistencies, normative gaps, and institutional ambiguities within Pakistan's evolving cyber governance regime. The analysis engages extensively with the PECA 2016 and subsequent amendments, particularly provisions concerning cyberstalking, online harassment, privacy, identity misuse, and unlawful online content (PECA, 2016, ss. 20, 21, & 24). Statutory interpretation is undertaken alongside constitutional guarantees relating to equality, dignity, freedom of expression, and political participation. Such analysis becomes necessary because digital harms affecting women increasingly intersect with constitutional protections and democratic freedoms. Existing legal provisions are therefore evaluated not merely through textual interpretation but through their broader social and political implications.

Feminist legal literature further informs the methodological framework by examining how technological regulation frequently reflects gendered power relations embedded within political institutions and digital cultures. Feminist approaches to technology law challenge assumptions that algorithmic systems operate objectively or neutrally. Instead, these perspectives recognise that AI systems may reproduce structural inequalities through biased datasets, discriminatory moderation practices, and unequal patterns of digital visibility. The methodology consequently situates online harassment and algorithmic exclusion within broader debates concerning patriarchy, democratic participation, and substantive equality (MacKinnon, 1989). Comparative policy analysis additionally contextualises Pakistan's regulatory framework within international developments concerning ethical AI governance. International instruments, including the United Nations Educational, Scientific and Cultural Organization (UNESCO) Recommendation on the Ethics of AI and the Organisation for Economic Co-operation and Development (OECD) AI Principles, provide normative benchmarks concerning transparency, accountability, human rights protection, and inclusiveness (OECD, 2019). Comparative engagement with these frameworks enables critical assessment of Pakistan's limited regulatory response to emerging harms associated with deepfakes, generative AI, and technology-facilitated gender-based violence. The methodology, therefore, combines doctrinal interpretation with feminist critique and comparative governance analysis in order to evaluate whether existing legal structures adequately protect women participating within Pakistan's increasingly digitised political sphere. It also exposes tensions between cyber regulation, democratic accountability, and the protection of fundamental rights within contemporary digital governance frameworks.

2. Literature Review

2.1 Artificial Intelligence, Algorithmic Governance, and Political Manipulation

AI increasingly influences governance, political communication, and regulation of digital spaces through systems capable of analysing behavioural patterns, automating decisions, and predicting human activity. The OECD defines AI as machine-based systems capable of generating outputs such as predictions, recommendations, or decisions affecting real or virtual environments (OECD, 2019). Contemporary literature emphasises that AI extends beyond technical automation and operates as a socio-political mechanism shaping public discourse, institutional authority, and democratic participation. Algorithmic governance consequently refers to the growing reliance upon automated computational systems to regulate social behaviour, distribute information, and influence political outcomes (Rouvroy & Berns, 2013). Automated decision-making systems increasingly shape political communication through voter profiling, content recommendation, and targeted advertising. Electoral campaigns employ predictive analytics and behavioural data to identify political preferences and tailor persuasive messaging towards specific audiences. Such technologies are frequently presented as objective and efficient; however, critical literature demonstrates that algorithmic systems often reflect inequalities embedded within datasets and institutional structures (O'Neil, 2017). Digital platforms rely heavily upon engagement-driven algorithms prioritising sensationalist content capable of generating reactions and prolonged user interaction. Consequently, political communication within online spaces increasingly rewards polarisation, hostility, and misinformation rather than substantive democratic debate. Generative AI has further intensified concerns regarding political manipulation and democratic instability. Synthetic media technologies permit the fabrication of realistic audio, images, and videos capable of damaging reputations and misleading audiences. Deepfake technologies increasingly threaten electoral integrity because manipulated political content may circulate rapidly through algorithmically amplified networks before verification mechanisms emerge (Chesney & Citron, 2019). Existing literature, therefore, identifies AI not merely as a neutral innovation but as a mechanism capable of reinforcing unequal power relations, influencing democratic participation, and reshaping political authority within digital environments.

2.2 Feminist Perspectives on Artificial Intelligence and Digital Patriarchy

Feminist legal theory challenges assumptions that law, governance, and technology operate impartially within society. Feminist literature argues that institutional structures frequently reproduce

patriarchal power relations by privileging masculine forms of authority and excluding women from meaningful participation (MacKinnon, 1989). These critiques increasingly extend towards AI systems because algorithmic technologies often inherit gendered assumptions embedded within social practices, labour structures, and historical datasets. Technological governance, therefore, reflects broader inequalities rather than existing independently from them. Gendered technology studies demonstrate that women experience digital environments differently because technological systems reproduce existing forms of social discrimination. Recommendation algorithms, content moderation systems, and automated visibility structures frequently amplify harmful stereotypes while marginalising women's political voices. Safiya Noble's research concerning search engine bias demonstrates how algorithmic systems may reinforce discriminatory representations through seemingly neutral computational processes (Schroeder, 2021). Such findings challenge narratives portraying AI as inherently objective or detached from social hierarchies.

The concept of digital patriarchy further explains how technological infrastructures sustain traditional mechanisms of gender control within online spaces. Digital patriarchy refers to the continuation of patriarchal dominance through digital communication systems, surveillance practices, and platform governance structures. Women participating in political discussions frequently encounter hostility intended to restrict visibility and discourage public engagement (Wajcman, 2013). Online abuse, therefore, functions not merely as individual misconduct but as a broader mechanism regulating women's participation within democratic discourse. Technology-facilitated gender-based violence increasingly demonstrates the harmful intersection between AI and patriarchal power. Existing literature identifies cyberstalking, doxxing, coordinated trolling, and non-consensual dissemination of manipulated intimate images as prominent forms of digital abuse targeting women journalists, politicians, and activists. Deepfake pornography has emerged as a particularly harmful practice because synthetic sexual imagery may be generated without consent and distributed rapidly across digital platforms. Such practices damage reputations, intensify psychological harm, and expose women to threats of violence (Posetti et al., 2021). Coordinated online harassment campaigns further exploit algorithmic amplification systems to maximise intimidation and public humiliation. Consequently, digital violence increasingly functions as a tool of political exclusion aimed at silencing women within public discourse.

