

FREE SPEECH IN PAKISTAN: A CRITICAL DISCOURSE ANALYSIS OF PREVENTION OF ELECTRONIC CRIMES ACT (2016) AND PECA ORDINANCE (2022)

BY

HAJRA KARIM



NATIONAL UNIVERSITY OF MODERN LANGUAGES

ISLAMABAD

December, 2024

**FREE SPEECH IN PAKISTAN: A CRITICAL
DISCOURSE ANALYSIS OF PREVENTION OF
ELECTRONIC CRIMES ACT (2016) AND PECA
ORDINANCE (2022)**

By

HAJRA KARIM

M.A., National University of Modern Languages, Islamabad, 2000

A THESIS SUBMITTED IN PARTIAL FULFILMENT OF
THE REQUIREMENTS FOR THE DEGREE OF
MASTER OF PHILOSOPHY

In **English**

To

FACULTY OF ARTS & HUMANITIES



NATIONAL UNIVERSITY OF MODERN LANGUAGES, ISLAMABAD

© Hajra Karim, 2024



FACULTY OF ARTS & HUMANITIES
NATIONAL UNIVERSITY OF MODERN LANGUAGES

THESIS AND DEFENSE APPROVAL FORM

The undersigned certify that they have read the following thesis, examined the defense, are satisfied with the overall exam performance, and recommend the thesis to the Faculty of Arts & Humanities for acceptance.

Thesis Title: Free Speech in Pakistan: A Critical Discourse Analysis of Prevention of Electronic Crimes Act (2016) And PECA Ordinance (2022)

Submitted by: Hajra Karim

Registration #: NUML-S21-22371

Dr. Shehr Bano Zaidi
Name of Research Supervisor

Signature of Research Supervisor

Dr. Farheen Ahmed Hashmi
Name of Head (GS)

Signature of Head (GS)

Prof. Dr. Arshad Mahmood
Name of Dean (FAH)

Signature of Dean (FAH)

Prof. Dr. Safeer Awan
Name of Pro-Rector (Academics)

Signature of Pro-Rector (Academics)

Date

AUTHOR'S DECLARATION

I, Hajra Karim

Daughter of Abdul Karim Khan

Registration # NUML-S21-22371

Discipline: English Linguistics

Candidate of **Master of Philosophy** at the National University of Modern Languages do hereby declare that the thesis entitled: **Free Speech in Pakistan: A Critical Discourse Analysis of Prevention of Electronic Crimes Act (2016) and Peca Ordinance (2022)** submitted by me in partial fulfillment of MPhil degree, is my original work, and has not been submitted or published earlier. I also solemnly declare that it shall not, in future, be submitted by me for obtaining any other degree from this or any other university or institution.

I also understand that if evidence of plagiarism is found in my thesis/dissertation at any stage, even after the award of a degree, the work may be cancelled and the degree revoked.

Signature of the Candidate

Hajra Karim

Name of the Candidate

Date

ABSTRACT

Free Speech in Pakistan: A Critical Discourse Analysis of Prevention of Electronic Crimes Act (2016) and PECA Ordinance (2022)

In the digital era, where legislations are promulgated to meet the challenges brought up with technological advancements, Pakistan's legal landscape regarding electronic transactions and cybercrimes has evolved significantly. This study aims to critically analyze the Prevention of Electronic Crimes Act 2016, and PECA Ordinance 2022, focusing on their impact on free speech in Pakistan. Using Wodak's Discourse Historical Approach (DHA) to analyze the linguistic and historical context of these legislations, the study reveals that these laws impose substantial constraints on free speech. The research considers the influence of political and ideological factors in shaping cyber laws, demonstrating how regulatory mechanisms can be leveraged to control narratives in the digital space. By analyzing public reactions at both national and international platforms, the study sheds light on the societal reception of these legal measures and their impact on democratic participation. Ultimately, the findings advocate for reforms that promote transparency, accountability, and a rights-based approach to digital legislations in Pakistan. The findings underscore the restrictive nature of these regulations, highlighting the tension between ensuring cyber security and preserving fundamental rights. The study's implications stress the need for a balanced approach that safeguards both digital security and the freedom of expression, contributing to ongoing discussions about policy reform in Pakistan.

TABLE OF CONTENTS

THESIS AND DEFENSE APPROVAL FORM	ii
AUTHOR’S DECLARATION	iii
ABSTRACT	iv
TABLE OF CONTENTS	v
LIST OF TABLES.....	viii
ACKNOWLEDGEMENTS	ix
DEDICATION	x
1. INTRODUCTION	1
1.1 Background of the Study	1
1.2 Pakistan and Freedom of Speech	3
1.2.1. Background to the Promulgation of ETO 2002.....	5
1.2.2. Background to the Enactment of PECA (2016) and PECA Ordinance (2022)	6
1.2.3. Re-Evaluating Free Speech in Pakistan.....	7
1.3. Application of Ruth Wodak’s Discourse Historical Approach (DHA)	9
1.4. Problem Statement.....	9
1.5. Objectives of the Study.....	10
1.6. Research Questions.....	10
1.7. Significance and Rationale of the Study.....	10
1.8. Delimitation of the Study.....	11
1.9. Overview of Research Methodology	11
1.10. Division of Chapters	12
2. LITERATURE REVIEW	13
2.1. Language of Legislation	13
2.2. Creating a Legal Narrative.....	14
2.3. Linguistic Features of Legislative Language: Language of Legislation.....	15
2.3.1. Lexical Choices in Legislations.....	15
2.3.2. Nominalization and Abstraction.....	16
2.3.3. Ambiguity in Legislation.....	16
2.3.4. Persuasive and Emotive Vocabulary	16
2.3.5. Legal Consequences and Enforcement Lexicon:.....	16
2.3.6. Mitigative Language.....	17
2.3.7. Cultural and Societal References.....	17
2.4. Legislative Activism.....	17
2.5. Legislative Activism in Pakistani Context.....	19
2.6. Right to Power Distinction	20

2.6.1. Power and Ideology in Critical Discourse Analysis	21
2.7. Background to Free Speech in Pakistan	22
2.8. Critical Discourse Analysis of Social Media Discourse	27
2.9. Review of Works Done by Application of DHA (Ruth Wodak)	28
2.9.1. Major Applications of DHA in Research.....	28
2.10. Research Gap	30
3. RESEARCH METHODOLOGY	32
3.1 Research Design	32
3.2. Research Data	33
3.3. Rationale for Selection of Data.....	33
3.4. Delimitation of Data	34
3.5. Epistemology	35
3.6. Theoretical Framework.....	35
3.7. Discourse Historical Approach (DHA).....	36
3.8. Ruth Wodak and Discourse Historical Approach.....	36
3.8.1. The Linguistic Co-text.....	37
3.8.2. Ruth Wodak's Discursive Strategies:	37
3.8.2.1. Referential Strategy or Strategy of Nomination	38
3.8.2.2. Strategy of Predication	38
3.8.2.3. Strategy of Argumentation	38
3.8.2.4. Strategy of Perspectivation, Framing and Discourse Representation.....	38
3.8.2.5. Strategies of Intensification and Mitigation.....	38
3.9. Ethical Consideration.....	40
4. DATA PRESENTATION, ANALYSIS AND DISCUSSION	41
4.1 Analysis of Pakistan Electronic Cybercrimes Act (PECA) 2016	41
4.1.1. Linguistic Co-Text in PECA (2016).....	42
4.1.2. Discursive Strategies used in PECA (2016).....	47
4.1.2.1. Referential Strategies Used in PECA (2016).....	47
4.2.1.2 Analysis and Discussion of Use of Referential Strategy in PECA 2016	59
4.1.2.3. Use of Nominalization Strategy in PECA 2016	61
4.1.2.4 Analysis and Discussion of Use of Nominalization Strategy in PECA 2016:.....	63
4.1.2.5. Use of Predicative Strategy in PECA 2016:	63
4.1.2.6 Analysis of Use of Predicative Strategy in PECA 2016	66
4.1.2.7. Use of Argumentative Strategies in PECA, 2016.....	67
4.1.2.8. Analysis of Use of Argumentative Strategy in PECA 2016	72
4.1.2.9. Use of Perspectivation Strategy in PECA 2016:	73
4.1.2.10. Use of Framing Strategy in PECA, 2016.....	75

4.1.2.11 Analysis and Discussion of Use of Framing in PECA 2016	77
4.1.2.12. Discourse Presentation in PECA (2016).....	78
4.1.2.13 Evidence of Discourse Presentation in PECA 2016	78
4.1.2.14 Analysis and Discussion of Use of Discursive Strategies in PECA 2016	79
4.2. Analysis of PECA Ordinance 2022	80
4.2.1. Linguistic co -text in PECA Ordinance 2022.....	81
4.2.2. Use of Discursive Strategies in PECA Ordinance 2022.....	83
4.2.2.1. Use of Predication Strategy	83
4.2.2.2. Use of Referential Strategy.....	83
4.2.2.3. Use of Perspectivation Strategy	84
4.2.2.4. Use of Argumentation Strategies.....	84
4.2.2.5. Mitigation and Intensification in PECA Ordinance 2022.....	85
4.2.2.6 Analysis of Use of Discursive Strategies in PECA Ordinance 2022	86
5. FINDINGS AND CONCLUSION	88
5.1. Findings of the Research	88
5.1.1. Textual, Social and Discursive Practices in PECA, 2016	88
5.1.2. Fulfillment of Free Speech Conditions in Ordinance 2022 of PECA	90
5.2. Conclusion	93
5.3 Suggestions for Future Researchers.....	93
5.4 Conclusion.....	96
REFERENCES	97

LIST OF TABLES

Table 1: A Selection of Discursive Strategies as Adapted from Rasegill and Wodak (2009: 104).....	39
Table 2: Linguistic Choices in PECA (2016) and Description of its Co-Text	43

ACKNOWLEDGEMENTS

I would like to pay my deepest reverence to the unwavering pillars of strength, Dr. Shehr Bano Zaidi, my supervisor, whose unwavering guidance, encouragement, and trust in me played a pivotal role in shaping my research journey. Your mentorship was the beacon that illuminated my path. My special thanks to Dean F.A.H, Dr. Arshad Mehmood, Head of GS Dept, Dr. Farheen Ahmed Hashmi, Coordinator MPhil, Dr. Samina Qayyum, and Mr. Zubair, Assistant GS Department whose guidance, and expertise provided invaluable direction to my research and academic progress. I also extend my deepest gratitude to my elder sister Dr. Attiya Karim, whose selfless financial support enabled me to pursue my dreams, to my younger sister, whose constant encouragement and moral support fueled my determination, and most importantly to my children. who endured challenges with resilience and optimism, always reminding me with their smiles that this too shall pass. Although this journey was mine alone, but your love and support made the path less daunting. Your contribution, though unseen by many, is embedded in every page of this work.

DEDICATION

I dedicate my thesis to Allah Almighty, the Beneficent and Merciful, who has blessed humanity with the gift of language and the cognitive ability to harness its power. His divine wisdom has enabled us to create, express, and comprehend the complexities of language, allowing us to connect, communicate, and shape our understanding of the world. I humbly dedicate this thesis to my beloved father Abdul Karim Khan who had always been a source of great inspiration for me throughout this journey but left this temporary world before its completion.

CHAPTER 1

INTRODUCTION

The emergence of digital technologies and the internet has substantially altered the landscape of free speech in Pakistan. Hence rendering to the need for taking legislative measures to sort out serious cybercrime issues that came up with the technological advancement. In this regard the key legal documents promulgated by the National Assembly of Pakistan are PECA 2016 and PECA Ordinance 2022 respectively. This study employs Ruth Wodak's Discourse-Historical Approach (DHA) to critically analyze the aforementioned legislations.. These regulatory measures have changed digital communication and the country's free speech boundaries. Exploring the discourse around these laws, the current research seeks to uncover the embedded stories and the overlapping power dynamics that influence the drafting and enforcement of these laws. It will make use of Critical Discourse Analysis (CDA) methodologies to uncover underlying power dynamics and ideologies inherent in these regulations offering a nuanced perspective on the ongoing debate about free speech in Pakistan.

1.1 Background of the Study

Language is an essential tool for expressing ideas between people via communication. It facilitates efficient communication by giving expression to difficult concepts, feelings, emotions, ideas, and cultural values. Before the current international human rights frameworks, there was a lengthy history of the notion of freedom of speech and expression. Saeed (2020) says "It is thought that free speech was highly prized in the democratic ideals of ancient Athens, which arose in the late sixth or mid-fifth century BC, as the earliest human rights treaties also include the concept of freedom of expression". The constitutional right to freedom of expression in Parliament was first established in 1689 by the English Bill of Rights which is still effective today.

As information and communication technologies have advanced, a lot of human activities that were formerly done offline have been shifted to online platforms. According to Kundi et al. (2014), "there has been a noticeable surge in internet usage due to this change, which is also observable in Pakistan". Human communication patterns, types, and breadth have all been profoundly altered by the internet. "Access to a great quantity of information through a variety of devices, including computers,

tablets, cellphones, and more, has quickly and easily changed modern civilizations throughout the world”. (Mailland, 2000).

“The Strasbourg Court recognized the internet technology as an unparalleled medium for expressing free speech. Although the development of technology has made many parts of life simpler but its malicious use at times has raised serious security concerns over time around the world. Many countries have enacted strict cyber laws in an effort to stop these acts, which had a major influence on freedom of expression among other liberties (Eboibi, 2017”).

Freedom of expression is the cornerstone of human rights upholding all other rights of the society together. It is the power and capacity to ensure the possibility of social change and advancement. It has the capacity to listen and respect the opinions of others. Free speech means communicating opinions and beliefs without fear of repression or legal ramifications. The ability to express freely in an acceptable way is one of the top priorities of almost every human being. Rachael Jolley, a reporter/editor of "The Times" magazine, believes free speech to be a crucial element of change in society. According to Rachael J. (2009), “free speech is a highly important element that tends to bring positive changes in a society, especially when the society is striving for change and betterment”. She further states that “the rights that human beings (men and women) are enjoying today, could not be possibly achieved without freedom of speech. If we look back at the past times when women did not have the right to vote and had to forcefully participate in projects like fields and mines, we realize that only freedom of speech has freed women of such drastic undue situations”.

Human rights activist Peter Tatchell (2006) “believes that change and progress in society and bring change, it is essential to protect rights and opinions in a challenging manner against those having different viewpoints”. He further states, that “freedom of speech does not allow anyone a license or a free pass to say anything, it also has moral and ethical boundaries that must be practiced. It includes the right and moral imperative to challenge, oppose, and protest bigoted views. If reasonable ideas within the limits of set boundaries are expressed, they can most effectively defeat opposite ideas despite implementing censorship and putting ban on them”.

