

Journal of Social Policy and Governance (JSPG)

Available Online:

<https://journalofsocialpolicyandgovernance.com/index.php/2>

ISSN Print: 3106-3764

ISSN Online: 3106-3772

Platform & Workflow by: [Open Journal Systems](#)

Digital Political Discourse in Pakistan: Legal Challenges of Online Hate Speech and Misinformation**Sadiq Ali**

Faculty of Law, University of Central Punjab, Lahore

sadiqderpakhil@gmail.com**Abstract:**

The fast growth of digital space has not only reshaped political communication, but also opened opportunities through which participation in Pakistan can take place, which also present challenges. This paper will look at the nature of cyber politics and the particular issue of online hate speech and political misinformation, and assess the effectiveness of Pakistan cyber laws in its efforts to correct this problem. The social media platforms Facebook, X (Twitter), Tik Tok, and YouTube have been turned into the focal point of political mobilization, but they are also the place where unfriendly rhetoric, sectarianism, fake news, and orchestrated propaganda campaigns are propagated rapidly. This paper, built on qualitative review of the current laws (such as the Prevention of Electronic Crimes Act (PECA) 2016) can be viewed as an analysis of the regulatory reaction of the state and how it can be complemented to address the lack of enforcement, digital literacy, and platform responsibility. This paper concludes that cyber laws are present but the best approach to curb online political harm in Pakistan is the combination of legal reform, media literacy and open-minded enforcement of the law.

Keywords: Cyber Politics, Hate Speech, Political Misinformation, Cyber Law (PECA), Digital Media Regulation

Introduction

Social media has emerged as a central arena of political engagement in Pakistan, serving as a platform for voter mobilization, agenda-setting, and narrative construction. However, it also functions as a conduit for hate speech and the dissemination of political misinformation, raising serious regulatory challenges. The legal framework governing this digital sphere is multifaceted, comprising constitutional restrictions on freedom of expression, relevant provisions of the Pakistan Penal Code (PPC), sector-specific broadcasting regulations, and the Prevention of Electronic Crimes Act (PECA), implemented under the supervision of the Pakistan Telecommunication Authority (PTA). This article seeks to critically examine this regulatory structure, highlight recent statutory and judicial developments, and provide a concise review of the existing literature on cyber politics and cyber law in Pakistan.

A disorderly flow of digitality changes the manner in which political communication occurs internationally while modifying how states and political actors utilize their time and how citizens interact with each other and take part in political activities. The use of social networks, such as Facebook, X (previously Twitter), and Tik Tok, in Pakistan gave people new opportunities to take political action, mobilize, and discuss issues. However, there are also other more important issues within this electronic revolution, and the spread of online hate speech and political false information may also be placed first among other issues. All these challenges represent a primary threat to the integrity of democratic institutions, the civic community, and the stability of the State.

The kaleidoscopic nature of politics in Pakistan has been increasingly taking on a new dimension through cyber politics; simply interactions and transactions over the cyberspace. Politics has become a medium to create, spread and struggle with in a digital space. On the one hand, this opens up space to marginalised voices and grassroots activism, but it also enables the proliferation of disinformation campaigns, character attacks and inflammatory content that could further polarise and lead to violence.

Policymaking of the online world thus turns into an immediate policy and legal challenge. Pakistan is also a nation endowed with bountiful cybers laws, the latest to hit the market being the Prevention of Electronic Crimes Act (PECA) 2016, which seeks to curb cybercrimes and abuse of digital platforms. However, one may question how much and to what degree these laws can be properly applied, and under the other priority agenda, whether to release the speech or to restrict the Internet usage and abuse. The opponents of the system accuse it of being applied selectively in its regulation, which raises doubts about its political partiality, censorship, harming human rights, etc.

This study is intended to familiarize itself with the convergence of cyber politics with cyber law on social media sites in Pakistan, using the example of regulating online hate speech and political lies. Due to a review of existing systems within legal, policy, and institutional environments, and the example of Socrates, there are gaps, issues, and possible changes that might be needed in order to help make cyberspace a place of freedom, inclusivity and safety when it comes to political representation.