2.3 Women's Political Participation and Digital Governance in Pakistan

Published literature concerning women's political participation increasingly recognises digital platforms as important sites for democratic engagement, electoral mobilisation, and political advocacy. Social media enables women politicians, activists, and journalists to communicate directly with audiences while bypassing certain institutional barriers embedded within traditional political structures. Digital communication technologies, therefore, possess transformative potential for enhancing political visibility and expanding opportunities for participation within democratic processes. Nevertheless, online political engagement simultaneously exposes women to intensified forms of surveillance, harassment, and reputational attacks (Norris, 2001). Research concerning digital democracies demonstrates that online violence generates substantial silencing effects upon women's participation in political discourse. Persistent harassment frequently discourages women from expressing political opinions, participating in campaigns, or pursuing leadership positions. Coordinated abuse campaigns commonly involve threats of sexual violence, misogynistic insults, and dissemination of manipulated content designed to undermine credibility and professional legitimacy (Krook & Sanín, 2020). Platform algorithms rewarding engagement frequently intensify these harms because inflammatory and abusive content often receives greater visibility than constructive political discussion. Consequently, unequal digital environments undermine substantive democratic participation despite constitutional commitments concerning equality and political representation.

Existing Pakistani literature increasingly documents widespread cyber harassment targeting women journalists, parliamentarians, and activists. Studies conducted by the Digital Rights Foundation reveal that women in Pakistan frequently experience online abuse involving threats, blackmail, stalking, and

the dissemination of private information (Digital Rights Foundation, 2020). Women participating visibly within political discourse encounter coordinated trolling campaigns aimed at discouraging public engagement and reinforcing patriarchal expectations concerning gender roles. Such harassment reflects broader social inequalities shaping political participation within Pakistan's digital landscape. Despite the enactment of the PECA 2016, scholars continue to identify substantial regulatory and institutional shortcomings concerning online harms affecting women. Existing legal provisions criminalise cyberstalking, offences against dignity, and unauthorised use of identity information; however, enforcement mechanisms remain inconsistent and technologically limited (PECA, 2016, ss. 20, 21, & 24). Pakistani digital governance frameworks primarily address conventional cybercrime while providing inadequate responses to emerging harms associated with AI, algorithmic discrimination, synthetic media manipulation, and coordinated disinformation campaigns. Current literature consequently highlights the absence of comprehensive gender-sensitive AI governance capable of protecting women participating within increasingly digitised political spaces while preserving democratic freedoms, equality, and constitutional rights within contemporary Pakistan amid accelerating technological transformations globally today.

3. Legal and Policy Framework

3.1 Constitutional Protections in Pakistan

Pakistan's constitutional framework provides several guarantees relevant to digital rights, political participation, and gender equality within technologically mediated environments. Article 19 of the Constitution guarantees freedom of speech and expression subject to reasonable restrictions imposed in the interests of national security, public order, morality, and integrity of the State (COP, 1973, art 19). Although freedom of expression constitutes a foundational democratic principle, the constitutional limitation clause permits significant governmental discretion concerning the regulation of digital communication and online content. Such discretion becomes increasingly contentious within algorithmically governed digital spaces where political speech frequently intersects with surveillance, platform moderation, and cyber regulation. Article 25 further guarantees equality before law and equal protection of law for all citizens while specifically prohibiting discrimination based on sex (COP, 1973, art 25). Constitutional equality, therefore, extends beyond formal legal recognition and encompasses substantive protection against exclusionary practices limiting women's participation within political and public life. Nevertheless, persistent online harassment and technology-facilitated abuse continue undermining women's ability to exercise political expression equally within digital spaces. Constitutional guarantees consequently remain difficult to realise where institutional protections fail to address emerging forms of technologically mediated discrimination. The constitutional right to dignity under Article 14 additionally possesses direct relevance within digital governance debates. Pakistani jurisprudence increasingly recognises dignity and privacy as essential constitutional values protecting individuals against intrusive and degrading treatment, as seen in *Mohtarma Benazir Bhutto v. President of Pakistan* [1998]. Online harassment, synthetic sexual imagery, and unauthorised dissemination of personal information, therefore, implicate constitutional concerns extending beyond conventional cybercrime. Digital violence directed towards women politicians and activists not only threatens personal security but also undermines democratic participation and political representation. Constitutional protections accordingly establish an important normative framework for evaluating the adequacy of cyber governance laws regulating digital harms and AI-enabled abuse.

3.2 Prevention of Electronic Crimes Act 2016

The PECA 2016 represents Pakistan's principal legislative framework regulating cyber offences and unlawful digital conduct. The legislation criminalises various forms of online harassment, identity misuse, and privacy violations while granting investigative powers to designated authorities. Several provisions possess particular relevance concerning harms disproportionately affecting women participating in digital political environments. Section 24 criminalises cyberstalking, including repeated online communication, surveillance, monitoring of internet activity, and unauthorised

dissemination of photographs or videos causing fear, distress, or intimidation (PECA, 2016, s. 24). The provision acknowledges psychological harm arising from persistent digital harassment and recognises cyberstalking as a significant threat within online environments. Women journalists, parliamentarians, and activists frequently experience coordinated harassment campaigns involving threats of violence, invasive monitoring, and publication of personal information. Despite statutory criminalisation, implementation challenges and limited institutional capacity continue to weaken practical enforcement against online abuse.