The Universal Declaration of Human Rights was drafted by United Nations officials in 1948. These declarations were developed to prevent the recurrence of global

conflicts like the Second World War. Article No.18 and article No.19 of Human Rights Declaration, 1948 are directly related to freedom of speech. Additionally, article no.18 gives all humans the right to practice according to their religious beliefs whereas, Article no. 19 ensures everyone the freedom to express their thoughts in their desired manner. This Declaration document has proved to be a key factor in initiating human rights campaigns all over the world. It was put into effect for most of the world's nations, including the United Kingdom. It guaranteed people's right to express themselves without restraint but also stated that this right would be subject to interrogation under certain circumstances as a national security risk.

In United States the “First Amendment” of the constitution guarantees freedom of speech, press and assembly. With the help of this amendment in the country's constitution, the American citizens were given the right to present their views in public places without any restrictions. According to Alexander Meiklejohns theory of Democratic Participation “freedom of speech is essential for a democratic self-government”. Hence freedom of expression plays a vital role to practice the true essence of democracy.

1.2 Pakistan and Freedom of Speech

After the independence of Pakistan, the founder of Pakistan, Quaid-e-Azam Muhammad Ali Jinnah declared the right of freedom of speech to every Pakistani in his address to the first Constitutional Assembly of Pakistan (www.pakistani.org). Quaid's concept of freedom includes not only the right to freely exercise one's religion, but in the broader perspective, it is the freedom to express ideas, thoughts, beliefs, and views reflected in our speech. In his historic speech on 11th August 1947(Quaid's speech, page no.4, para.3, 11th August 1947, Constitutional Assembly of Pakistan) he emphasized that social, political and religious justice will remain assured not only for the Muslims but also for minorities. He reiterated that there will be equal rights of citizenship for all without discrimination of religion. Thus, Quaid reinforced Meiklejohns theory of Democratic participation, by highlighting the significance of free speech, being essential for the survival and development of a democratic system. He expected the journalists to be completely fearless emphasizing his stance (Quaid and the Press, 1947).

Free speech is a fundamental component of a democratic society and must be protected as it is generally acknowledged in the 1973 Constitution of Pakistan. The right to free expression is among humanity's vital rights and free democratic community requires unrestricted dissemination of information and ideas. While some individuals think that the right to free speech should be protected at all costs, others believe it can be used as a justification for saying offensive things without being held accountable. In theory, someone may find offense in almost any notion depending on their point of view. Freedom of speech leads to freely expressing one's ideas and opinions which is a highly important factor for a society, being humanity's most cherished and significant human right. Almost every thought, view, or idea can annoy individuals. For instance, the most important and profound ideas in human history, such as those of Charles Darwin and Galileo, deeply upset the prevalent religious mood of the time.

In this regard, it is highly important to discuss freedom of expression on digital platforms. Internet can be seen as a form of a public forum that gives voice to people and also promotes the free exchange of information in more common place settings. For instance, the use of the internet sources such as Google, Wikipedia, Facebook, Instagram, WhatsApp etc. are full of authentic content that is created, revised, and verified by anybody who wishes to contribute or share through these platforms. Such freedom illustrates how ordinary people practice moderation through freedom of expression on these platforms. Many diverse aspects of society benefit from unrestricted access to freedom of expression. It is a fact that freedom of speech has great importance in democracies, justifying its worth. Due to regulated speech, our liberties can be compromised. To resolve minor to complicated issues critical dialogues are essential components, and they cannot take place without the freedom to express opposing viewpoints. Ideas can be contested, altered, and improved through free speech.

Jack M. Balkin (2004) has developed a theory on freedom of speech in the digital era. In his theory, Balkin argues that "the digital revolution has transformed the social conditions of free speech, enabling ordinary individuals to participate in the creation and dissemination of information on massive scale". However, the digital advancements have also created new conflicts. It is important to take measures to prevent unlawful activities on these platforms. Occasionally, these forums are reluctant to accept editorial accountability for the potentially harmful content on their platforms.

Digital platforms are highly vulnerable to harmful content, unauthentic information and harmful notions because they do not filter material like media platforms such as television or radio. The replacement of digital platforms is completely inevitable as it will be considered as depriving them of their freedom of expression.

Nevertheless, it is crucial to note that the restrictions on the right to free speech depend on the particular situation. As an illustration, even if the right to speak one's mind is granted at the workplace, it must be practiced in such a manner not causing harm or negative impact to others as well as to the speaker's career. It is unethical to exercise one's right to free speech to defame others whether in real life or on digital platforms.

In order to stop illicit activity on internet, Pakistan passed three major cybercrime legislations as Electronic Transactions Ordinance (ETO) in 2002, the Prevention of Electronic Crimes Act (PECA) in 2016 (Daudpota, 2016) and immediate amendment in PECA (2016) i.e. PECA Ordinance 2022. As compared to other cybercrime legislation around the globe, PECA 2016 imposes severe and harsh sanctions, including illegal behavior that is not deemed illegal in other nations. A few provisions under the PECA 2016 limit the freedom associated with the internet, including free speech, access to information, and privacy rights. According to Kamal (2017) and Khan, Tehrani, & Iftikhar, (2019) “enacting laws that strike a balance between protecting free expression and combating cybercrime has long been a top priority in influencing the ever-smaller public conversation area”. Here it is crucial to know the background that led to the enactment of these cybercrime legislations.

1.2.1. Background to the Promulgation of ETO 2002

The Electronic Transactions Ordinance (ETO-2002) is the first meaningful effort by the Pakistani government to control electronic transactions and online communication dates to 2002's ETO 2002. It was consequently enacted to respond to growing use of electronic commerce by providing a legislative framework for electronic transactions, ensuring the authenticity and integrity of electronic records and facilitating electronic signatures' acceptance. Though ETO 2002 originally focused on e-commerce despite that it served as a model for subsequent legislation required to monitor digital communication and freedom of speech. Its introduction in Pakistan coincided with the growing awareness and adoption of the internet in the country. This

legislative measure aimed to legitimize digital communications by providing legal recognition for electronic documents and signatures, thereby addressing the emerging issues associated with digital communication. However, the far-reaching implications of ETO 2002 on freedom of expression were not immediately apparent.

In Pakistan, before the implementation of PECA (2016), the Electronic Transactions Ordinance 2002(ETO) was in place to criminalize illegal/unauthorized access to information. It did not give direct instructions for data protection but indirectly illegalized any attempt to approach any individual's or organization's private information. ETO-(2002) authorized the government to certify electronic documents and regulate its users' privacy and protection. The increased use of digital media resulted in the emergence of alarming issues, which led to the formation and enforcement of a law that would help safeguard the digital rights of individuals. These laws were made for citizens' security and protection, which was an undeniable fact. The ETO (2002), an old-fashioned criminal justice framework, was declared insufficient to deal with the threats of the 21st-century cyber era. The tragic incident of the Peshawar Army Public School (2014) attack claiming 141 lives, mostly of school children, stood as an unparalleled sad example of the ineffectiveness of ETO (2002) and an eye-opener to develop technically well-equipped legislation to deal with such issues. These tragic events voiced the need to scrutinize any questionable extremist content, combat hate speech as well as stop the online harassment of women as well as innocent children. Hence, on August 11, 2016, the Prevention of Electronic Crimes Act (PECA, 2016) was passed by the National Assembly of Pakistan.

1.2.2. Background to the Enactment of PECA (2016) and PECA Ordinance (2022)

The technological advancements increased the use of digital media with time and proved ETO (2002) to be ineffective, as well as incomprehensible, in dealing with the growing threats of cybercrimes. Likewise, the situation led to the creation of the legislation Prevention of Electronic Crimes Act (PECA) by authorities that came into effect in 2016. After its approval, it was immediately made visible to the parliamentarians and the public, which raised eyebrows and uproar for bringing deprivation despite facilitation. As internet usage expanded over time, it became increasingly evident that comprehensive legislation was necessary to govern the complexities of online interactions, ultimately culminating in the enactment of the

Prevention of Electronic Crimes Act (PECA). This trajectory underscores the evolving nature of internet governance in Pakistan and the need for adaptive legislative frameworks to address the dynamic challenges posed by digital technologies.

The Prevention of Electronic Crimes Act is (PECA) 2016, is a law published as technology advanced aiming to prevent cybercrimes. As a pioneer of the same perspective Jack M. Balkins developed a theory on freedom of expression in the digital era also addresses the change of social conditions of speech leading to multiple opportunities as well as challenges. Digital media use has grown, creating problems referred to as cybercrimes. PECA (2016) soon acquired a negative reputation for being unlawful. Also, after its approval, it gained much attention and fame as the most controversial topic under discussion in the country's history. It was followed by an unending debate, mainly in the form of criticism. Facing such arguments is a part of legislative processes, especially when new laws are promulgated and made public in a democratic setup. Contrary to the naturally occurring reaction, in the case of PE), the wide range of criticism resulted in keeping it highly secret during its formation. To stifle free expression and prevent consultation from members of parliament, the authorities responsible for drafting PECA (2016) avoided seeking their input and instead maintained an unconstitutional level of secrecy. They intentionally refrained from set rules to be followed, as a matter of fact, in every democratic setup during its promulgation. Therefore, Pakistan, a purely democratic country, deprived its parliamentarians of their right to free expression, which they might have exercised if the legislation had been submitted for comment during its development.

After the completion phase of PECA (2016) when it was initially presented in the parliament, the opposition parties showed robust resistance. But, they soon agreed with the government to support it with the condition of making some proposed amendments. The suggested amendments were superficial, but the parliament members seemed satisfied with the justification that these changes would help scrutinize cybercrimes effectively. When the bill was presented for voting in the parliament in August 2016, the opposition parties, who were in the majority, voted against it, but with the efforts and valuable strategies of the ruling party, it was accepted with a two-thirds majority in the National Assembly ensuring that PECA (2016) would become a fact. After the imposed implementation of PECA (2016), it started to reveal its secret intentions. Its impact became evident when the torchbearers of freedom of speech, i.e., political

workers, journalists, and news anchors, were charged with defamation of natural persons and were also blamed for being involved in anti-state activities. They were served the summons to appear in front of the counter-terrorism wing of Federal Investigation Authority (FIA).

1.2.3 Re-Evaluating Free Speech in Pakistan

In Pakistan, the legal document PECA (2016) and its amendment called PECA Ordinance, 2022 (-III) gained much attention. Though critics and analysts showed great concern, to the best of my knowledge, none of them applied a theoretical framework to explore its contents. To close this gap, I will use Ruth Wodak's Discourse historical approach (DHA) to investigate the circumstances in the background leading to its formulation. While conducting the critical discourse analysis of this document, i.e., PECA (2016--1), previous studies on documents will be consulted as a helpful tool for the description and interpretation of the document. A special focus will be laid on those parts of the Act, such as Section#, 37 that gives uncontrolled powers to the Pakistan Telecommunication Authority (PTA). It allows the privileged authority to block or remove online content before the knowledge of the individual concerned, hence restricting freedom of speech, which was mentioned and guaranteed in Article#9 of the constitution. The analytical study procedure of the PECA (2016) will include a detailed description of the Acts in the entire document through critical discourse analysis (CDA) to foreground the hidden issues (elements), as mentioned earlier.

In the current research applies the framework of critical discourse analysis (CDA) to analyze PECA 2016 and the PECA Ordinance 2022 to provide a clear understanding of how these laws have shaped and redefined the boundaries of free speech in Pakistan. By examining the discourse surrounding these legislative measures, the study will shed uncover the motivations, justifications, and implications of digital rights regulation. The re-evaluation of free speech in Pakistan is particularly relevant in the current global context, where issues of digital rights and online freedom are increasingly foregrounded. The findings of the study will contribute to the discussion regarding security and freedom of speech in the digital age offering insights into the challenges and opportunities for safeguarding free speech in a rapidly evolving technological landscape. It also provides a comprehensive framework for understanding the complex interplay between legislation, digital communication, and free speech in Pakistan. By applying Ruth Wodak's Discourse-Historical Approach, the study aims to uncover the

underlying discourses that shape the regulation of online spaces and contribute to the ongoing debates about free speech in the digital era. Through this analysis, the research seeks to provide a detailed and nuanced perspective on the evolution of digital rights and the implications for free speech in Pakistan.

1.3. Application of Ruth Wodak's Discourse Historical Approach (DHA)

Ruth Wodak's Discourse-Historical Approach (DHA) offers a comprehensive framework for analyzing the discourse surrounding these legislative measures. DHA emphasizes the importance of historical context and the interplay of different discourses in shaping social and political realities. By applying DHA to the analysis of PECA 2016 and PECA Ordinance 2022, this study seeks to uncover the underlying narratives and power dynamics that influence the regulation of free speech in Pakistan.

Discourse Historical Approach involves a multi-dimensional analysis that considers the historical, socio-political, and linguistic aspects of discourse. It enables researchers to examine how laws and policies are constructed, negotiated, and contested over time. In the context of this study, Discourse Historical Approach will be used to trace the evolution of digital rights legislation in Pakistan and its impact on free speech.

In the current study, the critical discourse analysis of PECA (2016), and PECA Ordinance (2022--III) will be conducted using methodological frameworks of CDA, by Ruth Wodak, namely Discourse Historical Approach (DHA) of CDA. It will be helpful to find any implied elements targeting freedom of speech in Pakistan by highlighting related underlying issues. This study will employ only qualitative research techniques. Uncovering such a document like PECA, 2016 & its Ordinance, February 2022. will help the lay audience to better understand the legislations and discover insights related to various hidden issues. The present study will help to develop public awareness disguised as promising security but on the contrary depriving them of their fundamental right of freedom of expression. It will also enhance a better understanding of the Act and its Ordinance. In addition, they will be able to use it to seek legal protection if they are victims of the cybercrimes outlined in the PECA of 2016.

1.4. Problem Statement

The thesis critically examines the Prevention of Electronic Crimes Act (PECA) 2016 and the PECA Ordinance 2022 to evaluate their impact on free speech in Pakistan.

Utilizing Ruth Wodak's Discourse-Historical Approach (DHA), this study explores how these legislative frameworks shape and constrain public discourse, reflecting broader socio-political power dynamics. Since their enactment, these cybercrime laws have raised concerns both nationwide as well as on international forums too for curtailing freedom of speech in Pakistan. By analyzing the language and implementation of these laws, the research aims to uncover the implicit ideologies and power structures that influence regulatory practices. It seeks to contribute to the ongoing debate on digital rights and freedom of expression, highlighting the need for a balanced approach that safeguards both security and civil liberties.