Research Objectives

This study aims to discuss the definition of a new (cyber) politics to understand its consequences in terms of political discourse and patterns of communication in Pakistan.

We will answer the legal and regulatory setting in this article that has been extended to the hate speech and online pseudo misinformation that is viewed as political and Practices of Hate and National Counter-Messaging Strategy that explicitly address the Prevention of Electronic Crimes Act (PECA) 2016.

To evaluate the effectiveness and inefficiency of cyber laws in Pakistan and the balance that it strikes between freedom of speech and the imperative to restrict beneficial activities in the cyber arena.

To investigate the dimensions of the interactions of political actors, state apparatuses, and civil society between/with cyber regulations in Pakistan.

In order to give policy recommendations on improving cyber governance without interfering with democratic values and human rights;

Research Questions

1. What is the impact of emergence of cyber-politic on participation and involvement of people in politics in Pakistan?
2. What are the salient characteristics of cyber laws in Pakistan and how they are used to hate speech and political misinformation on the Internet?
3. How successful have these laws been, on a civil liberties front, and in facilitating the regulation of harmful content online?
4. Which reforms are required to the Pakistan model of cyber governance in order to balance cyber governance in the country in control, freedom of expression and democracy accountability?

Literature Review

The introduction to the Cyber Political.

Cyber politics means: Politics communication through the internet and more so online (Trechsel, 2022). Based on the nine discussion chapters, McGee finds that the rise of the Web and social media has transformed the public sphere where the old media had previously dominated. In fact, across nations that have a young, e-savvy population, whose numbers are rapidly increasing, such as Pakistan, cyber politics has emerged as a necessary field of electoral and grassroots mobilization and narrative-making (Kugelman 2020). Scholars (Castells, 2013) assume that the cyberspace is linked with freedom because the weak feel free enough to take action against the hierarchy of power of which society it belongs to. However, both sides of the coin are that democratization is accompanied by hate speech, political trolls, fake news and manipulation (Wardle and Derakhshan, 2017).

Cyber Politics in Pakistan

The case of cyber politics in Pakistan is quite different as Pakistan is a country which has very strong polarized political culture, weak democratic establishments and is progressively becoming online. Its greatest asset though is digital technologies and with the tool of a social media, the political parties like PTI, PML-N, PPP, ended up in a position to manipulate or rather control the entire narrative of people (Khan and Shah, 2021). More to the point, high-profile campaigns and trendy hashtags serve as alternative places to regular political events, creating so-called digital battlegrounds. Yet, they have hurled a dark cloud over fake news campaigns, media and communications motivated by hatred in cyberspace, coordinated by political interests (Youseaf, 2022).

What has also been indicated in other studies is that cyber politics in Pakistan is inextricably linked to the notion of youth participation as more than three-quarters of the Pakistani population is below 30 years of age (UNDP 2020). It is them that keep digital activism so viral and potentially a dangerous group effectively controlled by faux news.

Online hate speech: national and international.

Hate speech can be described as any activity involving the internet that in some way results in hatred, discrimination, or hate do act toward persons or groups of people based on race/religions/ethnicity/politicians (Brown, 2017). One of the aspects of governance where has delivered monolithic momentum ample and sundry sectors worldwide into which the Facebook and X consider a catalog of policies community in a bid to slay the malicious editorial (Gillespie, 2018).

Hate speech is easily confused with sectarian divisions and religious issues in Pakistan. Studies indicate that sectarian violence and polarisation of politics occur as a result of hate narratives that are shared via social media (Abbas 2019). Part of the means by which the state has endeavored to react to this under PECA 2016 in the form of legislation on cyber crimes is that the term hating speech is so extensive that there will no longer be any more cases so to speak that AI may get caught in this task (Khan and Shah, 2021).

Simulating News and Propagandizing Politics.