Section 21 addresses offences against modesty by criminalising non-consensual dissemination of sexually explicit material, superimposition of photographs onto explicit imagery, and online intimidation involving sexual content (PECA, 2016, s. 21). The provision possesses particular significance within contemporary debates concerning synthetic media and deepfake pornography targeting women in public life. Nevertheless, the statutory language primarily reflects conventional understandings of digital abuse and inadequately addresses technologically sophisticated forms of AI-generated manipulation increasingly emerging within digital environments. Section 20 further criminalises transmission of false information intended to harm the dignity, reputation, or privacy of individuals (PECA, 2016, s. 20. Protection of dignity and privacy remains particularly important for women participating visibly within political discourse because coordinated disinformation campaigns frequently target women through fabricated allegations and reputational attacks. Section 16 additionally prohibits unauthorised acquisition, transmission, or use of identity information (PECA, 2016, s. 16). Identity misuse increasingly intersects with AI technologies, enabling impersonation, synthetic representation, and deceptive online manipulation. Collectively, these provisions recognise several dimensions of digital harm affecting women. However, the legislation remains primarily reactive and technologically limited in responding to evolving algorithmic threats.

3.3 Critical Analysis of PECA: Gender and Artificial Intelligence Loopholes

Despite establishing a foundational cybercrime framework, the PECA 2016 contains substantial conceptual and regulatory gaps concerning AI governance and gender-sensitive digital protection. One significant limitation involves the absence of explicit recognition of algorithmic discrimination and automated decision-making harms. The legislation focuses predominantly upon individual criminal conduct rather than systemic technological processes shaping online visibility, content amplification, and discriminatory digital experiences. Consequently, algorithmic systems reproducing gender bias through recommendation mechanisms or automated moderation remain largely outside the regulatory scope of existing law. The legislation similarly lacks comprehensive accountability mechanisms addressing AI technologies and platform governance structures. PECA 2016 imposes criminal liability upon individual perpetrators while providing limited obligations concerning transparency, algorithmic auditing, or corporate responsibility for harmful technological systems. Digital platforms exercising significant influence over political communication and public discourse, therefore, operate without meaningful legal scrutiny concerning discriminatory algorithmic practices affecting women's participation and visibility (Baig & Jafary, 2025).

Weak statutory recognition of deepfake technologies and synthetic media manipulation further demonstrates the legislation's technological limitations. Existing provisions concerning modesty, dignity, and privacy may partially address harms arising from manipulated content; however, the legislation contains no explicit prohibition targeting AI-generated synthetic sexual imagery or deceptive political media. Deepfake technologies consequently expose women politicians, activists, and journalists to reputational harm while exploiting gaps within conventional cybercrime frameworks. Existing remedies remain inadequate for addressing the rapid dissemination and algorithmic amplification of synthetic content across digital platforms. Victim-centred protections within PECA 2016 additionally remain limited and procedurally difficult to access. Reporting mechanisms frequently involve delays, institutional insensitivity, and inadequate technological expertise among enforcement authorities (Digital Rights Foundation, 2020). Women experiencing online harassment often encounter barriers concerning evidentiary requirements, privacy concerns,

and fear of further victimisation during legal proceedings. Such deficiencies weaken the practical accessibility of legal remedies and discourage reporting of digital abuse. Ambiguities surrounding enforcement powers and online content regulation also generate concerns regarding potential chilling effects on political expression. Broad investigative powers and vague regulatory standards may enable selective enforcement against dissenting voices, including women activists and journalists engaging critically within political discourse (Bolo Bhi, 2019). Cyber governance frameworks lacking clear safeguards against arbitrary regulation risk undermining constitutional guarantees of expression, privacy, and democratic participation. Consequently, PECA 2016 simultaneously reflects an important attempt to regulate cyber harms and a structurally limited framework insufficiently equipped to address gendered implications of AI within contemporary digital politics.

3.4 PECA Amendment 2025 and Emerging Concerns

The Prevention of Electronic Crimes (Amendment) Act 2025 significantly expands governmental authority over digital communication, social media regulation, and online content governance. The amendment introduces new terminology concerning "fake or false information" and "unlawful or offensive online content," while establishing the Social Media Protection and Regulatory Authority with extensive regulatory powers. Although the amendment is presented as a mechanism for combating online disinformation and harmful content, its broad language and expansive enforcement provisions generate serious concerns regarding censorship, democratic participation, and digital rights protections. The amended framework defines "aspersion" as the dissemination of false or harmful information damaging the reputation of a person (PECA *Amendment Act,* 2025, s. 2(iiia)). It further empowers authorities to restrict online material considered offensive, false, or contrary to public order and state interests. Such provisions remain legally problematic because concepts including "false information" and "offensive content" lack precise definitional boundaries. Vague statutory terminology creates substantial risks of arbitrary interpretation and selective enforcement against political critics, journalists, activists, and dissenting voices, Bolo Bhi, 2015. Women participating visibly within political discourse may become particularly vulnerable because allegations concerning morality, reputation, and dishonour are frequently weaponised against politically active women in patriarchal societies.

The amendment additionally establishes the Social Media Protection and Regulatory Authority with powers to regulate, remove, and block online content as well as partially or fully restrict social media platforms for non-compliance (PECA *Amendment Act,* 2025, ss. 2A–2R). The Authority may direct the removal of content within twenty-four hours and exercise oversight concerning digital communication platforms operating within Pakistan. Such concentration of regulatory authority raises concerns regarding institutional accountability and proportionality because broad discretionary powers may undermine constitutional guarantees relating to freedom of expression and political participation (COP, 1973, art 19). Existing literature concerning cyber regulation consistently demonstrates that weak procedural safeguards frequently facilitate overbroad censorship and suppression of legitimate political criticism. The amendment's regulatory structure also possesses significant implications for women's political participation. Women politicians, journalists, and activists frequently encounter online abuse, reputational attacks, and coordinated disinformation campaigns intended to silence public engagement. However, broad censorship provisions lacking gender-sensitive safeguards may paradoxically expose women to further exclusion by enabling selective restriction of dissenting political expression under the guise of combating harmful content. Consequently, the amendment reflects tensions between the regulation of digital harms and the preservation of democratic freedoms within increasingly securitised digital governance frameworks.