1.5. Objectives of the Study

1. To locate textual, social and discursive practices found in the PECA document that has called for its amendment through PECA-Ordinance-2022.
2. To identify the amendments which are expected to fulfill the precept of free speech in Pakistan.

1.6. Research Questions

The questions are placed in chronological order to do justice to the passing of these legislations:

1. What textual, social, and discursive practices can be located in the PECA document that called for its amendment via Ordinance (PECA_Ordinance-2022)?
2. In what ways can the amendment document be expected to fulfill the conditions of free speech taken as a precept?

1.7. Significance and Rationale of the Study

Although the constitution guarantees the right to free speech, it is seldom used in Pakistan because of bureaucratic hurdles. This research aims to examine the present state of free speech in the country and to identify the elements /factors that have impeded this process. The topic under study is significant since it addresses an issue that has recently received a lot of focus. The study aims to put forward the shortcomings in the PECA 2016 and PECA Ordinance 2022 that withdraw the freedom of individuals regarding free speech in Pakistan. Additionally, it will increase public knowledge of the government's covert activities, which resulted in the PECA 2016 amendment by an Ordinance in February 2022.

1.8. Delimitation of the Study

This study focuses on a Critical Discourse Analysis (CDA) of the significant legislative documents in Pakistan regarding digital security such as the Prevention of Electronic Crimes Act (PECA) 2016, and the PECA Ordinance, 2022. Critical Discourse Analysis (CDA) of a legal document might be done using a wide range of available CDA models developed by linguists and sociolinguists. However, the present study will be delimited its analysis to Ruth Wodak's Discourse Historical Approach of CDA only. The primary data for this research will be the original text of the selected legislations i.e. PECA, 2016 and PECA Ordinance, 2022. These legislative frameworks will be analyzed as cybercrime laws reinforcing the implied intentions of curtailing freedom of speech while promising cyber security to citizens from digital crimes. This study delimits its scope to textual analysis of the documents as mentioned earlier and the discourse surrounding their implementation. It does not cover all digital rights laws or other forms of media regulation outside these acts. It also provides a well-established data for analysis being approved and enacted by the National Assembly. Such a study will hopefully yield useful information for the public, the issuing authorities, and concerned institutions. It will also address the need to handle through cybercrime laws enforcement action the emerging issues such as mischievous acts, misconduct, misbehavior, and discipline issues during online classes and seminars. The selection of PECA 2016 and PECA Ordinance, 2022 is pivotal due to their direct influence on digital communication and free speech in Pakistan. These documents represent significant shifts in legislative responses to emerging digital challenges. By focusing on these two legislations the study maintains a clear and manageable scope allowing for a detailed and balanced analysis. Given the legal and sociopolitical context of Pakistan, this delimitation ensures relevance and depth capturing the evolution of discourse on digital rights and free speech without diluting the analytical focus. This approach will provide a comprehensive understanding of how these legislative measures have shaped and redefined the boundaries of free speech in the digital era in Pakistan.

1.9. Overview of Research Methodology

Based on empirical knowledge the study utilizes the proposed frameworks of CDA and Ruth Wodak's Discourse Historical Model of CDA will be applied to it, consulting various sources to develop a better understanding of the document after

covering all the ambiguities. A rigorous and transparent document analysis will be conducted to clarify the confusion found in the document. The background of almost all Acts presented in PECA 2016 and PECA Ordinance 2022 will be explored, and its impact/effectiveness after its implication will be studied.

1.10. Division of Chapters

Chapter one will provide a detailed introduction to the topic along with the background information and circumstances that led to the creation of PECA Act (2016) and its amendments. It states the search problem. It will also include research objectives, significance and rationale of the study, and delimitation. The second chapter will critically review the related works and introduce the issues that will be foregrounded in the current study. Chapter three will reveal the theoretical framework applied to the document under study. It also explains the research methodology followed while conducting the CDA of the document under analysis. Chapter four contains the detailed analysis of the proposed research while applying theoretical framework of Critical Discourse Analysis through Ruth Wodak's model of Historical Discourse Approach. Chapter five summarizes the findings of the research work and will try to resolve the queries mentioned/asked in the research questions. Furthermore, it will give awareness to the public about the hidden intentions of the authorities that resulted in the amendment of ACT through an Ordinance in February 2022 called PECA Ordinance 2022.

CHAPTER 2

LITERATURE REVIEW

This literature review gives a summary of literature on free speech in Pakistan and on forms of regulation of online expression. It particularly focuses on the regulatory legislative frameworks related to electronic transactions and cybercrime preventions such as Electronic Transactions Ordinance (ETO) 2002, the Prevention of Electronic Crimes Act (PECA) 2016 and most recently, the PECA ordinance 2022. Nevertheless these laws have also brought up serious questions about freedom of speech, security of the nation, and social order. Using the currently existing research on this intersection of technology, speech and regulation in Pakistan, this chapter explores the main debates, themes, and gaps in existing research. This literature review looks at the theoretical and empirical literature in this area in an effort to contextualize the critical discourse analysis of the legislative documents such as PECA2016 and PECA Ordinance 2022 in the next few chapters.

This work employs Discourse Historical Approach by Ruth Wodak which has been derived from Critical Discourse Analysis (CDA). It is an interdisciplinary approach that examines how language and discourse contribute to the construction of power relations, ideologies, and social identities (Duran, 2020). It aims to uncover hidden meanings, power imbalances, and social injustices within texts and discourses. Various theoretical frameworks have been developed to guide the analysis and understanding of critical discourse. This chapter gives a detailed background of the legislative process involved in the promulgation of a legislation.

2.1. Language of Legislation

To prevent any room for interpretation, legislative language strives for absolute precision. In other words, it is important to stick to words and phrases that have already been defined in the law. The serious and authoritative character of law is reflected in the language's formality. It frequently employs cliches and a style that has been maintained throughout the years. Legal writings sometimes have difficult-to-understand language, lengthy phrases, and specialized terminology. The necessity to account for every conceivable circumstance and interpretation is what causes this level

of complexity. The use of words must be able to withstand the test of time without becoming out of date because, once passed, legislation is often in effect for a long period. Legislation, while being everlasting, must also be flexible enough to accommodate changing conditions; hence, the wording utilized must be expansive enough to incorporate new information without requiring regular revision. Lack of bias and representation of the variety of the governed society are essential components of inclusive legislation that takes into account all impacted parties. The end aim, however complicated, is for the language to be intelligible and plain for both individuals who are subject to the laws and those who interpret and enforce them. To make laws that can be enforced and understood by judges, the language of legislation is about more than simply the words employed; it's also about the structure of those words. The language strikes a good mix between being precise and clear and being flexible and adaptable.

2.2. Creating a Legal Narrative

The construction and dissemination of a legal narrative are crucial in shaping public perception and understanding of technological and socio-political phenomena. The Electronic Transactions Ordinance (ETO) 2002, Prevention of Electronic Crimes Act (PECA) 2016, and PECA Ordinance 2022 demonstrate how language and legal frameworks craft specific narratives that guide and manage societal behavior within digital spaces.

The establishment and evolution of legal narratives surrounding digital transactions and cybercrimes in Pakistan reflect the country's efforts to regulate burgeoning digital spaces while contending with global technological advancements and local socio-political challenges. ETO 2002 laid the groundwork for recognizing electronic signatures and transactions, heralding a new era of digital communication and commerce. PECA 2016, responding to growing concerns about cybercrimes, introduced more comprehensive measures to curb various forms of online misconduct. The subsequent PECA Ordinance 2022 further refined legal provisions, reflecting an ongoing commitment to enhancing digital governance.

Discursive strategies employed to construct and reinforce the legal narrative include nominalization, ambiguity and broad language, speculation and framing, argumentation, and mitigation. These narratives significantly impact free speech in

Pakistan, creating an atmosphere where free expression is constrained by a legal framework designed to prioritize security and order. The legal narrative, while addressing genuine concerns about digital crimes, also opens avenues for potential misuse, where dissenting voices may be silenced under the pretext of maintaining public morality and safety.

In conclusion, the legal narratives constructed through ETO 2002, PECA 2016, and PECA Ordinance 2022 not only articulate the state's stance on digital governance but also shape the societal understanding of permissible online behavior. By strategically employing discursive elements, these legal texts embed power dynamics and ideologies that influence public discourse, ultimately curbing free speech under the guise of legal and moral safeguarding.

The current effort will add to the existing body of knowledge by delving into the role of power and belief systems in legislative processes through the analytical lens of critical discourse analysis applying Ruth Wodak's Discourse Historical Approach on the electronic/cybercrime legislations of Pakistan; this is necessary because there has been very little research in this particular area.

2.3. Linguistic Features of Legislative Language

In constructing legislation such as ETO 2002, PECA 2016, and PECA Ordinance 2022, lexical choices i.e. the choice of vocabulary plays a crucial role in shaping legal narratives and enforcing regulatory measures. Legal texts are carefully drafted to balance precision, ambiguity, and authority, thus reflecting the socio-political context and regulatory intentions. Language of legislation is characterized by the following key features.

2.3.1. Lexical Choices in Legislations

Legislative texts often employ technical jargon and specific legal terminology to ensure precision and clarity. Terms like "electronic signature," "digital certificate," "authentication," and "data breach" are used within ETO 2002, PECA 2016, and PECA Ordinance 2022 to define legal concepts and processes. These lexical choices embed the legislation within a technical framework, positioning it as a specialized legal document requiring expert interpretation.

2.3.2. Nominalization and Abstraction

The use of nominalization, or converting actions into nouns, abstracts legal actions and reduces the visibility of agents. For instance, terms like "unauthorized access," "spreading false information," and "cyber terrorism" are prevalent in these laws. This nominalization shifts focus from individuals to generalized actions, creating a sense of universal threat that justifies regulatory intervention. By abstracting actions, the language depersonalizes the legislation, making it easier to apply broadly across varying contexts.

2.3.3. Ambiguity in Legislation

Ambiguity in legislative language allows for flexible interpretation and application. Phrases like "offensive communication," "public order," and "moral values" are deliberately broad, providing authorities with significant discretion in enforcement. This ambiguity can lead to subjective enforcement, where officials interpret and apply the law based on situational context and perceived threats. The broad terms ensure the legislation can adapt to emerging challenges without frequent amendments.

2.3.4. Persuasive and Emotive Vocabulary

The vocabulary used in these legislative texts often includes persuasive and emotive terms to garner public and political support. Words like "protection," "security," "safety," and "national interest" evoke a sense of urgency and necessity. By framing the legislation as essential for safeguarding public welfare, these terms help justify stringent measures and regulatory control. This persuasive language aims to shape public perception, presenting the law as a benevolent force against cyber threats.

2.3.5. Legal Consequences and Enforcement Lexicon:

Legislation relies on a well-defined lexicon to outline legal consequences and enforcement mechanisms. Terms such as "penalty," "imprisonment," "cognizable offense," and "prosecution" delineate the punitive aspects of the law. The inclusion of specific penalties and enforcement provisions underscores the seriousness of cybercrimes and the state's commitment to combating them.

2.3.6. Mitigative Language

Mitigative language is used to soften the perception of harsh measures and highlight the broader benefits of regulation. By emphasizing the importance of public safety, moral values, and national security, the legislation mitigates concerns about potential overreach. Phrases like "ensuring public safety" and "protecting moral values" present the legislation in a positive light, downplaying the restrictive aspects and portraying the measures as necessary for the common good.

2.3.7. Cultural and Societal References

The legislative texts often use vocabulary that reflect cultural and societal norms. Terms like "moral values," "public decency," and "religious sentiments" are tailored to resonate with the local socio-cultural context. By aligning the legislation with prevailing cultural values, these references enhance its acceptance and legitimacy within society.

The vocabulary employed in ETO 2002, PECA 2016, and PECA Ordinance 2022 is carefully crafted to reflect the regulatory intentions, balance precision with flexibility, and align with cultural norms. Through nominalization, ambiguity, persuasive language, and mitigative strategies, these legislative texts construct a legal narrative that prioritizes security and order while potentially restricting free expression. Understanding the linguistic nuances in the vocabulary of legislation is essential for a critical discourse analysis, as it reveals how language shapes and is shaped by socio-political contexts and regulatory goals.

2.4. Legislative Activism

In the framework of "Critical Discourse Analysis of ETO 2002, PECA 2016, and PECA Ordinance 2022," the concept of legislative activism emerges as a driving force that shapes and regularizes the legislative framework of a country. Legislative activism involves the proactive and deliberate creation and amendment of laws to address emerging issues and requirements of the society according to its needs. This section explores how legislative activism is manifested through these ordinances and acts and its implications for digital governance and free speech in Pakistan.

Legislative activism is characterized by the proactive development of legal frameworks that anticipate and respond to challenges resulted from technological

advancements. ETO 2002 marked the beginning of Pakistan's journey towards regulating electronic transactions, electronic signatures, and digital contracts. This legal framework, stood as pioneering tool for the government to foster a secure digital environment that would facilitate e-commerce and digital communication.

PECA 2016 exemplifies legislative activism in response to the growing threat of cybercrimes. The increasing reliance on digital platforms for communication, commerce, and social interaction necessitated robust legal measures to tackle cyber threats. PECA 2016 introduced comprehensive regulations to address issues such as online harassment, data breaches, hate speech, and cyber terrorism. This act reflects the state's commitment to maintaining digital order and protecting citizens from cyber threats. The subsequent PECA Ordinance 2022 highlights the continuous nature of legislative activism. By expanding and refining existing provisions, the ordinance addresses gaps and ambiguities within PECA 2016. It includes broader definitions of cybercrimes, enhanced penalties, and additional protections for public figures and entities. This iterative process illustrates the dynamic nature of legislative activism, ensuring that laws remain relevant in the face of evolving digital challenges.

While legislative activism aims to create a safe and secure digital environment, it also raises concerns about potential restrictions on free speech. The broad and sometimes vague terms used in these laws can be interpreted subjectively, leading to the potential misuse of legislative power. The proactive stance of legislative activism, while addressing legitimate concerns, can inadvertently create an atmosphere of caution and self-censorship among citizens.

Legislative activism involves a delicate balance between regulating harmful online activities and preserving fundamental rights such as freedom of expression. The critical discourse analysis of these legislative texts reveals how language is used to justify regulatory measures while potentially curbing dissent and critical voices. By examining the discursive strategies within these laws, this thesis seeks to uncover the underlying power dynamics and ideologies that influence legislative activism in Pakistan.

Legislative activism plays a crucial role in shaping digital governance in Pakistan. Through proactive legal frameworks, responses to emerging threats, and continuous refinement, legislative activism seeks to address the complex challenges of

the digital age. However, the impact on free speech must be critically examined to ensure that the balance between security and freedom is maintained. Understanding the linguistic features and discursive strategies within these legislative texts is essential for a comprehensive analysis of their implications.