Table Lent craft Light of over-saturation of information and the electronic era is an international concern implicit manipulation. Wardle (2019) observes misinformation typology (the false content distributed without any intention of producing harm) and disinformation (the false content distributed with the purpose of misleading viewers). These are but a few examples of what is very common throughout the digital frontier of Pakistan.

Among young people, there are also fake, alleged, hyped videos, explosive news leaks and springs on political leaders, among other constant things it does not matter at all to the children during the election period; at a time when it is building a criteria through which individuals will be viewed (Azraiza, 2022). Although it might be rather through the actions of

opposition parties, state actors have the possibility and often participate in such dealings and the notion of media manipulations and their authoritativeness may be considered fully relevant. Other assumptions made in the work are that in Pakistan, they spread political misinformation, and, in addition to an already high level of distrust of the government expected of citizens, the barrier between the two layers of society is further increased (Naseer, 2020).

PECA 2016 Cyber Law in Pakistan Beyond.

The most important interaction regulation with the internet in Pakistan is Prevention of Electronic Crimes Act (PECA) 2016. Cyberstalking, identity theft, online harassment, hate speech and sharing of fake news are criminalized (Government of Pakistan 2016). According to proponents, PECA is a giant leap towards regulating cyberspace and ensuring that citizens are not harmed by the Internet.

Nevertheless, it is the vagueness that worries both the thinkers and the critics of the civil society as something that can be easily adapted by the governments (in fact, as a mean of the criminalization of the intelligible activities of its doctrines opponents) due to their vagueness, their unreasonable limits of definitions (Shad 2018). In particular, it has documented the cases in which PECA has been used to prevent a form of speech that otherwise would have been speech that, although not hate speech, qualifies as hate (Baloch 2021). This is symptomatic of a broader issue that seems to occur in many parts of the world, that of being able to censor online expression without infringing the right to the freedom of expression (article 19, ICCPR).

How to debate the tensions between regulation and the freedom of expression.

Whatever maybe should be implemented against the source of hate speech on the Internet including misinformation, it mini slides into the question of the right of dry freedom. On the one hand, the virtual world of the internet devoid of a sufficient system of peer review and control may contribute to the destabilization of states, to the promotion of violence, and to a decrease in trust of democratic procedures. Then another, since it has not and it will be by the toil of cannibalization against their opinion and conquest the governments in a more powerful manner (MacKinnon, 2012).

The issue that Pakistan is facing is that of balance. Peace activist organizations, including Amnesty International (2020), have lamented that PECA and equivalent are punishing political actors, but not actors who have actually engaged in actual violence in the real world via the internet. Compared to the connotation of the European states powers of which continue to pursue the question (Hussain 2021), then China will carry the equality of the right orientation of an issue in the hands of those actors in the foreign arena who are structuring the things in the digital world.

Ways We Speak about Regulating Online Hate Speech Around the World.

The practice governments and digital platforms have experimented with different regulatory models that have been tested across international borders. Udtica is a stranger.

The models provide global design experiences to guide Pakistan to reform regulation in context-specific and human rights-compliant manner. This commercial deviance concerns a form of co-regulated practices that constitute the institutions of the state as well as tech corporations or civil society, who scholars have long advocated (Gorwa 2019).

Cyber Governance Emerging Issues.

Other cyber governance challenges that are common in Pakistan besides hate speech and disinformation include digital adjudication, privacy, and external intrusion into political conversations (Shad 2018). Such predicaments are only bound to rise as the internet penetration goes up. It is no longer able to list the extra risk of deepfakes or any other source

of other artificial intelligence mainstreaming the pressure to regulation already, already overwhelmed by the usage (Chesney and Citron, 2019).

Cybers politics in Pakistan has created a re-empowering threatening pledge of democracy, the land of substance prohibitions which have been circulated in literature. Hate talk and fake news are abhorred on the Internet. Although pivotal laws such as energy-related PECA 2016 have been seen to achieve a lot in addressing the above scenario, its vagueness, selective application, corruption and abuse of human rights have raised concerns to date. When introduced as an international comparative view, we infer, that Pakistan direly requires a composite outlook of regulation which will heal rape-some digital inadequacies without offending those individual liberties which for the union of democracy is inalienable.