3.5 Technology-Facilitated Gender-Based Violence in Pakistan

Technology-facilitated gender-based violence increasingly constitutes a serious barrier to women's political participation and digital inclusion within Pakistan. Emerging forms of online abuse include cyberstalking, deepfake pornography, coordinated trolling, doxxing, and algorithmically amplified harassment directed towards women occupying visible public positions (Posetti et al., 2021). Such

violence extends beyond individual misconduct and reflects broader structural inequalities shaping digital political culture. Deepfake pornography represents one of the most harmful emerging forms of AI-enabled abuse. Generative technologies permit the production of fabricated sexually explicit images and videos using women's likenesses without consent. Women journalists, politicians, and activists face particular vulnerability because manipulated sexual content frequently aims to damage credibility and discourage public engagement. Existing legal frameworks remain technologically limited in responding effectively to synthetic media manipulation and rapid algorithmic dissemination across social media platforms (Blitz, 2018). Political trolling and coordinated disinformation campaigns similarly target women participating in democratic discourse. Women parliamentarians and activists frequently encounter misogynistic abuse involving threats of violence, defamatory allegations, and gendered humiliation. Such campaigns exploit platform algorithms prioritising inflammatory engagement while intensifying hostile digital environments. Research conducted by the Digital Rights Foundation demonstrates that online harassment significantly discourages women's participation in public debate and reinforces self-censorship within digital spaces (Digital Rights Foundation, 2020). Technology-facilitated violence, therefore, undermines substantive political equality despite constitutional guarantees concerning participation and representation.

3.6 International Legal and Ethical Frameworks

International legal and ethical frameworks increasingly recognise the necessity of gender-sensitive and human rights-based AI governance. The Convention on the Elimination of All Forms of Discrimination against Women obligates States to eliminate discrimination affecting women's political participation and public engagement (CEDAW, 1979). Technology-facilitated violence and discriminatory digital governance, therefore, implicate international obligations concerning equality, dignity, and participation within public life. The UNESCO Recommendation on the Ethics of AI further emphasises transparency, accountability, and protection of human rights within the development and deployment of AI systems (UNESCO, 2021). The framework specifically recognises risks of algorithmic discrimination and highlights the importance of gender responsiveness within technological governance. Similarly, the OECD AI Principles advocate inclusive growth, transparency, accountability, and respect for democratic values (OECD, 2019). Such frameworks increasingly establish normative expectations concerning ethical AI regulation and protection against discriminatory technological harms. UN Women additionally advocates gender-inclusive digital governance frameworks capable of addressing structural barriers limiting women's participation within technological environments. Existing international standards, therefore, increasingly support regulatory approaches prioritising equality, accountability, and democratic participation within AI governance structures.

3.7 Comparative Perspectives

Comparative regulatory developments demonstrate increasing international recognition of risks associated with AI and harmful digital content. The European Union Artificial Intelligence Act adopts a risk-based regulatory model imposing obligations concerning transparency, accountability, and protection of fundamental rights (European Parliament and Council Regulation, 2024). The United Kingdom's Online Safety Act similarly imposes duties upon digital platforms to address harmful online content and protect vulnerable users. Canada increasingly emphasises algorithmic accountability and human rights protections within automated decision-making frameworks, while India's Information Technology Rules expand governmental oversight concerning digital platforms and online communication (*Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules,* 2021). Compared with these jurisdictions, Pakistan's regulatory approach remains fragmented and heavily securitised. Existing legal frameworks prioritise content control and cybercrime enforcement while providing limited safeguards concerning algorithmic accountability, transparency, and gender-sensitive digital governance. Consequently, comparative analysis

highlights the urgent need for regulatory reforms balancing online safety, democratic participation, and protection of constitutional rights within rapidly evolving technological environments.

4. Analysis: AI, Gender Bias, and Women's Political Participation

4.1 AI-Driven Political Communication and Gendered Visibility

AI increasingly shapes political communication through algorithmic systems determining visibility, engagement, and dissemination of information across digital platforms. Social media algorithms operate primarily through engagement-based metrics, privileging content capable of generating reactions, interactions, and prolonged user activity (Gillespie, 2018). Although such systems are often presented as neutral mechanisms organising online communication efficiently, algorithmic visibility frequently reflects structural inequalities embedded within social and political relations. Women participating in political discourse consequently experience unequal digital exposure because platform architectures amplify hostility, sensationalism, and polarising narratives over substantive engagement. Visibility suppression constitutes a significant dimension of gendered algorithmic governance. Political communication by women frequently receives lower amplification compared with inflammatory or masculinised content designed to provoke engagement. Published literature demonstrates that recommendation systems disproportionately reward aggression and controversy because emotionally charged material increases user interaction and advertising revenue (Nakamura & Chow-White, 2012). Consequently, women politicians and activists advocating policy-oriented or rights-based perspectives frequently encounter diminished digital reach compared with highly polarised political actors. Algorithmic prioritisation, therefore, contributes towards unequal participation within the digital public sphere. Engagement bias further intensifies gendered disparities in political visibility. Platforms reliant upon automated moderation and recommendation systems often fail to distinguish between legitimate political discourse and coordinated misogynistic harassment. Abusive commentary directed towards women politicians may generate substantial interaction and visibility despite producing harmful digital environments. Such dynamics create a paradox whereby harassment itself becomes algorithmically profitable, reinforcing the circulation of misogynistic narratives through increased engagement metrics. AI, therefore, not only mediates political communication but also shapes conditions determining which voices remain visible, credible, and influential within digital democratic spaces (Venturini et al., 2025).