2.5. Legislative Activism in Pakistani Context

Legislative activism refers to the strategic use of laws and the legal system to bring about social, political, or economic change. It involves advocating for new laws or changes to existing ones, as well as using the courts to challenge or enforce existing laws.

The Electronic Transactions Ordinance (ETO) is a legislative framework implemented in Pakistan in 2002 to facilitate safe electronic transactions. Also, Prevention of Electronic Crimes Act, 2016 and PECA Ordinance 2022 are laws enacted in Pakistan to regulate and govern electronic transactions and digital activities. While the purpose of these laws is to provide digital governance and prevent cybercrimes, but some critics argue that these legislations also display certain hidden ideologies such as granting extensive powers to law enforcement agencies to monitor and control online activities raising concerns about privacy and freedom of expression. PECA 2016 has been criticized for its vague definitions of offences likely to be used to silence dissenting voices and stifle political opposition. Some provisions in PECA 2016 have been interpreted as reinforcing gender stereotypes and religious biases, promoting discrimination against marginalized groups.

Hence these legislative frameworks prioritize the interests of large corporations and financial institutions over individual citizens, favoring capitalist ideologies. Such laws may be used to justify increased military and intelligence agency involvement in civilian affairs, potentially undermining democratic norms. It is important to note that these interpretations are not universally accepted and may be subject to ongoing legal and political debates.

The legislative activism has played a significant role in shaping the legal landscape in Pakistan. In the context of promulgation of legislations Electronic Transactions Ordinance 2002, Prevention of Electronic Crimes Act 2016 (PECA) and its Ordinance PECA Ordinance 2022 are the most significant moves in the legislative history of Pakistan.

Legislative activism around ETO and PECA has taken various forms, including the advocacy campaigns by civil society organizations and political parties, petitions and challenges in the courts, public protests and rallies, lobbying and negotiations with lawmakers and government officials. For example, the Pakistan Tehreek-e-Insaf (PTI) party, led by Imran Khan, used legislative activism to push for the passage of the 18th Amendment to the Constitution, which granted more autonomy to provinces and limited the power of the federal government.

Similarly, civil society organizations and human rights groups have used legislative activism to challenge the provisions of PECA, arguing that they are overly broad and could be used to suppress free speech and political dissent. Through legislative activism, individuals and groups can influence the lawmaking process, hold elected officials accountable, and shape the legal framework that governs society. Reports and statements from civil society organizations, such as the Human Rights Commission of Pakistan (HRCP) and the Pakistan Civil Society Forum (PCSF).

2.6. Right to Power Distinction

Establishing the republic's dedication to democracy and the people's sovereignty, the 1973 Pakistani Constitution enshrines the notion of the "Right to Power" within its framework. Ensuring a balance and separation of powers to prevent any one body from becoming too dominant, explains the allocation of authority across the several parts of government. The ability to rule is transferred to elected officials who are responsible to the public by the right to elect their representatives, which is granted to the people by the Constitution. Equal protection under the law, freedom of expression, and religious liberty are all cornerstones of a democratic society, and they are protected by this document as well. To further strengthen the democratic character of the country, the Constitution also establishes an independent judiciary to defend individual rights and maintain the rule of law. To ensure that the nation's governance is done with their permission and for their benefit, the Constitution of Pakistan 1973 provides forth the legal framework for the people's right to power.

It is essential to understand that the separation of powers among the three branches of government i.e. executive, legislative, and judiciary that form the foundation of a healthy democracy. According to the famous French philosopher Montesquieu, "expose the liberty of the citizens to arbitrary control" (Vile, 1998, p. 99)

if the separate functions of different state organizations are mixed up. This, in turn, would constitute a huge threat to the state's freedom

2.6.1. Power and Ideology in Critical Discourse Analysis

Language plays a crucial role in human existence through communication, information transmission, and understanding the world. Linguists have developed a deep interest in the study of language, focusing on its phonological, semantic, syntactical, and pragmatic aspects. Critical discourse analysis has emerged as a discipline that examines language about power mechanisms. The use of language is often governed by the need to advance academic theories, protect sociopolitical interests, or propagate religious ideologies. These limitations create power structures that favor certain values, norms, ideologies, beliefs, and theories.

The technique of critical discourse analysis encourages a process of reversal and discontinuity by challenging and undermining the power structures present in speech (Hook, 2007). Hook's work effectively uses Foucault's notion of discourse to investigate the internal and exterior dynamics of power, but it ignores the political environment in which discursive formation occurs. The influence of political issues on language development is not fully addressed in Hook's work because it largely takes a psychological approach.

In contrast, Frantz Fanon's concept of counter-discourse is more politically deconstructive. According to Fanon, speech is a battleground where ongoing power conflicts occur (Fanon, 1994). Fanon's analysis of French colonial discourse and his development of Algerian independence discourse show that speech challenges dominant power. Fanon argues that resisting via language creates individuals who ultimately oppose and overthrow oppressive forces. However, Fanon's method focuses on colonial subjectification.

Edward Said effectively articulates post-colonial concerns by challenging dominant Western narratives that objectify the Orient (Said, 2016). Said argues that Orientalism has imposed inferiority and subordination on Eastern people since the 1750s. In his book "Orientalism," Said explores power dynamics and speech, tracing them back to Aeschylus' "The Persians." He also recognizes Orientalism's characteristics in contemporary American social sciences. Said's method incorporates

Foucaudian and Gramscian concepts, as well as Vico's non-essentialist perspective, to deconstruct Western discourses on the Orient.

Whitaker (2005) examines political exclusion in Zambia, focusing on politicians' strategic manipulation of legal institutions to label opponents as "aliens" and strip them of their rights. She argues that this rhetoric threatens Zambia's democratic progress. However, her study neglects discourses of assimilation and co-existence, focusing solely on exclusion.

Spivak (2017) is aware of the process of "othering" subalterns, the most marginalized individuals in society. According to her, marginalized groups, especially women, have been prevented from expressing themselves in discussions of authority. The subaltern lacks verbal expression. While Spivak's examination of speech shaping subaltern subjectivity is enlightening, it is unacceptable that the subaltern cannot articulate their problems.

Ruth Wodak (2012) states that discourse is formed through historical processes, social norms, values, and hermeneutic interpretations. Although extensive study has been conducted on Orientalism from cultural, economic, and anthropological viewpoints, there has been limited work on critical discourse analysis. Therefore, the researcher will employ Wodak's critical discourse analysis methodology to examine cybercrime legislations such as PECA 2016 and PECA Ordinance 2022. As Wodak herself reveals that "this framework effectively reveals historical processes, cultural norms, and subjective interpretations that give rise to speech (Wodak, 2004).

2.7. Background to Free Speech in Pakistan

Free speech is the right to express one's opinions without fear of censorship or reprisal. It is a fundamental human right that is enshrined in many constitutions and international treaties. However, there are limits to free speech, such as the prohibition of hate speech and incitement to violence. Within the discipline of critical Discourse Analysis (CDA), the Discourse Historical Approach by Ruth Wodak can be used to analyze how free speech is both protected and restricted in society. For example, analysis of news articles about controversial speech might reveal that the article focuses on the negative aspects of the speech, such as the fact that it offended some people. This focus on the negative aspects can lead to the public viewing the speech as harmful, which can in turn lead to calls for restrictions on free speech

Article 19 of the 1973 Pakistani Constitution guarantees freedom of expression to all Pakistanis, following boundaries set within the "glory of Islam", "law and order" and "national security, Hamdani (2014) These limitations are commonly exploited. Antiblephemy laws and vote subordination have targeted religious minorities, notably (CRSS 2014). Wodak's Discourse Historical Approach can also be used to analyze the language used by people who are trying to restrict free speech. For example, a DHA of a speech by a politician who is arguing in favor of restricting hate speech might reveal that the politician uses words and phrases that delegitimize the views of those who support free speech. This delegitimization can make it more difficult for people to defend their right to free speech.

According to Siddique and Hayat (2008), General Zia's dictatorship supported state sponsored religion, which incited fanaticism. Freedom of expression includes not just speech but also religious freedom, political rights, information access, and protection against hate speech (Haque 2012). However, the current theocratic-political legislative framework does not protect these rights. Authorities routinely abuse freedom of expression exemptions for hate speech, accusing minorities and Muslims of blasphemy, and denying access to information based on national security concerns (ibid.).

Ahmed (2012) argues that with limited freedom of expression in Pakistan, there is no room for individual opinion-making, leading to a collective mindset that hinders innovation. Uddin and Tarin (2013) argue that regulations regulate free speech, but they also allow powerful offenders to go unpunished while penalizing non-violent speakers. To conclude, religious intolerance may be detrimental and cause greater disruption in society.

Blasphemy deaths often result from communities taking matters into their own hands and attacking the accused. In 2009, eight Christians were killed, 18 wounded, and two churches and 75 dwellings burned in Gojra hamlet due to accusations of desecration of the Holy Quran (Rashid 2012). Public personalities who urged improvements in the blasphemy legislation were slain, indicating the seriousness of freedom of speech violations (Suleri 2011).

The executions of Punjab Governor Salman Taseer and Federal Minister for Minority Affairs Shahbaz Bhatti are clear examples of human rights violations

(USCIRF 2011). Additionally, Hindu and Christian females regularly undergo forced conversions. About 25 Hindu females convert to Islam monthly, according to estimates (ibid.). While attempts are underway to prevent forced conversions, the Sindh Assembly overwhelmingly enacted a measure banning forced marriages (Ahmed 2014).

Chaudary (2014) argues that unrestricted freedom of expression might cause confusion and anarchy, making it not desirable. Limitations and constraints are necessary to prevent misuse of freedom of speech for provocation, false statements, obscenity, and hate speech.

While Pakistani journalists are allowed to criticize the government, they suffer persecution from the military, intelligence services, politics, and courts (Naveed 2013). The Freedom Network (2015) said that 2014 was the deadliest year for media and journalists in Pakistan, with 14 journalists, media assistants, and a blogger slain. Last year's death of prominent human rights activist Sabeen Mehmud highlights the rise of extremist ideology and the decreasing political debate (Lisa Curtis, Enos 2015).

Imam (2012) argues that while Articles 19 and 19A of the Pakistani Constitution provide freedom of expression and information, there is no regulation governing online content publication and access. The author analyzes the Acts and Ordinances of the Pakistan Telecommunications Authority (PTA) regarding internet information. The author also examined the response of the Pakistani government to blasphemous content, namely the YouTube ban. As blasphemous and improper information on the internet cannot be prevented, shutting down entire websites is not an effective approach. To address these challenges, options include prosecuting content authors, ignoring online speech, or developing screening technologies.

As of 2015, the Pakistan Electronic Media Regulatory Authority (PEMRA) has established a code of conduct that limits media comments on specific issues during live broadcasts (CPJ, 2015). Topics often include security operations, hostage situations, terrorist attacks, and religious hate speech. Regulators say they defend national security.

Hamid Mir, a Pakistani journalist who survived a 2014 terrorist attack, stated in an interview with Dietz (2015) that the news channel lost its independence after the attack. He stated that the channel has been restricted from discussing human rights

violations in certain areas of Pakistan and prohibited from criticizing former generals' political roles.

Despite criticism of media and free speech, Nizamani (2014) asserts that the media portrays reality, contrary to popular belief. The author claims that the occurrences covered by the media were real and not fictional. The public fears being targeted by terrorists, political parties, or the military for expressing political, religious, or human rights opinions. The author finds that fear has led to intellectual corruption, moral apathy, and religious bigotry in the Pakistani community. According to him, intellectual development in society requires the ability to communicate one's thoughts without fear or harm.

The latest Cybercrime Bill (Prevention of Electronic Crimes Act, 2016) enacted by the National Assembly and Senate raises concerns about freedom of expression in Pakistan, as it contradicts the constitutional right to free speech. Section 31 of the bill is controversial as it allows the government to remove or block access to intelligence sources for national security, friendly relations, public order, decency, morality, or contempt of court.

The measure allows for internet limitations, including blocking content on newspapers, online media, and social media based on objections (Latif 2015). Critics call the measure "draconian" for limiting civil freedoms and focusing on morality rather than cybercrime (Haider 2015).

Baloch (2016) argues that this measure will hinder free speech and opinion online. He suggests redrafting the bill to target offences without criminalizing expression or essential rights to avoid this predicament.

The Constitution of Pakistan guarantees freedom of expression with certain restrictions related to religious respect, public order, and national security. However, these restrictions have often been exploited to discriminate against minorities, particularly through voting laws and blasphemy legislation. The obstacles faced by Pakistani people concerning free speech are immense for instance the era of General Zia saw a rise in extremism, fueled by state-endorsed religion. Freedom of expression encompasses various rights, including political participation and access to information, but these are not ensured in the present scenario. Authorities and religious leaders have

misused speech limitations to perpetuate hate speech, levy false blasphemy charges and restrict information flow.

The suppression of free speech has led to mob violence and blasphemy-related murders, such as the Gujrawala city incident in 2009 where Christians were killed over alleged charge of desecration of the Holy Quran. Calls for blasphemy law reforms have resulted in high-profile assassinations, highlighting severe human rights violations. Also, forced religious conversions particularly of Hindu women, are frequent, though legislation against forced marriages and conversions has been introduced.

Critics also argue that unchecked free speech can lead to chaos, hence the need for regulation to prevent misuse. Despite the nominal freedom for journalists to critique the government, media censorship is prevalent, with 2014 being the deadliest year for Pakistani journalists. The murder of social activist Sabeen Mahmud exemplifies the dangers faced by those challenging extremist ideologies and the narrowing space for political dialogue.

Khan & Moslemzadeh (2019), in their article, explore the scenario of post-speech freedom. Qualitative research methodology has been applied to the case study, demonstrating that certain parts of PECA (2016. .1) are not enough to protect the individuals' right to freedom of speech. This research has suggested that it amend its certain acts for the public's welfare.

Sharif (2019), in his article, refers to issues regarding freedom of expression. He explores the authenticity of the claims concerning freedom of speech in Pakistan. He also aims to determine whether the freedom of speech will be helpful in the progress of law enforcement and promising good governance in society. Referring to Article#19 of the constitution of Pakistan, he points out that it provides freedom of speech and some restrictions based on Islamic ideology. He says that the right of freedom of speech seems inapplicable in the true sense of the current political as well as legislative circumstances.

The works mentioned above are related to my topic but are different in that they relate to the CDA of texts and spoken or written discourses and methodologies. The other reviews of articles are associated with PECA (2016) or freedom of speech, providing insight into the emerging cybercrimes and the status of freedom of speech in Pakistan.