Methodology

Research Design

The qualitative research pattern adopted by this study is coupled with doctrinal legal analysis methodology and case study design. The qualitative methodology would work best since the research is about an exposed interpretation and implication or the meaning of cyber politics and cyber law in Pakistan, but is not an intention to measure variables (Creswell and Poth, 2018). Part of analysis to be carried out and strictly theoretical in nature: A critical analysis of the laws that are already in place, Prevention of Electronic Crimes Act (PECA) 2016 and its provisions will be carried out and evaluated to present its shortcomings or strengths as the case may be and combat the problem of online hate speech or political fake news. Besides, as a case study, it also probes into some of the instances in which those laws have either been implemented or opposed in Pakistan.

Research Paradigm

The rationale of these research questions has been set in a constructivist produce, which opines that social and political actualities are produced through the relationship among human beings, computer and superiority-based communication, and the law as a rule. The conceptual framework aptly aims to examine the senses and ways in which the stakeholders (political actors, citizens, and institutions) use cyber regulation in Pakistan to make sense.

Data Collection Methods

Secondary sources that will be used in the research include:

Statutes, acts and legislation: Laws which are brought into effect such as the Prevention of Electronic Crimes Act (PECA) 2016 and those which have already been amended and provisions relevant and articles (and concern expression etc) into the relevant constitution such as article 19 and the others.

Cases and verdicts, Cases have been submitted in high profile websites that have posted terms of PECA with reference to the Internet have been offended, have been misinformed (hate speech on the internet) and misinformed (misinformation) on political matters.

Journals, books, and reports: scientific publication concerning cyber-politics, hate speech and misinformation online, and online digital governance.

Think-tanks articles and policy reports: Books by the Council of Europe, Amnesty international, and the ministry of information technology in Pakistan.

News media and credible internet sources: To learn about the latest controversies, movements or events of internet hate speech/misinformation in Pakistan.

Several visions can be triangulated as relates to such a multi-source method and therefore, such a multi-source method would provide more support to the finding.

Data Analysis

The data will be collected through thematic analysis defined by Braun and Clarke (2006). This involves:

The acquaintance with data through repeated patterns;

The development of initial codes (some are: "selective enforcement of PECA," freedom of expression issues, political manipulation).

Trying to define themes (e.g. State control vs. civil liberties, Platform governance gaps, Digital authoritarianism vs. democracy checks).

Using thematic approach, this paper aims to describe such trends of sibling imagined mobilities and contradictions of cyber governance in Pakistan.

Scope and Delimitations

The emphasis of the study shall primarily be on Pakistan i.e the legal and political status; sources shall be primarily the international ones which shall serve as a benchmark in terms of position (EU, USA, China). Although the main channels of analysis will be the broadly occupied social media platforms of public relations Facebook, X (Twitter), Tik Tok and YouTube, other digital communication channels are not covered in analysis. It is not also a research based on a survey with radio interview; the secondary data of the experimenter is utilized.

Ethical Considerations

It is a secondary source analysis, not fieldwork. The study ensures:

Intellectual Property will turn into APA quotation of information.

Bias free Multipolarism (state, civil society, international organisations).

A respectful communication recognizing the need and relevance of control and maintaining freedom of expression as well as attempting to find a solution between the two.

Limitations of the Study

The outcomes are not quantitative but qualitative since they were obtained based on second-hand data.

The incredibly rapid growth of technological disruption (e.g., artificial intelligence-based misinformation) may saturate the body of research that has already been undertaken, and diminish the empirical utility of research over time.

As noted previously, access to some official documents or data can be restricted by political sensitivities on digital governance in Pakistan.

Nevertheless, the study does provide some insight in understanding cyber politics and cyber law in Pakistan.