4.2 Online Violence Against Women Politicians and Activists

Women politicians and activists increasingly experience targeted digital abuse designed to undermine public credibility, intimidate participation, and reinforce patriarchal authority within political spaces. Online violence frequently extends beyond isolated incidents of harassment and instead reflects coordinated strategies intended to silence women occupying visible public positions. Existing research concerning political violence against women demonstrates that gendered abuse disproportionately targets women through sexualised threats, reputational attacks, and identity-based humiliation rather than ideological disagreement alone (Bardall et al., 2020). Digital technologies consequently facilitate the continuation of traditional patriarchal exclusion through technologically mediated forms of intimidation. AI intensifies these harms through automated disinformation and synthetic media manipulation. AI-generated misinformation increasingly permits the fabrication of false narratives, manipulated statements, and deceptive visual material targeting women politicians and activists. Deepfake technologies present particular dangers because fabricated audio and visual content may appear highly authentic while circulating rapidly across algorithmically amplified networks. Within politically polarised societies, synthetic media possesses significant potential to damage reputations before verification processes emerge. Women politicians, therefore, remain uniquely vulnerable because patriarchal political cultures frequently scrutinise women's morality, appearance, and personal conduct more aggressively than those of male political actors (Gielow Jacobs, 2022). Deepfake attacks additionally produce broader democratic consequences extending beyond individual reputational harm. Manipulated sexual imagery and fabricated political statements may discourage women from participating visibly within electoral politics, media engagement, and

digital advocacy. Such attacks undermine trust, increase psychological insecurity, and reinforce social pressures restricting women's public visibility. Existing legal frameworks within Pakistan remain technologically inadequate in responding effectively to synthetic media harms because current cyber legislation primarily addresses conventional offences rather than AI-generated manipulation (PECA, 2016, ss. 20, 21, & 24). Consequently, women confronting online abuse frequently encounter institutional barriers concerning enforcement, evidence collection, and digital protection.

4.3 Digital Patriarchy and Democratic Exclusion

Digital patriarchy increasingly shapes contemporary democratic participation through technological systems reproducing existing gender hierarchies within online spaces. Patriarchal norms regulating women's visibility, speech, and mobility increasingly operate through digital communication platforms where surveillance, harassment, and reputational policing restrict women's political engagement (Gill & Grint, 2018). Online violence, therefore, functions not merely as individual misconduct but as a structural mechanism preserving unequal distributions of political power and authority. Persistent harassment contributes significantly to self-censorship among women participating in digital political environments. Women politicians, journalists, and activists frequently moderate opinions, avoid controversial subjects, or reduce online engagement because of fears concerning coordinated abuse and reputational attacks. Such self-censorship reflects rational responses to hostile digital environments rather than voluntary withdrawal from democratic participation. Existing studies concerning online political violence demonstrate that women often experience psychological distress, anxiety, and professional insecurity resulting from sustained digital harassment (Posetti et al., 2021). Consequently, digital participation becomes conditioned upon women's willingness to tolerate disproportionate abuse and surveillance.

Withdrawal from political spaces further illustrates the exclusionary consequences of digital patriarchy. Women subjected to persistent online intimidation may reduce public visibility, disengage from political campaigning, or avoid leadership positions entirely. These patterns undermine substantive democratic representation because political participation increasingly depends upon digital communication and online visibility. Algorithmically amplified harassment, therefore, weakens democratic inclusion by restricting equal access to political discourse and public influence. The chilling effect produced by hostile digital environments additionally threatens constitutional commitments concerning equality, representation, and freedom of expression. Women excluded through technologically mediated intimidation remain formally entitled to political participation yet substantively constrained by unequal digital conditions. AI consequently operates within broader patriarchal structures shaping democratic engagement, institutional legitimacy, and political representation. Without effective safeguards addressing algorithmic bias, digital violence, and discriminatory platform governance, technological systems risk normalising exclusionary political cultures that silence women while reinforcing unequal power relations within democratic spaces.

4.4 Implications for Women Parliamentarians in Pakistan

Digital communication platforms increasingly constitute essential instruments for parliamentary engagement, constituency outreach, legislative advocacy, and political visibility. Women parliamentarians in Pakistan increasingly utilise social media platforms to disseminate policy positions, engage with constituents, and participate in national political debates. Digital technologies potentially expand political accessibility by enabling women legislators to communicate beyond traditional gatekeeping structures historically dominated by male political actors and conventional media institutions. Nevertheless, increased digital visibility simultaneously exposes women parliamentarians to intensified forms of online harassment, misogynistic abuse, and reputational attacks (Dutton & Reisdorf, 2019). Women legislators participating actively within online political spaces frequently encounter coordinated trolling campaigns involving threats, defamatory allegations, and gendered humiliation. Existing research concerning women in politics demonstrates that female political actors experience abuse disproportionately targeting appearance, morality, and family life rather than ideological disagreement alone. Such harassment reflects broader patriarchal

assumptions questioning women's legitimacy within political leadership and public authority. Algorithmically amplified hostility consequently transforms digital political engagement into a site of continuous reputational vulnerability for women parliamentarians (Håkansson, 2024).

AI technologies further intensify these risks through synthetic media manipulation, impersonation, and automated disinformation campaigns. Women politicians remain particularly vulnerable to deepfake pornography and fabricated political content designed to damage public credibility and discourage participation in political discourse. Such attacks exploit social norms surrounding honour and morality within patriarchal societies, where reputational harm may produce broader social consequences for women than for male political actors. Consequently, AI-enabled abuse not only undermines individual security but also weakens democratic representation by discouraging women's visible participation within legislative and political processes (Levi, 2017). Institutional support mechanisms addressing online violence against women parliamentarians additionally remain fragmented and inadequate. Existing parliamentary procedures provide limited guidance concerning digital security, coordinated online abuse, and AI-generated harassment targeting elected representatives. Although the PECA 2016 criminalises certain forms of cyber harassment, implementation challenges, weak investigative capacity, and procedural delays frequently discourage effective legal recourse (PECA, 2016, ss. 20, 21, & 24). Women parliamentarians, therefore, navigate digital political spaces without comprehensive institutional protections capable of responding to evolving technological harms.