The intricate connection between free speech and power can be better understood with the help of DHA. It may be utilized to bring attention to the limitations on free speech, question the media's portrayal of free speech, and push for legislation that safeguards free speech. One approach to researching free speech using DHA is to examine the media's portrayal of the topic, the terminology used in legal and political arguments, and the social and cultural elements that impact free speech. Create innovative strategies to safeguard free expression and fight for legislation that upholds this value.

When it comes to defending this basic human right free speech DHA is an invaluable tool for delving into the complexities of the topic. Finally, DHA is a potent instrument for knowing how society, power, and language interact with one another. Many social phenomena, including free speech, may be studied using it. The goal of DHA is to provide light on the construction and maintenance of power relations, as well as their potential for challenge and transformation, through a critical examination of language usage.

2.8. Critical Discourse Analysis of Social Media Discourse

Media discourse has significant impact on power dynamics. The systematic production of topics and facts through media sustains certain interests. It shapes people's perceptions and understanding of the world, influencing their actions. Its subjectification of the public leads to the "manufacture of consent" (Bennet, Herman, & Chomsky, 1989). However, this examination focuses primarily on American perspectives, neglecting influential media discourses in non-American contexts.

Language exerts its standards and principles on individuals' volition, suggesting cognitive liberty. However, this process can be "dehumanizing" (Kattakayam, 2006). Power discourse plays a crucial role in shaping global governance and individual self-perception. The state's discourse, particularly in dominant states, shapes policies and contributes to desirable global arrangements. Chomsky (1992) argues that "the American elite strategically used rhetoric to develop a new global system based on Western virtue and Communist malevolence".

Social Media theory is a framework that has been integrated into critical discourse analysis to examine how social media platforms shape and influence discourse. Social media is seen as a powerful tool in disseminating and shaping

discourses, with the potential to either challenge dominant ideologies or reinforce existing power structures. Moreover, Political Discourse theory is another theoretical framework that informs critical discourse analysis (Chiluwa, 2012). This framework focuses on the analysis of political discourse, including political speeches, policy documents, and media representations. In this context, critical discourse analysis aims to uncover the underlying power dynamics, ideologies, and social realities that are reflected in political discourse. In summary, critical discourse analysis draws on multiple theoretical frameworks, including Critical Linguistics, Power theory, Political Identity theory, Social Media theory, and Political Discourse theory. These frameworks help researchers analyze and understand the complex relationship between language, power, politics, and social identities within discourses (Sajjad et al., 2017).

2.9. Review of Works Done by Application of DHA (Ruth Wodak)

Ruth Wodak's Discourse-Historical Approach (DHA) has been influential in showing how discourse constructs socio-political contexts and vice versa. This method integrates historical, socio-political, and linguistic considerations to analyze the multifaceted nature of discourse within various domains. This section reviews key works that have applied the Discourse Historical Approach to explore the relationship between language, power, and ideology across different contexts. This approach is distinguished by its focus on three primary dimensions of discourse critique: text or discourse-immunity critique, socio-diagnostic critique, and future-related perspective critique. The former identifies inconsistencies and contradictions in texts, while the latter critiques persuasive and manipulative discursive practices using social theories and contextual knowledge.

2.9.1. Major Applications of DHA in Research

Ruth Wodak's analysis of political discourse is one of the most prominent areas in which DHA has been employed. In "The Politics of Fear," Wodak (2015) examines the discursive strategies used by right-wing populist parties to construct fear and exacerbate social divides. Her analysis illuminates how metaphors, slogans, and narratives are used to construct 'us versus. them' dichotomies, reinforcing power dynamics and xenophobic ideologies.

A significant body of work has utilized DHA to explore media representations of migration. Baker et al. (2008) combined DHA with corpus linguistics to analyze UK

press portrayals of refugees and asylum seekers. They uncovered how language perpetuated xenophobic ideologies and influenced public perception. Similarly, Khosravinik (2010) used DHA to examine the portrayal of immigrants in British newspapers, highlighting how discourse strategies marginalize and stigmatize immigrant communities.

Koteyko, Nerlich, and Crawford (2008) applied DHA to analyze climate change discourse in the British press. Their findings revealed how specific linguistic choices reflected and reinforced particular ideological stances. They showed how metaphors and frames within climate change narratives could shape public understanding and policy preferences.

Reisigl and Wodak's (2001) analysis of Austrian healthcare policy discourse demonstrates DHA's application in understanding policy-making processes. They elucidated how language strategies in policy documents and speeches construct notions of 'acceptable' and 'non-acceptable' behavior, influencing public attitudes and practices.

Weiss and Wodak (2005) applied DHA to the discourses of education reforms in Austria. Their analysis highlighted how educational policies and curricula are influenced by broader socio-political ideologies, constructing and legitimizing certain identities while marginalizing others.

The application of DHA has consistently uncovered the interplay between language, power, and ideology. By analyzing how discourse constructs social realities, researchers have revealed how power dynamics are embedded in everyday language. Wodak's model has been used to study the language used by politicians in a variety of contexts, such as election campaigns, parliamentary debates, and press conferences. This research has shown how politicians use language to construct and maintain power relations, promote their agendas, and silence their opponents.

Van Dijk's (2008) work on discourse and power complements Wodak's approach by examining how elite discourses shape public opinion and reinforce structural inequalities. This intersection of DHA with critical discourse analysis highlights the role of language in legitimizing and sustaining power structures.

Ameer Ali (2020), in his research article titled "A Critical Discourse Analysis of An Essay Employing Ruth Wodak's Model on Bernard Lewis' Essay: The Roots of

Muslim Rage by employing Wodak's Model of Discourse Historical Approach. The research findings have revealed critically that discourse is a hermeneutic process that can either be plausible or implausible. The social norms, values, relations, ideologies, and historical processes impact the production of discourse. Similarly, Lewis has Orientalized the Muslims through hermeneutic interpretations. Moreover, this research is a human effort that is open to faults and defects, therefore, it makes no claims of perfection. Besides, this research has its gaps and faults that might be improved through further criticism. Furthermore, this research work will be a helpful tool for scholars of critical discourse analysis and students who want to understand critically the power mechanisms of truth-making processes through discourse.

These are just a few examples of the many ways in which Ruth Wodak's model has been applied. The model is a powerful tool for understanding the relationship between language, power, and society. It can be used to study a wide variety of social phenomena, from political discourse to everyday interactions.

2.10. Research Gap

Power discourses exhibit significant bias, generating specific subjectivities, interests, behaviours, global arrangements, and social truths. Questioning their assertions is crucial for individuals to comprehend the mechanisms of speech that construct realities. The objective of this research is to analyze the legislations using Wodak's Critical Discourse Analysis (CDA) framework to re(evaluate) free speech in Pakistan.

Similarly, this research attempt will also contribute to the field of critical discourse analysis. The research assignment also deconstructs the policymaking process by exposing the interest-oriented mechanisms of power. (This research employs Ruth Wodak's theoretical model to analyze a legal document that is not only related to one area of society but has a profound impact on the whole of it. Moreover, as far as PECA (2016) and PECA Ordinance (2022), are concerned, not much literature is available on them. The minimal work related to these Acts is more related to their analysis concerning their impact on society after implementation will be used to reveal the opaque relationships of power and hegemony as they are embedded in the discourse. Furthermore, the implication of freedom of speech will be possible only if the amendment in PECA 2016 via PECA, Ordinance 2022 will be drawn. The extensive application of DHA in various fields demonstrates its versatility and depth in analyzing

discourses. Future research can further explore how digital and social media platforms are reshaping discursive practices and power relations. Understanding these dynamics is crucial for addressing contemporary challenges related to misinformation, digital surveillance, and the construction of public opinion.

Ruth Wodak's DHA provides a powerful analytical framework for uncovering the intricate relationships between language, power, and ideology. The reviewed works illustrate DHA's effectiveness in dissecting political, media, environmental, healthcare, and educational discourses, shedding light on how language both reflects and shapes socio-political realities. Ongoing and future research will continue to benefit from applying DHA, offering nuanced insights into the evolving landscape of discourse in diverse contexts.

CHAPTER 3

RESEARCH METHODOLOGY

This chapter presents the methodology for conducting a critical discourse analysis (CDA) of the Prevention of Electronic Crimes Act (PECA) 2016, and the PECA Ordinance 2022. Based on the Discourse Historical Approach (DHA) offered by Ruth Wodak, this study chooses to investigate the linguistic and discursive approach employed in regulatory documents to construct and regulate online free speech in Pakistan. This research seeks to offer a nuanced understanding of the power dynamics, social implications, and the ideological underpinnings of these regulatory frameworks through triangulation of qualitative content analysis with historical contextualization. This chapter overviews the methodological approach, the choice of data, and the analytical steps employed to critically analyze representations of free speech in Pakistan's online environment.

3.1 Research Design

The research employs a qualitative approach using the Discourse Historical Approach (DHA) by Ruth Wodak to examine the discourse surrounding the Prevention of Electronic Crimes Act (PECA) 2016, and its amendment PECA Ordinance 2022. The use of Ruth Wodak's Discourse-Historical Approach (DHA), emphasizes the importance of historical, social, and political contexts in understanding discourse. The qualitative design is suitable for this research as it allows for an in-depth exploration of the complex and nuanced ways in which legislative texts shape and are shaped by socio-political contexts. By focusing on the discourse surrounding these laws, the study aims to uncover the underlying power dynamics and ideologies that influence their implementation and impact on free speech.

In DHA, qualitative research involves a detailed examination of the legal document's language, structure, and content to identify key concepts, relationships, and contextual factors. It involves an in-depth analysis of the legal document, considering the historical, social, and cultural context in which the document was created. The analysis also includes non-numerical data, such as the language, tone, and structure of the document. The interpretive approach of the researcher helps identify meanings,

relationships, and patterns that may not be immediately apparent. The benefits of qualitative research in DHA include rich insights, contextual relevance, and in-depth understanding. By employing qualitative research methodologies in DHA, researchers gain a deeper understanding of the legal document and its context, providing valuable insights into the historical, social, and cultural significance of the document.

The research also intends to explore the notions of power and ideology in PECA 2016 and its amendment PECA Ordinance 2022. It re-evaluates its implication in freedom of speech to individuals in Pakistan. Moreover, when CDA is applied to a text/document, it intervenes in the favour of oppressed groups and highlighting the hidden addenda of the dominating groups, thus showing strong support for the oppressed. It is also a very effective tool for evaluating the validity of the text/document by collecting information from different authentic sources.

3.2. Research Data

The main objective of using this methodology is to apply a framework of CDA to analyze the original texts of the cybercrimes legislations of Pakistan i.e. , PECA 2016 and PECA Ordinance 2022. To conduct CDA of the documents mentioned above, the primary data source is the original legal documents. The cybercrime legislation under analysis is the original text of PECA 2016 comprised of 29 pages, with seven chapters and 55 acts mostly subdivided into further acts. And lastly, the actual legislative document of cybercrime i.e. PECA Ordinance 2022(Amendment in PECA 2016) will also be analyzed under the same framework.

It has four pages with seven main amendment points and multiple sub-points. The analysis of the legislation mentioned in the documents under study will be carried out under the DHA framework to foreground the hidden agenda of stifling freedom of expression.

3.3. Rationale for Selection of Data

The data for this study consists of the major cybercrime laws of Pakistan, namely the Prevention of Electronic Crimes Act (PECA) 2016 and the PECA Ordinance 2022. These laws were selected for analysis because they represent the primary legislative framework governing cybercrimes in Pakistan. The rationale behind the selection of these laws for analysis is to provide an authentic examination of the linguistic devices used to construe power and ideology in legal narratives related to

cybercrime. The legislative framework is a critical component of a country's cyber governance, as it reflects the government's priorities, values, and policies regarding online activities.

The analysis of these laws through linguistic devices is essential to uncover the ways in which power and ideology are constructed, negotiated, and reinforced through legal discourse. By examining the language and narratives employed in these laws, this study aims to reveal the underlying assumptions, biases, and interests that shape Pakistan's cybercrime legislation. The selection of these three laws allows for a comprehensive analysis of the evolution of cybercrime legislation in Pakistan, from the early days of e-commerce regulation to the current era of social media and online activism. By analyzing the linguistic devices used in these laws, this research seeks to contribute to a deeper understanding of the complex relationships between language, power, and ideology in the context of Pakistan's cyber governance.

Through this analysis, this study aims to shed light on the ways in which the legislative framework reflects and reinforces existing power structures, and how it shapes the country's cybercrime policies and online environment. By examining the linguistic devices used in these laws, this research seeks to provide insights into the ideological underpinnings of Pakistan's cybercrime legislation and its implications for online freedom, privacy, and security. The data analysis using the approach of DHA provides an authentic analysis through linguistic devices which are used to construe power and ideology narrative in the document of free speech. The selected data brings to light how these documents blur the right of freedom of speech.

3.4. Delimitation of Data

This study uses Ruth Wodak's Discourse-Historical Approach to critically analyze three key Pakistani legislative documents: the Prevention of Electronic Crimes Act (PECA) 2016 and the PECA Amendment 2022. The focus of the current study is on the direct influence of these laws on digital communication and free speech in Pakistan, as they represent significant shifts in legislative responses to emerging digital challenges. The study maintains a clear scope, allowing for a detailed and nuanced analysis, while capturing the evolution of discourse on digital rights and free speech. This approach provides a comprehensive understanding of how these legislative measures have shaped and redefined free speech boundaries in the digital era.

3.5. Epistemology

This research is based on a critical realist epistemology, which relates that knowledge is socially constructed and power relations shape reality with social structures. It assumes that the three cybercrime laws of Pakistan are not neutral or objective legislations but are legislations that assume the social, cultural, and historical context from which they are created. These are considered expressions of power dynamics and interests of powerful groups in society and representatives of existing social structures and relationships. Using critical discourse analysis, the research will analyze the language and the narratives employed in the legislation and seek to explore how they construct and (re)produce specific meanings and interpretations, which in turn act on, and are influenced by, the social and cultural environment within which they find themselves. Power knowledge relationship, social constructionism, and critical realism are three key epistemological concepts.

It will be a critical reflexive research that will contextualize the laws within the social, cultural, and historical context in which the laws were made and use critical discourse analysis to analyze the language and narratives used in the laws. This thesis seeks to provide a nuanced and critically informed reading of three cybercrime laws of Pakistan by acknowledging the power knowledge relationship and the social construction of reality.

3.6. Theoretical Framework

A critical discourse analyst has to explore society's most challenging issues, following a theoretical framework. For instance, social inequality, freedom of speech, racial discrimination, violation of human rights, social abuse, misuse of power and relation, ideology building, and all the social issues are characterized under a vast umbrella. This thesis traces the mutually constitutive relationship of lawmaking and power dynamics with free speech in the digital governance of Pakistan. To critically analyze legislative texts, it uses Ruth Wodak's Discourse Historical Approach (DHA) that studies how discourse builds social realities by combining linguistic analysis with a historical and socio political context.