Findings and Discussion

This research study is based on the outcome of thematic analysis of legal texts, case studies, literature and policy documents. No-but it is in all of this race of RatRelations of power Relations of power however Once of this, the then issues of hate speech and false Information in Pakistan on the Internet, the questions of really making an intervention to have worked in her favour. The resultant convergence of legislative frameworks, political practices, and democratic laws were predetermined by the following themes.

Theme 1: The two sides of a coin of cyber politics.

With the introduction of social media in Pakistan, novel and unheard-of opportunities of engagement in politics have been generated. It has made possible as well as per the opportunities the social media that Facebook and X (Twitter) in (Shah and Khan, 2021) suddenly found themselves in, and with a bit more added to it (Khan and Shah, 2021) allowed the politicians to get familiar with one another and form networks. During this period hate speech, trolling and misinformation experiences fostering on the same platforms. This is

explained by the fact that that any participation was not merely democratized due to the cyber politics, but also the polarized politics.

Discussion: Shares the notion of Castells (2013) of the internet as a networked public sphere, although in the Pakistani context this battleground is quite conflictual, and, to a great extent, toxic.

Theme 2: PECA 2016 strengths and weaknesses.

The main component of cyber regulation in Pakistan remains to be the Prevention of Electronic Crimes Act (PECA) 2016. The new findings have established that despite all the provisions in PECA law on hate speech and misinformation, the law has not been fully and consistently applied. Civil society organizations and journalists also reported PECA was used against the political elite more than against people who do harm online (Baloch 2021).

Digital authoritarianism concerning This is the situational prephenomenality of one of the modifications of digital authoritarianism in the act which has already become imported into practice, and which the citizens themselves pre-reflect in that it is peaceful, has been pre-harbored in a denial of political disengagement.

Theme 3: the Idiotically Toad Ideas: Hate and Misinformation.

I found in the literature that the laws defining hate speech and misinformation are absent in Pakistan as a nation (Shad, 2018). Consequently, practice tends to reduce to the way authorities have things to say. Case reports have been published where the sensitivity of religion was selectively nurtured towards suppression rather than protection.

Discussion: Pakistan model will not be optional in contrast to universal models such as Digital Services Act in the EU, and will not be viable as an ad hoc model.

Theme 4: Digital Behavior: Coercive Politics.

Political agents meanwhile regularly peddle falsehoods themselves whilst simultaneously demanding regulation in content they personally do not favor. Being politicians, we provide examples of how political parties release doctored videos or hashtags in the style of debunking of their political opponent (Youseaf, 2022). Meanwhile, the cyber authorities monitor the opposition voices by using the cyber laws.

Rationality is what is the antithesis of the case flying-foxes has political regulation of the cyber. And its perspective is consistent with the platform governance triangle as articulated by Gorwa (2019) which pits states, political actors, and tech companies in competition over who will gain the upper hand in cyberspace.

Theme 5: Pakistan, Ownership of Comparisons and Learning in the World.

In comparing the visions around the different technologies of the matter it might occur that other states such as the EU is interested in salary among states, pictures consolation and the civil storey though the US is researching into the rights of the language of expressions. Instead, Pakistan is caught in the middle of an open door and suffocation censorship.

Discussion: The results appear to suggest that in Pakistan, a hybrid model should be considered - borrow the best ideas of the world but alter them according to the particularities of the local socio-political state. This includes the improved definitions of and response to offline mishap, autonomous examination agents and the proliferated cooperation with social network companies.

Theme 6: Democratic Dilemma: Liberty vs. Police.

The outcomes point out a primary contradiction: we require free cyber-space to collect polarization and misinformation, and, pushing the concept of this free-space as far as possible, we degrade freedom of speech. Similarly, according to Opinion Group (Adherence,

Opinions, Amnesty International), PECA through the appropriate means developed by the systematically harassment of dissent in a disproportionate manner.

Included: Discussion: Circle Not tension per se, but circling it, cyber regulation in Pakistan. Reforms must therefore provide a balance of ensuring citizens are not ill-treated, but rights provided in Article 19 of the Constitution of Pakistan or under the international covenant on civil and political rights must not be hindered.