4.5 Artificial Intelligence Governance Deficit in Pakistan

Pakistan's AI governance framework remains underdeveloped despite increasing technological integration within political communication, digital regulation, and public administration. Although policy discussions concerning emerging technologies have expanded in recent years, the comprehensive implementation of a national AI governance strategy remains limited. Existing regulatory structures primarily address conventional cybercrime and online content regulation rather than broader concerns surrounding algorithmic accountability, discriminatory automated systems, and platform governance (OECD, 2019). Regulatory fragmentation further weakens the effective governance of AI technologies within Pakistan. Multiple institutions exercise overlapping authority concerning cybercrime enforcement, telecommunications regulation, and digital communication oversight without coherent coordination concerning AI governance standards. Such fragmentation produces uncertainty regarding accountability, transparency, and enforcement responsibilities. Existing legal frameworks consequently struggle to address harms arising from recommendation algorithms, automated moderation systems, and synthetic media technologies operating across transnational digital platforms. Weak digital rights protections additionally intensify governance deficiencies. Existing cyber governance approaches frequently prioritise securitisation, surveillance, and content restriction over protection of democratic participation and individual rights (Bolo Bhi, 2015). Women experiencing online harassment, disinformation campaigns, and algorithmic discrimination, therefore, encounter limited institutional safeguards protecting digital participation and political expression. The absence of gender-sensitive AI regulation further reflects broader policy failures concerning inclusion, equality, and democratic accountability within technological governance frameworks.

4.6 Balancing Regulation and Freedom of Expression

Regulation of AI and digital communication platforms presents complex tensions between protection from online harms and preservation of democratic freedoms. Expanding regulatory powers concerning online content moderation may assist in addressing misinformation, coordinated harassment, and technology-facilitated gender-based violence. However, broad censorship frameworks lacking procedural safeguards simultaneously risk undermining constitutional guarantees concerning freedom of expression and political participation (COP, 1973, art 19). Overregulation remains particularly concerning within politically polarised environments where vague legal terminology concerning "false information" or "offensive content" may facilitate arbitrary

enforcement against journalists, activists, and dissenting political voices. Women engaging critically within political discourse may experience disproportionate vulnerability because patriarchal narratives frequently frame outspoken women as socially disruptive or morally transgressive. Consequently, cyber governance frameworks emphasising control rather than rights-based protection may inadvertently reinforce exclusionary political structures.

Democratic accountability, therefore, requires regulatory approaches grounded in transparency, proportionality, and human rights protections. International governance standards increasingly emphasise accountability mechanisms ensuring that AI systems operate consistently with equality, dignity, and democratic participation. Human-rights-based governance approaches recognise that technological regulation must simultaneously address online harms and preserve constitutional freedoms essential for democratic inclusion (UNESCO, 2021). Balancing these competing concerns remains particularly important within Pakistan's evolving digital political environment, where women's participation already encounters structural inequalities and persistent online hostility. Effective AI governance consequently requires not only criminalisation of harmful conduct but also institutional safeguards protecting political expression, gender equality, and democratic accountability within technologically mediated public spaces.

5. Conclusion

AI increasingly shapes political communication, democratic participation, and governance structures within Pakistan's expanding digital environment. However, technological development has not occurred within socially neutral conditions. Existing evidence demonstrates that AI systems frequently reproduce historical inequalities embedded within political institutions, digital infrastructures, and social relations. Algorithmic systems prioritising engagement, visibility, and behavioural prediction often amplify misogynistic narratives, coordinated harassment, and exclusionary political discourse affecting women participating in public life. Consequently, AI does not merely reflect technological innovation but also reinforces unequal distributions of political power and digital visibility. Women politicians, activists, journalists, and parliamentarians increasingly encounter technology-facilitated abuse involving cyberstalking, synthetic media manipulation, coordinated trolling, and reputational attacks. Such harms extend beyond individual victimisation because persistent digital hostility undermines substantive democratic participation by discouraging women's political engagement and public visibility. AI-enabled harassment, therefore, contributes towards broader structures of democratic exclusion operating through digitally mediated forms of intimidation and surveillance. Online participation increasingly requires women to navigate disproportionate hostility and reputational vulnerability within algorithmically governed communication spaces.

Pakistan's legal and regulatory framework remains largely reactive in addressing these emerging technological harms. The PECA 2016 criminalises cyberstalking, offences against dignity, and identity misuse; nevertheless, the legislation primarily reflects conventional understandings of cybercrime rather than contemporary challenges associated with AI and automated digital systems (PECA, 2016, ss. 20, 21, & 24). Existing provisions inadequately address algorithmic discrimination, platform accountability, synthetic media manipulation, and discriminatory recommendation systems shaping political participation and online visibility. Weak enforcement mechanisms, fragmented institutional oversight, and limited victim-centred protections further undermine effective legal responses to gendered digital harms. The Prevention of Electronic Crimes (Amendment) Act 2025 additionally expands governmental authority concerning online content regulation while raising concerns regarding censorship, overregulation, and democratic accountability (PECA *Amendment Act,* 2025). Broad statutory terminology relating to "false information" and "offensive content" creates risks of arbitrary enforcement against journalists, activists, and dissenting political voices, including women participating critically within public discourse. Consequently, Pakistan's cyber governance approach increasingly reflects tensions between securitised digital regulation and the

protection of constitutional freedoms concerning equality, political participation, and freedom of expression.