Various strategies of DHA are applied in the legislative texts such as nominalization, referential, perspectivation, argumentative, framing, and mitigation. By the application of the aforementioned DHA approach this thesis offers an

overarching view to examine the inter-relatedness between the use of discourse under legislative language, power dynamics and free speech principles regarding digital governance in Pakistan.

The use of the framework of DHA also acts in the best interests of their users, to protect their free speech rights, with loyalty that requires an information fiduciary to prioritize users' interests over its own above all else. This work analyzes the way these laws affect the activities of information fiduciaries in Pakistan, the degree to which they protect or constrain free speech rights of users and the effect of these laws on the duty of information providers.

3.7. Discourse Historical Approach (DHA)

In order to explore the notion of power and ideology in legal documents and intersubjective positioning in relation to building authority the selected corpus or data (cybercrime legislations) is analyzed through some strategies and a framework. Since the legal discourse is concerned with the inter-connectedness of texts and interpreted through history so is known to have developed through history. Therefore, this is pertinent to apply Wodaks (2009) Discourse Historical Approach (DHA) for analyzing power and authority in cybercrime legislation (Levels of analysis are discussed below). The data is analyzed at syntactical and lexical level in order to realize the presence of power and ideology, for example the use of metaphors, metonyms, juxta positioning of texts the use of modal verbs, material verbs, deictic expressions. Therefore, it makes an attempt to describe the legal documents through different linguistic levels, Reisigl & Wodak (2009) argues that language is used by the powerful to maintain domination (p. 87). The cited model is described below in terms of table after briefly describing discourse historical Approach DHA by Ruth Wodak.

3.8. Ruth Wodak and Discourse Historical Approach

Discourse Historical Model (Wodak, 2009) DHA, attempts to describe the narratives developed through history and based on bringing together the textual and contextual levels of analysis. The DHA is a three-dimensional approach; firstly, having identified the specific contents or topics of a specific discourse. Secondly, discursive strategies are investigated and then, linguistic means and the particular context-dependent linguistic realizations are examined. DHA includes levels of context which are elaborated in digressive approaches. According to Wodak and Reisigl (2015) it

generally means a more or less intentional plan of practices (including discursive practices) adopted to achieve a specific social, political, psychological, or linguistic goal. Discursive strategies are located at different levels of linguistic organization and complexity. Wodak and Meyer (2009: 133) presented the model of context used in this approach invokes historical knowledge understood in terms of layers:

3.8.1. The Linguistic Co-text

The linguistic co-text is the immediate text of the communicative event in question, for example in a detailed legal transcript, for Federal Government, the word federal is used to define the type of government civil party, where the word civil is used to co-text party to make the concept of party clear.

3.8.2. Ruth Wodak's Discursive Strategies:

The broader socio-political and historical context in which discursive practices are embedded and related to knowledge derived from ethnography of the relationships, and aspects of the broader social and cultural macro-environment that influence the legislative process. The DHA considers inter-textual and inter-discursive relationships between texts, genres, and discourses, as well as extra-linguistic social/sociological variables, the history of an organization or institution, and situational frames. While focusing on all aspects aforementioned, the study aims to investigate the aspect of discourses, genres, and texts influenced by the Socio-political variations. Intertextuality refers to words and narrations in a manuscript that are interrelated with the other statements embedded with the touch of past and present. These patterns are established in various forms either through overt orientations related to phenomena or through incidents of similar origins, by the use of explicit transitions within the text, or through the establishment of insinuation.

Inter-discursivity highlights the texts' interrelationships and associations with each other in numerous ways. By the conception of digressive notion as a basic related headline, this interprets that text established on legal narratives often relates to themes or sub-themes of multi-faceted dimensions of Power and Ideology. Discourse by its nature is cross-breed and vast, with the inclusion of innovative premises regarding the Field of action. Girth (1996) indicates a segment of social reality that constitutes the frame of a discourse. Various aspects of motions are elaborated by numerous actions of digressive procedure such as in the backdrop of political outset, differentiation political

activities are categorized in subsets. The offset of a discursive argument transits from the groundings of one pitch to another. Thus, it can be claimed that discourses are widespread from one field of study to another and sometimes result from overlapping of both.

To practically perform the above-stated parameters, DHA has further produced a series of analytical and descriptive tools (discursive strategies) to identify ideological positioning in a text as follows:

3.8.2.1. Referential Strategy or Strategy of Nomination

It is the construction of in and out-group and labeling of the social actors where the linguistic devices of interest are membership categorization, metaphors, metonymies, and synecdoches). For example: The regular nomination of metaphors, synecdoches categorization like, IP address refers to an online person, personifying nonhuman objects like computers etc.

3.8.2.2. Strategy of Predication

It is the labeling of social actors that appear in stereotypical, evaluative attributions of positive or negative traits and implicit or explicit predicates). For example: the use of words like secure, authentic, efficient, unlawful, fraudulent, etc.

3.8.2.3. Strategy of Argumentation

It is the justification of positive or negative attributions reflected in certain *topoi* used to justify in the form of argumentation schema. For example Topos of threat, Topos of burdening, Topos of authority, Topos of urgency

3.8.2.4. Strategy of Perspectivation, Framing and Discourse Representation

Perspectivation is the process of presenting a particular viewpoint as the dominant one, such as the government's perspective on cybercrime in PECA 2016. Framing highlights certain aspects of an issue while downplaying others, like online content's potential harm to public morality (PECA 2016). Discourse presentation is the way language is used to represent different voices and perspectives, such as the government's authority in implementing laws, potentially silencing or marginalizing the voices of other stakeholders.

3.8.2.5. Strategies of Intensification and Mitigation

The use of Intensification strategy emphasizes the seriousness and growing threat of cybercrime, justifying stricter laws. Whereas, mitigation strategy downplays

the impact of content blocking, creating a sense of measured approach. For example, PECA 2016 aims to shape public opinion and perception of the law by using intensification and mitigation strategies the law states that authorities may only block online content that is clearly in violation of the Act. These strategies aim to emphasize the importance of strict regulation while downplaying concerns about censorship and freedom of expression.

These discursive strategies along with their discourse objectives and linguistic devices are presented below in Table 1.

Table 1: A Selection of Discursive Strategies as Adapted from Reseigil and Wodak (2009: 104)

Strategy	Objectives	Devices
referential/ nomination	discursive construction of social actors, objects/phenomena/events, and processes/actions	Membership categorization devices, deictics, tropes such as metaphors, metonymies and synecdoches. verbs and nouns used to denote processes and actions
Predication	discursive qualification of social actors, objects, phenomena/events/processes, and actions (more or less positively or negatively) explicit predicates or predicative nouns/adjectives/ pronouns collocations	stereotypical, evaluative attributions of negative or positive traits (e.g., in the form of adjectives, appositions, prepositional phrases, relative clauses, conjunctive clauses, infinitive clauses and participial clauses or groups)
Argumentation	justification and questioning of claims of truth and normative rightness	• explicit comparisons, similes, metaphors and other rhetorical figures (including metonymies, hyperboles, litotes, euphemisms) allusions, evocations, and presuppositions/ implicatures • other • topoi (formal or more content- related) fallacies
Perspectivization	positioning speakers or writers point of view and expressing involvement or distance	• deictics • direct, indirect or free indirect speech • quotation marks, discourse markers/particles □ metaphors • animating prosody • other

Intensification and mitigation	Modifying (intensifying or mitigating) the illocutionary force and thus the epistemic or deontic status of utterances	• diminutives or augmentatives • (modal) particles, tag questions, use of the subjunctive, hesitations, vague expressions, etc. • hyperboles, litotes, • indirect speech acts (e.g., question instead of assertion) • verbs of saying, feeling, thinking other
---------------------------------------	---	--

3.9. Ethical Consideration

Using Ruth Wodak's DHA model this thesis conducts a detailed analysis of PECA 2016 and PECA Ordinance 2022 to highlight important ethical considerations. The research is about examining sensitive, and possibly controversial, topics like censorship, free speech, and online regulation. To ensure ethical integrity, the study adheres to the following principles: The four ethical principles (1) anonymity and confidentiality of sources, (2) accurate representation of data, (3) avoidance of harm or offense to individuals or groups, and (4) transparency in methodology and findings.

However, the researcher recognizes the possibility of power dynamics within the analysis of legal discourse, and aims to project a critical and nuanced approach. The findings and recommendations of the study are intended to serve in the public interest and to stimulate informed discussion on the regulation of online speech in Pakistan, while discouraging any particular ideology or agenda. The data is publicly available, therefore informed consent is not required.

CHAPTER 4

DATA PRESENTATION, ANALYSIS AND DISCUSSION

This chapter aims to conduct a Critical Discourse Analysis of Cybercrimes legislations such as the Prevention of Electronic Crimes Act, PECA 2016 and PECA Ordinance 2022, applying Ruth Wodak's Discourse Historical Approach (DHA). Discourse is inherently a hermeneutic process, subject to neither absolute correctness nor error, but rather shaped by historical contexts, power dynamics, societal norms, and prevailing ideologies (Wodak, 2004). Unveiling these layers of interpretation serves the public interest by revealing underlying biases and misrepresentations. In the context of Pakistan, the freedom of speech warrants a critical re-evaluation through the Discourse Historical Approach (DHA). The analysis of the present research employs Ruth Wodak's DHA to the Electronic Transactions Ordinance 2002(ETO), the Prevention of Electronic Crimes Act 2016(PECA), and the subsequent PECA Amendment i.e. PECA Ordinance 2022 to scrutinize the challenges, distortions and narratives that have influenced these legal frameworks. By doing so, the study aims to dismantle the flawed hermeneutics that has previously shaped the discourse on freedom of speech within the nation.

4.1 Analysis of Pakistan Electronic Cybercrimes Act (PECA) 2016

The Pakistan Electronic Cybercrimes Act (PECA) enacted in 2016 addresses Pakistan's growing issue of cybercrimes through comprehensive legislation.⁵ It aims to control escalating offenses in the digital realm and properly regulate acts concerning information systems. As J. Balkin's theory of Information Fiduciaries (2016) also suggest that online platforms have a fiduciary duty to protect the right of its users to free speech, privacy and security in a similar way, PECA's objectives center around combating electronic crimes through investigation, prosecution and trials of such infractions. It covers a wide-range of offenses that include unauthorized access to computer networks, digital fraudulence, cyberbullying, online harassment and more. Key provisions outline explicit transgressions and correlating punishments, notably those involving critical infrastructure such as information technology systems, cyber terrorism, hateful speech, child pornography and cyberstalking. The Act moreover establishes an investigatory body, defines procedural powers for inquiries and ensures

victim and witness security. It addresses preservation and acquisition of data, search warrants and handling confiscated digital material or networks. International cooperation in addressing electronic crimes is emphasized by PECA, recognizing crimes in cyberspace ignore geographical boundaries. In summary, the Prevention of Electronic Crimes Act plays a pivotal role in safeguarding Pakistan's virtual landscape and promoting cyber safety by furnishing a lawful framework to tackle cyber threats and shield individuals.

It is important to analyze the Prevention of Electronic Crimes Act, 2016 (PECA) through Ruth Wodak's Discourse-Historical Approach (DHA) as it will help discover the underlying meanings and the kind of power agenda that lies within the law. With the application of DHA, the linguistic options in the text, ideas and social practices that are instantiated within it will be foregrounded as more than just manageable features. In this way, the language used by PECA is scripted and scripting, which highlights the relationship between language and broader contexts.

4.1.1. Linguistic Co-Text in PECA (2016)

The Prevention of Electronic Crimes Act, 2016 (PECA) is a legal framework shaped by linguistic co-texts. It provides specific definitions of electronic crimes, criminalizes certain offenses, and prescribes penalties. The Act also establishes an investigation body and outlines procedural powers, emphasizing global cooperation in combating cybercrimes. The linguistic co-text also covers prosecution, trial, appeal, compensation, victim assistance, and expert opinions. The Act's lexical co-context includes related laws, administering powers, and Parliament requirements. This semantic guidance ensures successful enforcement and interpretation, impacting legal processing, scholarly research, and policy-making. The words acting as co-text to the main word in PECA (2016) are explained in the table given below:

Table 2: Linguistic Choices in PECA (2016) and Description of its Co-Text

(Reproduced exactly as mentioned in the text of PECA 2016)

S.No	Words	Description
(i)	"act":	means : a series of actions or inactions that violate this Act's provisions; or the act of causing another person to do an act, whether directly or through an automated system, mechanism, self-executing, adaptive, or autonomous device, and whether the effect is temporary or permanent;
(ii)	"obtaining access to data":	Implies being able to use, copy, alter, or erase any data stored in or produced by any device or information system.
(iii)	Access to an information system:	Refers to the act of obtaining control or the capacity to utilize any portion or whole of an information system, regardless of whether it involves violating any security measure.
(iv)	The term "Authority":	Refers to the Pakistan Telecommunication Authority, which was formed in 1996 under the Pakistan Telecommunication (Re-organization) Act.
(v)	The term "authorization":	refers to a legal declaration or the signature of an authorized official: - Subject to the following: for this Act, access to or transmission of any information system or data that is openly accessible by the general public must be considered approved
(vi)	"Authorized officer"	refers to an officer of the investigating agency who has been granted the authority to carry out any task on behalf of the agency as outlined in this Act;
(vii)	"Code"	refers to the Criminal Procedure Code of 1898 (Act V of 1898)
(viii)	"Content data"	Encompasses any representation of fact, information, or idea meant to be processed in an information system, including source code or programs that may be used to drive the operation of an information system.
(ix)	The "Court"	refers to the courts that have been appointed under this Act;
(x)	"Critical infrastructure"	refers to essential infrastructure components such as assets, facilities, systems, networks, or processes that, if lost or compromised, could have:

		a) Major negative effect on essential services (including those services whose integrity, if compromised, could cause significant loss of life or casualties, considering significant economic or social impacts) or on national security, defense, or the state's ability to function. b) The government has the authority to designate any infrastructure, whether public or private, as critical infrastructure in accordance with the goals of subparagraphs and above, as necessary under this Act.
(xi)	"Critical infrastructure information system or data"	Refers to any data, software, or system that assists an essential infrastructure in its operations;
(xii)	"Damage to an information system"	Refers to any unlawful alteration to the regular operation of an information system that hinders its performance, accessibility, output, or relocation, whether ongoing or one-time and regardless of whether the system itself is altered:
(xiii)	"Data"	Includes both content and traffic data.
(xiv)	"Data damage"	Refers to the destruction, corruption, modification, relocation, suppression, or temporary or permanent inaccessibility of data.
(xv)	"Device"	The definition of "device" here refers to : a tangible object or item; (c) a digital or non-physical tool; data, whether digital or otherwise, that allows access to an entire or partial information system; or automated, self-executing, adaptive, or autonomous devices, programs, or databases;
(xvi)	"Dishonest intention"	(d) refers to the purpose to injure, wrongfully gain, or harm any person, or to promote hate or violence;
(xvii)	"Electronic"	(e) encompasses a wide range of technologies, including but not limited to electronics, computers, networks, photonics, biometrics, electrochemistry, wireless, and electromagnetic fields;
(xviii)	"Identity information"	(f) describes data that may be used to authorize or identify a person or an information system, allowing them to access any data or system;