Thematic Table

Theme	Key Findings	Supporting Evidence	Implications
Cyber Politics as a Double-Edged Sword	Social media expands participation but increases polarization	Khan & Shah (2021); Castells (2013)	Opportunity for democratization, but risk of toxic political culture
Effectiveness & Limitations of PECA 2016	PECA provisions exist but applied selectively	Government of Pakistan (2016); Baloch (2021)	Undermines trust in law; promotes “digital authoritarianism”
Ambiguity in Definitions	Lack of clear definitions of hate speech & misinformation	Shad (2018)	Enables arbitrary enforcement and censorship
Political Exploitation of Regulation	Political actors use misinformation while calling for regulation	Yousaf (2022)	Politicization of cyber laws; erosion of credibility
Global Comparisons	EU = co-regulation; US = free speech; Pakistan = oscillation	Gorwa (2019); Hussain (2021)	Need for hybrid model tailored to Pakistan
Freedom vs. Regulation Dilemma	Risk of censorship vs. risk of online harm	Amnesty International (2020)	Requires balance between democratic rights & regulation

Findings and Discussion conclusions.

The conclusiveness indicates just how much potential and at the same time a curse and a blessing cyber politics and cyber law in Pakistan are, and just how applicable they are in the context of the role of the state in parliamentary life of the democratic state and the dilemma of the state. Insofar as PECA 2016 is on the right path in terms of regulation, and insofar as this is so, the act is flawed with shortcomings in lack of straightforwardness, and partisanship and prejudice in application. This paper identifies what is learned during the experience of the international models which suggested that a hybrid, balanced, model should be created in such a way that it will improve cyber governance in Pakistan and at the same time will not cause any breaking of the rules of democracy.

To some extent, it is revealed that resolutions of the investigation will be capable of demonstrating that, in spite of a fundamentally new chance the political intervention into the movie of online space, the very question of polarisation, of disinformation and of abuse has worsened, as well.

Conclusion

This study has carried out an analysis of cyber politics and cyber law in Pakistan, as applied to hate-speech and misinformation through online use in political affairs. The opposite of co-

regulatory model in the EU, the free-speech model in the USA, in which the state incentives will unscrupulously regulate, and the accumulation will take place in the circumstances in which it may be required. Not only are social media platforms rather contentious spaces in which to narrate specific stories, but are also exploited by political actors as a means to propagate hate speech.

By imitating the Pakistan version of the Prevention of Electronic Crimes Act (PECA) 2016, electronic regulation is being shifted in the right direction. However, due to broad wordings of the provisions, selective interpretation and misapplication, the question of the effectiveness of the anticorruption laws, and how it impacts on human right and good democracy to the people has been raised. The danger lies in the middle of this debate, and there is a narrow border between safety clauses on the internet and free speech.

As part of the retrospective, Pakistan should make an effort towards an omnibus platform which will not only tame the annihilatory digital trend, but also venerate the democratic principles of liberty, globality and accountability. The menacing wave of sectarianism and hate speech of the internet in Pakistan.

Recommendations

Referring to the findings, one would offer the following policy recommendations:

Clear Legal Definitions

Modify PECA 2016 to provide clear definitions of what is referred to by hate speech, misinformation and disinformation.

make sure that they comply with the international human rights law, such as ICCPR Article 19, Propeller Head (Independent Oversight Mechanism)

- o Establish a professional, cyber regulatory body to overrule PECA implementation that is unaffected by politics.
- o Ensure that there are oversight structures which have civil society, academic and legal representation.

Platform Accountability

Establish collaborative measures on a legal platform under which social media corporations would be obliged by law to remove harmful information within a time regulation.

| Subject Platforms may operate using the local language (Urdu, Pashto, Punjabi, Sindhi) content moderation policies of Pakistan.

Securing the right to expression.