International frameworks concerning ethical AI governance increasingly emphasise transparency, accountability, inclusiveness, and gender responsiveness within digital regulation (OECD, 2019). Comparative developments demonstrate growing recognition that technological governance must protect democratic participation alongside addressing harmful online conduct. Pakistan's evolving digital environment, therefore, requires comprehensive gender-responsive AI governance capable of addressing technology-facilitated violence, algorithmic discrimination, and unequal digital participation. Without meaningful legal reform and institutional accountability, AI risks reinforcing patriarchal political structures while weakening democratic inclusion and substantive political equality for women within contemporary Pakistan. Effective governance additionally requires institutional mechanisms capable of supporting women confronting online abuse through accessible reporting procedures, digital security protections, and transparent regulatory oversight. Human-rights-based AI governance cannot operate exclusively through criminalisation or content restriction because technologically mediated discrimination frequently emerges through opaque algorithmic processes embedded within digital platforms themselves. Democratic inclusion, therefore, depends upon regulatory frameworks recognising that gender equality, political participation, and digital rights remain interconnected constitutional and social imperatives within rapidly transforming technological environments across Pakistan's increasingly networked public sphere.

6. Recommendations

6.1 Legal Reforms

Pakistan's cyber governance framework requires comprehensive reform addressing AI-enabled harms affecting women's political participation and digital rights. The PECA 2016 should incorporate explicit provisions regulating algorithmic discrimination, automated disinformation, synthetic media manipulation, and platform accountability (PECA, 2016). Existing legal protections concerning cyberstalking and offences against dignity remain insufficient for responding to technologically sophisticated harms emerging through generative AI systems. Legislative reform should therefore criminalise the creation and dissemination of non-consensual deepfake pornography, manipulated political content, and AI-generated impersonation targeting women in public life. Gender-sensitive cyber legislation must additionally recognise technology-facilitated violence as a structural democratic issue rather than merely an individual criminal offence.

6.2 Institutional Reforms

Institutional accountability mechanisms remain essential for effective AI governance within Pakistan's political and digital environment. Parliamentary oversight committees should exercise regular review concerning the deployment of automated technologies affecting democratic participation, online regulation, and digital rights protections (COP, 1973, art 19, 25). Independent digital rights commissions with investigatory authority may further strengthen accountability concerning algorithmic discrimination, online harassment, and platform governance practices. Existing regulatory institutions primarily prioritise cybercrime enforcement and content restriction while neglecting broader concerns regarding equality, transparency, and democratic participation. Gender-responsive AI regulators should therefore include multidisciplinary expertise involving technology specialists, legal scholars, parliamentarians, and women's rights advocates capable of evaluating discriminatory technological practices and harmful algorithmic systems.

6.3 Protection Mechanisms for Women Politicians

Women politicians and parliamentarians require specialised institutional safeguards addressing online harassment, synthetic media attacks, and coordinated digital abuse. Parliamentary institutions and political parties should adopt comprehensive online safety protocols, establishing procedures concerning digital security, rapid response coordination, and psychological support for women

experiencing technology-facilitated violence. Accessible and rapid complaint mechanisms remain particularly necessary because online harassment frequently spreads through algorithmically amplified networks before legal intervention occurs. Digital platforms operating within Pakistan should additionally remain subject to enforceable accountability obligations requiring transparent moderation practices, timely removal of harmful synthetic media, and effective reporting procedures concerning coordinated abuse campaigns targeting women participating in political discourse.

6.4 Artificial Intelligence Ethics and Transparency

Ethical governance of AI requires mandatory transparency obligations concerning automated systems influencing political communication and digital participation. Platform operators and technology companies should conduct regular algorithmic audits assessing discriminatory outcomes, harmful recommendation patterns, and amplification of misogynistic content (OECD, 2019). Bias assessments should further evaluate whether automated moderation systems disproportionately suppress women's political expression or reinforce unequal visibility structures within digital spaces. Transparency reporting obligations concerning content moderation, algorithmic decision-making, and AI deployment may additionally strengthen public accountability while improving democratic oversight concerning digital governance practices.

6.5 Capacity Building and International Cooperation

Effective governance additionally depends upon institutional capacity building and international cooperation concerning emerging technological harms. Women parliamentarians, journalists, and political activists require specialised digital literacy initiatives, AI awareness programmes, and cybersecurity training enabling safer participation within digital political environments (UNESCO, 2021). Educational initiatives should further strengthen understanding concerning deepfake technologies, online disinformation, and privacy protections affecting democratic engagement.

Pakistan's regulatory framework should additionally align more closely with international governance standards, including the UNESCO Recommendation on the Ethics of AI and OECD AI Principles. Regional cooperation concerning cyber governance, platform regulation, and technology-facilitated gender-based violence may strengthen institutional responses to transnational digital harms while supporting rights-based and gender-sensitive AI governance frameworks. Meaningful reform also requires sustained collaboration between civil society organisations, parliamentary caucuses, technology companies, and academic institutions capable of producing evidence-based policy responses concerning AI and democratic participation. Inclusive consultation mechanisms may improve legitimacy, strengthen institutional trust, and ensure that women affected by digital violence remain centrally represented within future governance initiatives.

References

Baig, K., & Jafary, H. A. (2025). Cyber harassment and online violence against women in Pakistan: Legal gaps and enforcement challenges. *Journal of Political Stability Archive*, *3*(4), 900-916.

Bardall, G., Bjarnegård, E., & Piscopo, J. M. (2020). How is political violence gendered? Disentangling motives, forms, and impacts. *Political Studies*, *68*(4), 916-935.

Biroli, F. (2018). Violence against women and reactions to gender equality in politics. *Politics & Gender*, *14*(4), 681-685.