(xix)	"information"	(g) includes words, phrases, numbers, audio, video, databases, computer programs, codes (both object and source code), and any kind of intelligence as defined by the Pakistan Telecommunication (Reorganization) Act, 1996 (XVII of 1996).
(xx)	"information system"	(h) refers to an electronic platform that may produce, encode, transmit, receive, store, replicate, display, record, or process data;
(xxi)	"Integrity"	(i) refers to the state of an electronic document, signature, or advanced electronic signature that has not been changed, altered, or tampered with since a certain point in time:
(xxii)	"Interference with information system or data"	(j) encompasses any kind of unlawful activity that may disrupt the regular operation or format of an information system or data, whether or not it actually damages the system or data;
(xxiii)	"investigation agency"	(k) is defined as the law enforcement agency appointed by the Office of the Chief Executive Officer in accordance with this Act.
(xxiv)	"offence"	(l) refers to any crime punishable under this Act, with the exception of those committed by persons under the age of ten or by those between the ages of ten and fourteen who lack the mental capacity to comprehend the gravity of the situation or the potential outcomes of their actions.
(xxv)	"minor"	(m) means any individual who has not yet turned eighteen, regardless of any other laws that may be in place.
(xxvi)	"rules"	(n) refer to regulations promulgated under this Act;
(xxvii)	"Seizing"	(o) Making and keeping a copy of data or taking control of an information system or data also constitutes "seizing";
(xxviii)	"service provider"	(a) A "service provider" is defined as an individual who does one or more of the following: (b) provides services related to the transmission, reception, storage, processing, or distribution of electronic communications or other services related to electronic communications through an information system; (c) owns, possesses, operates, manages, or controls a public switched network or telecommunication services; or

		(d) Processes or stores data on behalf of customers or electronic communication service providers.
(xxix)	"Subscriber information"	(e) refers to any data on a subscriber that a service provider stores, except traffic data;
(xxx)	"traffic data"	(f) pertains to information about a communication that shows its start, end, route, size, length, kind of service, time, and origin;
(xxxi)	"Unauthorized access"	(g) refers to getting into a restricted system or accessing private data without permission or in violation of the agreement's terms and conditions;
(xxxii)	"Unauthorized interception"	(h) refers to the act of intercepting data or information systems without permission; and
(xxxiii)	"Unsolicited information"	Means data sent for marketing and commercial purposes despite the recipient's explicit rejection, excluding legally authorized marketing. The terms used in the Pakistan Penal Code, 1860 (Act XLV of 1860), the Code of Criminal Procedure, 1898 (Act V of 1898). (i) The Qanoon-e-Shahadat, 1984 (P.O.No.X of 1984) shall have the same meanings as those in this Act and any rules made thereunder unless the context indicates otherwise. Given the circumstances.
(xxxiv)	"Interference with information system or data"	encompasses any kind of unlawful activity that may disrupt the regular operation or format of an information system or data, whether or not it actually damages the system or data;
(xxxv)	"investigation agency"	refers to the law enforcement agency authorized under this Act by the Office of the Chief Justice (OCJ)
(xxxvi)	"minor"	means any individual who has not attained the age of eighteen, regardless of any other legislation to the contrary
(xxxvii)	"offence"	An "offence" is defined as any violation of this Act that carries a penalty, with the exception of violations committed by individuals under the age of ten or by those between the ages of ten and fourteen who lack the mental capacity to comprehend the gravity of their actions at the time;
(xxxviii)	"rules"	refer to regulations promulgated under this Act;
(xxxix)	"seizing";	Making and keeping a copy of data or taking control of an information system or data also constitutes "seizing";

(xl)	"service provider"	A "service provider" is defined as an individual who does one or more of the following: (a) provides services related to the transmission, reception, storage, processing, or distribution of electronic communications or other services related to electronic communications through an information system; (b) owns, possesses, operates, manages, or controls a public switched network or telecommunication services; or processes or stores data on behalf of customers or electronic communication service providers.
(xli)	"Subscriber information"	refers to any data on a subscriber that a service provider stores, except traffic data;

The above table illustrates in detail how lexical expressions function as verbal co-text for important terms in the Pakistan Electronic Crimes Act, 2016, and influence their use within the legal genre/register. The frequent use of the same term with different meanings makes it crucial to recognize the words that appear together to differentiate legal language from other types of writing. Undoubtedly, the differentiation heavily relies on the presence of intertextuality and interdiscursivity.

4.1.2. Discursive Strategies used in PECA (2016)

Discursive strategies in the Pakistan Electronic Cybercrimes Act, 2016, identify devices that re/de-position ideological perspectives and create facts across and beyond textual subjectivities, constituting an ideological apparatus for power. These devices include:

4.1.2.1. Referential Strategies Used in PECA (2016)

Ruth Wodak's Discourse-Historical Approach (DHA) model provides a framework for analyzing the language and discourse of legal documents like Pakistan's Electronic Crimes Act 2016. Referential and nomination strategies play a crucial role in shaping the meaning and impact of the Act.

1) Use of Anaphora

Repetition of a word or phrase at the beginning of successive clauses or sentences (anaphora):

Prevention of Electronic Crimes Act, 2016, (PECA) was a welcomed statutory response to digital crimes and electronic data preservation issues in the state. This act is a consolidated legal framework for the prevention and control of cybercrimes to

ensure the official recognition of illegal acts committed against the security and integrity of electronic communication and data.

It defines crimes, as well as the process to investigate and penalize cybercrimes under three categories: offenses against confidentiality, Integrity, and availability of computer data and systems and data-related offenses.

Anaphora refers to the repetition of words or phrases at the beginning of clauses in any text or legislation to make it more persuasive.

To use anaphora as a rhetorical device is a well-known feature of literary texts, henceforth it is also used in multiple legal texts such as Pakistan's Prevention of Electronic Crimes Act (PECA) 2016. In examining the anaphora in this legislation, it is important to recognize the functional role of repetitive organization within legal writing, as repetition foregrounds key points, ensures clarity, reinforces important concepts, emphasizes ideas, and creates cohesion in the text. In the Prevention of Electronic Crimes Act 2016, anaphora is used to stress the violations and strict controls. There are multiple instances of the use of anaphora in the Prevention of Electronic Crimes Act 2016, showing how this rhetorical element strengthens legislative content and drives home legislative impact. Some examples of the use of anaphora are as follows:

1. For example, if we turn to Section 3 of the Act, the repetition of "to prevent" "is not accidental" as it evidences "that the Act in general, seeks to combat cybercrime proactively rather than "to react" to it after the electronic crime has already occurred". This careful repetition serves to bring home to the reader the importance of stopping cybercrimes, making the persuasive purpose of the legislation more convincing.
2. Also, the usage of anaphora in the Act functions as different subcategories of electronic crimes and their penalties. This can be seen in Section 16 of the Act which states "Whoever commits... shall be punished". This dichotomization naturally separates multiple offenses and strengthens the perceived weight of the punishment laid on those found guilty of electronic crime. This, using anaphora in the lines of the legislation, allows the law to send a strong message directly to the civil population by intimidating further

cybercriminal behavior. Relating, the Act uses anaphora to emphasize that international cooperation is crucial in fighting computer crimes.

3. In emphasizing this need for mutual legal assistance of public authorities, repeat repetition to section 359, under the Act that " there is provision for cooperation by " mutual legal assistance" for extraditions that are as well done by a treaty, among states to tackle cross-border ecosystem of kinky cyber offenses. The rhetorical strategy emphasizes the transnational character of cyber treatment and the intimate nature of the activities required to counter it — which reinforces the aim of international trust within the cybersecurity surroundings.
4. Furthermore, the use of the anaphoric device has been noted in the use of words like "electronic", and "digital" which have a focus on digital crimes. "Electronic" is redefined in Section 2 (Definitions) and repeatedly used in the context of direct commissions: electronic means", "electronic", data, "elements related to abuse of an electronic device" section C #55. Section 3 has the word "Cyber" repeated around to, indicate that it happened online:- Cyberstalking / cyber harassment / cyber bullying, etc.
5. As a further example, the title of the act might repeatedly reference "unauthorized access," "unauthorized copying," and "unauthorized transmission," in order to emphasize the seriousness of these crimes.
6. Breaking into an information system illicit copying of data, unauthorized transmission of information..." This repeated emphasis serves to reinforce the various kinds of unauthorized activities that can be understood as offenses.
7. By the repetition of specific phrases the law ensures to avoid ambiguity in its legal provisions using plain language and successfully attains clarity. This is done to avoid any misunderstanding of crimes and their penalties. For example, the repeated use of the following such as: "Whoever dishonestly as means, gains unauthorized access to any critical infrastructure information system; or Whoever, dishonestly as means, copies or extracts any data; or Whoever dishonestly as means transmits data". In this case above, the law is clear that whoever, with dishonest intention, Whoever, so commits any of the offenses specified in the opening part of this section shall be punished with imprisonment for a term that may extend to three years or with a fine not exceeding ten million Pakistan rupees or with both.

8. In the aforementioned legislation (PECA,2016), anaphora has been used to reiterate the power of the authorities as well as their limitations. This repetition ensures that the law enforcement authorities clearly understand their responsibilities. Thus, anaphora is used to highlight the duties of authorities and to set the boundaries of their power. So that, enforcement authorities should not be in doubt about their operational limitations. This repetition underlines the sweep of powers being given to the authority and the duties they have to tackle cybercrimes.
9. To emphasize penalties and consequences the act may use anaphora to elaborate on the sanctions for different offenses, which in turn makes it clear what the repercussions are for contravening the law.

Example: "Shall be punished with imprisonment for a term which may extend to three years, or with fine which may extend to five million rupees, or with both..." The attempted repetition of "shall be punishable with" also highlights the severity of the section as well as the variety of punitive actions possible.

2) Use of Cataphora

Cataphora is a term in linguistics referring to where in the discourse a word/phrase points to. It has been used in the Prevention of Electronic Crimes Act (PECA) 2016, to maintain precision, coherence, and streamlining of legal provisions. PECA (2016), being a milestone piece of legislation for the digital age, covers practically most of the regulations preventing cybercrimes. Although there are multiple instances illustrating the use of cataphora in the legislation some of which are as follows:

We look into instances of cataphora in the legislative document, which illustrates the use/rest of the preceding specified content and thereby provides an account as regards the nature of cataphora and its contribution to legal discourse.

1. The first example of cataphora in the Prevention of Electronic Crimes Act 2016 is Section 3, where definitions of various terms used in the act have been provided. Its use of the phrases "the following" or simply "such" act results in the antecedent being the acts enumerated in succeeding provisions defining specific offenses related to electronic crimes. It does so to link and direct a reader's understanding of what constitutes prohibited activities within the act

2. There is also another example of cataphora from Section 17, which discusses unauthorized access to information systems. The prank pundits make cataphoric references through the phrase "such data" and "such information" to link the definitions of unauthorized access to the aforementioned specifications of penalties for the same. With this type of cataphoric method, not only is the legal text comprehensible and applicable, but also logical and interconnected.
3. In addition, the connection is created between the prohibition of unauthorized interception and the consequences through the use of cataphoric references as in Section 21 of the Prevention of Electronic Crimes Act 2016 "such services" "such act". The legislative drafters therefore use cataphora in this context in a manner that facilitates the preciseness and systematisation of the legal content, also simplifying the mode of application and enforcement on the part of the agencies enforcing the act.
4. Furthermore, examples of cataphory make a question like that found in § 31 of the statute with terms "such device" and "such". The relevance of cataphora with the legal clauses, would help the stakeholders to understand and apply the provisions in a more effective manner, and it gives more coherence and clarity to the text of the law.
5. Finally, undersection 47 of Prevention of Electronic Crimes Act 2016 uses cataphoric references to 'such data' and 'such information' by connecting them to cyber-terrorism or the penalties with respect to the commission of any offence. This way by utilizing cataphora, the flow of this section goes with a clear coherence and flow which increases the level of precision and executability of the provisions of the act. No doubt, the Prevention of Electronic Crimes Act 2016 is one such example where cataphora is used effectively to create syntactic unity among its legal provisions.

3) Use of Metonymy

Metonymy refers to one thing that is supposed to represent whole other things. It is a figure of speech in which one term is substituted for another term with which it is closely associated. This has been observed frequently in legal documents. For instance, after critically analyzing the language used in the Pakistan Electronic Crimes Act, of 2016, the use of related terms for words like authority, instrument, or actions

instead of explicitly mentioning the word has been noticed at various points as mentioned in the examples below:

Metonymy in The Pakistan Electronic Crimes Act 2016 is used in various acts as follows:

1. In Article ##2, the term "authority" is often used as a shorthand for the official enforcement/investigatory/regulatory body, replacing the generic term with specific agencies such as the F IA.
2. In Article# 3 of the Act, in the use of the term “Unauthorized Access to Information System or Data” the word "Access" in this context is a metonym of the actual act of hacking or unauthorized system entry
3. In section #10 of the Act the use of the phrase “Cyber terrorism” is a metonym for the more general category of crimes that may be committed using a computer or the internet versus being restricted to individual or isolated criminal acts.
4. Section # 21, while describing Offences Related to the Modesty of the Natural Person and the Minor uses the term "Offences against modesty. This expression is a place name for some human actions that are morally wrong or hurtful and include theft, rape, and killing.
6. Section #24 uses the term "cyberstalking" as a metonym for the behavior of stalking someone using electronic devices to harass or intimidate.
7. In section #29 in the phrase “Retention of data the word "Data" becomes a metonym for all of the electrons and holes in all the information or documents that are in a digital format.

4) Use of Hyperbole

The Pakistan Electronic Crimes Act (PECA) 2016 employs hyperbolic language in various sections to emphasize the severity and urgency of cyber threats. Here are detailed examples of the use of hyperbole in PECA 2016, with references to specific articles such as:

1. Article 10: Cyber-Terrorism

Text: "Whoever commits or threatens to commit any of the offences under this Act, with the intent to create a sense of fear, panic, or insecurity in the government or the public or a section of the public..."