- o Include clauses in PECA so that there is no misuse of cyber laws to persecute journalists, activists and political enemies.

requires the court check of a measure such as the suspension of an account, seizure of person, or seizure of content,

Digital Literacy Campaigns

- o Host national awareness campaigns about misinformation detection, Internet laws, and good digital citizenship.

n. bring media and digital literacy into ed. schools/universities.

Capacity Building Law Enforcement Organizations.

- o Specifically educate the Federal Investigation Agency (FIA) cybercrime wing on the way to handle hate speech and malicious information cases in a professional and impartial manner.

Local and global work.

share best practices and technical expertise with foreign organization and transnational internet networks on ways to counter online harms.

Begin activities to participate in international governance forums in cyberspace and ensure that the regulatory environment follows global standards.

Guest lecture at Policy Dialogue on Research.

- o Mobilize the efforts of universities and think tanks to conduct continuous research on cyber politics, misinformation and digital governance;
- form policy negotiation between government, political parties, civil society and media to facilitate unanimity on cyber regulations,

Final Remark

Cyber politics is here to stay and its effects are bound to grow in Pakistan as the number of people using the internet keeps swelling. This requires an open, transparent and rights-based cyber governance framework. That is, sufficient laws governing hate speech or political misinformation online have to go hand in hand with protecting the freedom of expression online in the digital era in order to make Pakistan strong in democracy in the post-internet era.

References

- Abbas, A. (2019). *Digital hate speech and sectarianism in Pakistan: An emerging threat*. *Journal of South Asian Studies*, 34(2), 145–162.
- Amnesty International. (2020). *Human rights concerns in Pakistan's digital regulations*. London: Amnesty International Publications.
- Baloch, F. (2021). Cyber laws and press freedom in Pakistan: A contested terrain. *Asian Journal of Media and Communication*, 12(3), 55–72.
- Brown, A. (2017). *Hate speech law: A philosophical examination*. Routledge.
- Castells, M. (2013). *Networks of outrage and hope: Social movements in the internet age*. Polity Press.
- Chesney, R., & Citron, D. (2019). Deep fakes: A looming challenge for privacy, democracy, and national security. *California Law Review*, 107(6), 1753–1820.
- Gillespie, T. (2018). *Custodians of the internet: Platforms, content moderation, and the hidden decisions that shape social media*. Yale University Press.
- Gorwa, R. (2019). The platform governance triangle: Conceptualizing the relations between states, firms, and civil society in the platform economy. *Internet Policy Review*, 8(2).
- Government of Pakistan. (2016). *Prevention of Electronic Crimes Act*. Islamabad: Ministry of Law and Justice.
- Hussain, S. (2021). Digital authoritarianism and freedom of expression in Pakistan. *Pakistan Journal of Political Studies*, 28(1), 33–50.
- Khan, M., & Shah, S. (2021). Cyber politics and political communication in Pakistan: Opportunities and threats. *Journal of Political Studies*, 28(2), 101–118.
- Kugelman, M. (2020). Pakistan's digital transformation: Opportunities and risks. *Wilson Center Report*.
- MacKinnon, R. (2012). *Consent of the networked: The worldwide struggle for internet freedom*. Basic Books.
- Naseer, A. (2020). Misinformation in Pakistan's digital age: Causes and consequences. *South Asian Media Journal*, 11(1), 77–96.
- Shad, S. (2018). Cyber law and governance in Pakistan: A critical review. *Asian Yearbook of International Law*, 23(1), 212–234.

- Trechsel, A. (2022). Cyber politics: The new frontier of political engagement. *Journal of Democracy and Technology*, 3(1), 14–26.
- UNDP. (2020). *Pakistan national human development report: The next generation*. United Nations Development Programme.
- Wardle, C. (2019). *Information disorder: Toward an interdisciplinary framework for research and policymaking*. Council of Europe Report.
- Wardle, C., & Derakhshan, H. (2017). *Information disorder: Definitions and typology*. Council of Europe Report.
- Yousaf, F. (2022). Social media, political misinformation, and democracy in Pakistan. *Asian Journal of Communication*, 32(4), 289–306.