Blitz, M. J. (2018). Lies, line drawing, and deep fake news. *Okla. L. Rev.*, *71*, 59.

Bolo Bhi. (2015). *PECB2015: The story so far*. https://bolobhi.org/pecb2015-the-story-so-far/.

Bolo Bhi. (2019). *Note on the implementation of the Prevention of Electronic Crimes Act 2016*. https://bolobhi.org/note-on-the-implementation-of-prevention-of-electronic-crimes-act-2016/.

Chesney, B., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *Calif. L. Rev.*, *107*, 1753.

Constitution of the Islamic Republic of Pakistan (COP)*, 1973* (Pakistan), arts 19 and 25.

Convention on the Elimination of All Forms of Discrimination Against Women (CEDAW) (adopted December 18, 1979, entered into force September 3, 1981), 1249 U.N.T.S. 13.

Digital Rights Foundation. (2020). *Measuring Pakistani women's experiences of online violence 2020*. https://digitalrightsfoundation.pk/wp-content/uploads/2017/05/Hamara-Internet-Online-Harassment-Report.pdf.

Dutton, W. H., & Reisdorf, B. C. (2019). Cultural divides and digital inequalities: attitudes shaping Internet and social media divides. *Information, communication & society*, *22*(1), 18-38.

European Parliament and Council Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence, *[2024] OJ L 1689*.

Gielow Jacobs, L. (2022). Freedom of speech and regulation of fake news. *The American Journal of Comparative Law*, *70*(Supplement_1), i278-i311.

Gill, R., & Grint, K. (2018). Introduction the gender-technology relation: Contemporary theory and research. In *The Gender-Technology Relation* (pp. 1-28). Taylor & Francis.

Gillespie, T. (2018). *Custodians of the Internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.

GSMA (2023). *Mobile gender gap report 2023*. https://www.gsma.com/wp-content/uploads/2025/12/The-Mobile-Gender-Gap-Report-2023.pdf.

Håkansson, S. (2024). The gendered representational costs of violence against politicians. *Perspectives on Politics*, *22*(1), 81-96.

Hart, C. G. (2025). Tensions of Making Women's Marginalization Salient in Men-Dominated Workplaces. *Work and Occupations*, *52*(3), 358-387.

Hutchinson, T., & Duncan, N. (2012). Defining and describing what we do: doctrinal legal research. *Deakin Law Review*, *17*(1), 83-119.

Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 (India).

Jipguep-Akhtar, M. (2020). Review of *Race after technology: Abolitionist tools for the new Jim code*. *Social Forces, 98*(4), 1–3.

Krook, M. L., & Sanín, J. R. (2020). The cost of doing politics? Analyzing violence and harassment against female politicians. *Perspectives on Politics*, *18*(3), 740-755.

Levi, L. (2017). Real fake news and fake fake news. *First Amend. L. Rev.*, *16*, 232.

MacKinnon, C. A. (1989). *Toward a feminist theory of the state*. Harvard University Press.

Mohtarma Benazir Bhutto v. President of Pakistan, PLD 1998 SC 388 (Pakistan).

Nakamura, L., & Chow-White, P. (Eds.). (2012). *Race after the Internet* (p. 203). New York: Routledge.

Noble, S. U. (2018). Algorithms of oppression: How search engines reinforce racism. In *Algorithms of Oppression*. New York University Press.

Norris, P. (2001). *Digital divide: Civic engagement, information poverty, and the Internet worldwide*. Cambridge University Press.

O'Neil, C. (2017). *Weapons of math destruction: How big data increases inequality and threatens democracy*. Crown.

Organisation for Economic Co-operation and Development (OECD). (2019). What are the OECD principles on AI? *OECD Observer, 2019*. https://doi.org/10.1787/6ff2a1c4-en.

Organisation for Economic Co-operation and Development (OECD). (2019). *OECD AI principles overview*. https://oecd.ai/en/ai-principles.

Posetti, J., Shabbir, N., Maynard, D., Bontcheva, K., & Aboulez, N. (2021). The chilling: Global trends in online violence against women journalists. *New York: United Nations International Children's Emergency Fund (UNICEF)*.

Posetti, J., Shabbir, N., Maynard, D., Bontcheva, K., & Aboulez, N. (2021). The chilling: Global trends in online violence against women journalists. *New York: United Nations International Children's Emergency Fund (UNICEF)*.

Prevention of Electronic Crimes (Amendment) Act, 2025 (Pakistan), ss. 2(iiia), 2A–2R.

Prevention of Electronic Crimes Act, 2016 (Pakistan), ss. 16, 20, 21, & 24.

Rouvroy, A., & Berns, T. (2013). Algorithmic governmentality and prospects of emancipation: Disparateness as a precondition for individuation through relationships?. *Réseaux*, *177*(1), 163-196.

Schroeder, J. E. (2021). Reinscribing gender: social media, algorithms, bias. *Journal of Marketing Management*, *37*(3-4), 376-378.

United Nations Educational, Scientific, and Cultural Organization (UNESCO). (2021). *Recommendation on the ethics of artificial intelligence*. UNESCO. https://unesdoc.unesco.org/ark:/48223/pf0000381137.

Venturini, T., Acker, A., Plantin, J. C., Walford, T., & Crichlow, C. (2025). The Co-Constitution of Race and Data. In *The Sage Handbook of Data and Society* (pp. 275-297). Sage Publications Ltd.

Wajcman, J. (2013). *TechnoFeminism*. John Wiley & Sons.

Woolley, S. C., & Howard, P. N. (Eds.). (2018). *Computational propaganda: Political parties, politicians, and political manipulation on social media*. Oxford University Press.

Zuboff, S. (2023). The age of surveillance capitalism. In *Social theory re-wired* (pp. 203-213). Routledge.