The words "create a sense of fear, panic, or insecurity" fall under hyperbole as it overstates the emotional impact and potential consequences of cyber activities. It seems to imply that any offence under the Act can cause mass terror and chaos, whereas in reality, it does not seem to have such a grave impact. Hence, the statement is over exaggeration and falls into the category of the use of the figure of speech i.e. hyperbole

2. **Article 11: Hate Speech**

The Text: "Who, on an information system or a computer device creates or transmits information that fosters interfaith, inter-ethnic or racial discord..."

Analysis: This phrase "likely to advance interfaith, sectarian or racial hatred" is so over the top to assume that if anyone were to even share certain ideas, the entire society would suddenly collapse into civil war. This is an exaggeration of whatever the effect of the speech can be in society.

3. **Chapter II: Offences against Dignity of a Natural Person# Article 20**

Text - Whoever knowingly and - with direct intent and so the whole country can perceive it - exhibits or takes advantage of the occasion to display in the mass media or communicates information about a factual event or facts which could harm the reputation or privacy of a natural person."

The phrase "harms the reputation or privacy" could be deemed to be hyperbolic in that it suggests that any disclosure of information has the potential to inflict serious or lasting damage to the reputation or privacy of an individual regardless of context or actual harm.

4. **Article 21: Offenses against Dignity of Natural Person and Minor**

Example of text: "A person who... makes public or uses for advertising purposes or otherwise, importing, disseminating, distributing or making available electronically a statement... defaming the good name or infringing on the privacy of a (...) natural person..."

Another Example: This article parallels Article 20 in its exaggeration, playing up the irreversible risk of disclosing certain types of information and heightening the threat.

5. **Article 22: Pornography of Child**

Text: "It is a crime to intentionally produce, keep, publish, transmit or exhibit any material through an information system that knows or should know that it contains child pornography..."

The term "knows to be child pornography" comprises a hyperbolic element that highlights the fact that the offender is fully aware and deliberate in their harmful activities. By using hyperbole, the certainty and intent behind the actions is emphasized.

6. **Article 24: Cyber Stalking**

"Whoever knowingly or intentionally with the intent to coerce, intimidate, or harass any person, transmitted an information which is - false, or obscene; or carrying false information to cause distress, or; promoted an illicit relationship; or identity of ***** by placing picture, name, address, or phone number without permission, shall be punishable"..."

The repetitive "intimidate" and "harass" in the article, in turn, employs a hyperbolic edge to present these actions as threats themselves. The language implies that the offender intended to do better than the existing status if the guy was here

5) **Use of Presupposition**

Presuppositions shape how the provisions of the Act are interpreted and the enforcement of this act. They provide the framework by which actions are judged in legal and judicial decisions. In legal texts, presupposition is an assumption or implication made in the language intended to be accepted, without explanation. In the case of cybercrime and regulation, the Pakistan Electronic Crimes Act (PECA) 2016 has reinforced the creation of specific norms to establish certain truths about cybercrimes and their regularization. The use of presupposition in PECA 2016 can be seen in specific excerpts, having detailed explanations of certain truths about cybercrimes and their regularization. The details from PECA 2016, with references to specific articles are as follows:

1. Article# 3: Unauthorized Access to Information System or Data

Text: "Whoever with dishonest intention gains unauthorized access to any information system or data shall be punished with imprisonment for a term which may extend to three months or with fine which may extend to fifty thousand rupees or with both". In the above text of article#3 it is assumed dishonest and unlawful to access information systems or data without permission. This assumption undermines the basis for making "unauthorized" access as a criminal offense, implying that any such malicious act is the product of wrong intention involving a conscious mind that must face a penalty for wrongdoing.

2. Article 4: Unauthorized Copying or Transmission of Data: Text: "Whoever with dishonest intention and without authorization copies or otherwise transmits or causes to be transmitted any data shall be punished with imprisonment for a term which may extend to six months, or with fine which may extend to one hundred thousand rupees or with both".

Explanation: The use of presupposition in this article implies that copying or transmitting data without permission is an act done with dishonest intentions. It is a general notion that unauthorized actions are the product of malicious intent, hence justifying punitive measures.

3. Article 5 - Interception of Information Systems or Data: Text: "Whoever with dishonest intention interferes with or damages or causes to be interfered with or damages any part or whole of an information system or data shall be punished with imprisonment which may extend to two years or with fine which may extend to five hundred thousand rupees or with both". Interpretation: The use of presupposition in the above-mentioned article of the Act implies that tampering with information systems or information, with dubious intention, is a malicious crime. It means that any interference is apt to cause harm or disruption, justifying the intervention of the law.
4. Article 10: Cyber Terrorism (Text) " Cyberterrorism.-Whoever commits or threatens to commit any of the offenses under sections 6, 7, 8 or 9, where the commission or threat is with the intent to,—

- (a) Coerce, intimidate. create a sense of fear, panic or insecurity in the Government or the public or a section of the public or community or sect or create a sense of fear or insecurity in society; or
- (b) Advance inter-faith. sectarian or ethnic hatred; or advance the objectives of organizations or individuals or groups proscribed under the law, shall be punished with imprisonment of either description for a term which may extend to fourteen years or with fine which may extend to fifty million rupees or with both.

The above Article 10 presupposes that the conduct of cyber offences or the possibility of cyber offences inevitably generates feelings of dread, panic, or insecurity. In doing so, it presumes that the activities in question are intended to disrupt the functioning of the government or society, which would call for harsh punishments.

5. Article 21 and 22: Offences against modesty of a natural person and minor—
Text (Article 21): " (l) Whoever intentionally and publicly exhibits or displays or transmits any information which—
 - (a) Superimposes a photograph of the face of a natural person over any sexually explicit image or video; or
 - (b) Includes a photograph or a video of a natural person in sexually explicit conduct; or
 - (c) Intimidates a natural person with any sexual act, or a sexually explicit image or video of a natural person; or cultivates, entices, or induces a natural person to engage in a sexually explicit act.

Article 22: **Child Pornography:** To fully understand the social and legal implications of Child Pornography from PECA 2016, its assumptions have to be evaluated:

1. Text: Whoever intentionally produces, offers or makes available, distributes or transmits through an information system or procures for himself or another person or without lawful justification possesses material in an information system that visually depicts:

- (a) A minor engaged in sexually explicit conduct;
 - (b) A person appearing to be a minor engaged in sexually explicit conduct; or
 - (c) Realistic images representing a minor engaged in sexually explicit conduct; or
 - (d) Discloses the minor's identity, shall be punished with imprisonment for a term extending to seven years, or with a fine extending to five million rupees or with both.
2. Any aggrieved person or his guardian, where such person is a minor. may apply to the Authority for removal. destruction of or blocking access to such information referred to in subsection
 3. And the Authority, on receipt of such application, shall forthwith pass such orders as deemed reasonable in the circumstances, including an order for removal, destruction, preventing transmission of or blacking access to such information and the Authority may also direct any of its licensees to secure such information including traffic data.

6) Use of Personification

Giving the quality of humans to digital objects (e.g. “computer system”) leads one to agency sense in which personification has been used in the legislation under study i.e. PECA, 2016.

In legal texts, personification means attributing person-like qualities or characteristics to an abstract notion, organization, or non-human. In the general frame of the Pakistan Electronic Crimes Act (PECA) 2016, it is personified to highlight the tragedy and the seriousness of cyber- crimes and their outcomes. Detailed instances of personification in PECA 2016 (references to article numbers are as under:

1. Article 10: Cyber Terrorism

Text: Whosoever, commits or threatens to commit an offence punishable under this Act then the offence is nothing except with the intention to evoke a sense of terror or panic or insecurity in the Government or the public or a section of the public..."

Explanation: The words "create a sense of fear, panic, or insecurity in the government" represent the government by giving fear, panic, or insecurity

qualities that belong to humans. In emphasizing the seriousness of the threat, attention to the fact that cyber terrorism can harm the political stability and public order is reflected in this personification.

2. Section 19 Offences Relating to Absence of Consent (a) Offences Against Person Misbehaving Modestly with a Natural Person (b) Offences Against Minors..."

Analysis: The phrase "harms the reputation or privacy" personifies "reputation" and "privacy," attributing to these abstract concepts the ability to be harmed, a quality normally associated with living beings. This reinforces the gravity of the harm and the effects of the dignity and the victim and the society.

3. Article 20: Malicious Code

Text: "whoever- with Intent to cause harm to an information system or data, or harm to users of an information system, knowingly- (1) writes, offers, makes available, distributes, or transmits malicious code or (2) when an offense results in- (A) the corruption, destruction, reduction in value or utility, or theft of information from, an information system."

This phrase expressly animates an information system or the data itself capable of being, that is, by putting the least stretching that is about being injured. In human terms, the personification signifies the havoc and chaos that an infected code can wreak the world of technology. In legal texts, personification means giving an abstract notion, organization, or a non-human person-like qualities or characteristics. In the general frame of the Pakistan Electronic Crimes Act (PECA) 2016, it is personified to highlight the tragedy and the seriousness of cybercrimes and their outcomes. Detailed instances of personification in PECA 2016 (references to article numbers):

4. ARTICLE 21: Illegally Issued SIM Card states, "Whoever sells, provides, transfers, or otherwise offers to another SIM cards or reprograms numbers for mobile telephones without express or implied permission and in a way that harms another person's interest or well reputation..."

The clause "causes injury to the interest or reputation of another person" turns both "interest" and "reputation" into people-ish entities; it suggests that the ether

can be injured. The personification of said "international economy" demonstrates the impact such unauthorized action could lead to upon individual social and economic being.

5. Section 23: Interference with Communication Equipment

Text: "Whoever dishonestly - (a) connects or disconnects or reconnects or tampers with, whether by way of installation, removal or maintenance, or (b) tampers with, alters or reprograms any communication equipment in a manner that causes wrongful loss to any person..."

The term "causes wrongful loss" purports to personify "loss", like physical or psychological harm and attributes that it can be caused, and accomplished in the duration. More of that personification, here stressing the damage communication sabotage can do to people and businesses.

4.2.1.2 Analysis and Discussion of Use of Referential Strategy in PECA 2016

The Prevention of Electronic Crimes Act 2016 in Pakistan effectively uses referential strategies to highlight clauses, emphasize the weight of cybercrimes, and reiterate the main aim of the laws and regulations. Anaphora is used to make the Act more persuasive and clearer, leaving an impression on future legislation that can address the challenges of cybercrimes. Cataphoric references are used to make the legislative text clearer, more cohesive, and easier to interpret and understand, contributing to the resolution of electronic crimes.

Metonymy is a linguistic device used in the Pakistan Electronic Crimes Act 2016 to describe various criminal activities, such as "Authority" for enforcement bodies, "Access" for unauthorized access to information systems or data, "Cyber terrorism" for broader criminal activities, "Electronic forgery" for falsification or alteration of electronic documents or data, "Offences against modesty" for acts that violate personal dignity and modesty, "Cyber stalking" for using electronic means to harass or intimidate someone, and "Data" for any type of electronic information or records stored in digital format.

Hyperbole is used in PECA 2016 to increase the perceived severity of cybercrimes and justify the implementation of stringent monitoring and severe penalties by exaggerating the seriousness and scope of any potential cyber threat to society or national security. This exaggerated language may lead to disproportionate punishments

and potential misuse of the law, as well as create ambiguity and lead to misinterpretation, impacting the enforcement and adjudication of cyber-related offences.

The examples of hyperbole in PECA 2016 highlight the need for a critical examination of legislative language in the context of cyber legislation. Striking a balance between protecting digital rights and addressing cyber threats without resorting to hyperbolic language is crucial for effective cyber legislation.

The use of presuppositions in PECA 2016 plays a crucial role in framing the understanding and regulation of cybercrimes. By embedding assumptions about the nature and impact of certain actions, the Act establishes a normative framework that justifies its provisions and enforcement mechanisms. This rhetorical device helps convey the seriousness of cyber threats and the necessity of robust legal measures to address them.

In the Article on Child Pornography in PECA 2016, the use of presuppositions is pivotal in shaping the interpretation and application of the law as a whole. By casting alleged transgressions as so intentionally benighted by attackers that there is no alternative, or by their vilely implied victims that the only response can be exclusively punitive and regressive, the article reminds of the gravity of these offenses and the imperative of shielding innocent children at their unwilling center.

Personification in PECA 2016 serves several purposes, including reputation, privacy, and interest as subjects. It adds human qualities to abstract concepts, making cybercrimes more real and understandable to the public. This language technique makes cybercrimes seem more severe, justifying harsh measures and penalties. Overall, personification in PECA 2016 highlights the severity of cybercrimes and the need for robust legal measures to protect innocent children.

PECA 2016 employs various referential strategies to shape the narrative around digital communications and cybercrime. By using terms like 'offensive', 'harmful', and 'threatening', the act creates a negative reference framework that associates online dissent and criticism with criminal behavior. This framing serves to delegitimize and criminalize free speech, particularly when it criticizes the government or sensitive institutions. Its various sections uses broad and ambiguous language to classify certain online activities as offenses and cybercrimes. These referential strategies not only

provide grounds for legal action against dissenters but also discourage individuals from expressing their views openly, thereby hindering free speech. By framing critical voices as potential threats, PECA effectively curtails the freedom of expression, promoting a culture of self-censorship and limiting public discourse.

4.1.2.3. Use of Nominalization Strategy in PECA 2016

The technique of nominalization involves turning actions or processes into nouns. The use of this strategy makes the legal text more formal and legal documents. The conversion of turning acts or processes into nouns helps the legal document to project a sense of objectivity, and authority, to distance themselves from everyday reality. Transforming a verb into a noun makes it a more abstract idea rather than a concrete description of a particular activity; this is what an act does. Enclosing the legal language in this abstraction elevates its formality.

Nominalization depersonalizes actions and gives seriousness and formality to cybercrimes under the Pakistan Electronic Crimes Act, 2016 (PECA) At the same time they do not outperform any other law, here are detailed examples of the use of nominalization in PECA 2016, with references to specific articles:

1) Article #10: Cyber Terrorism

"Whoever commits the following acts; or threatens to commit any of the offences punishable under this Act, to unduly influence the course of justice, to create a sense of fear, panic, or insecure; in the Government or the public or a section of the public..."

Nominalization: Hides the perpetrators: Again, the (doing) words "commit" & "threaten to commit" get (put into) nouns (offences) to smother the very idea of a person doing wrong. It removes the spotlight from the person and put it on this nebulous philosophy of 'offences.

2) Article #20 - Offences against the Dignity of a Natural Person

Text: "Any person who, with deliberate intent, discloses or directs any information... that can damage a natural person's reputation or privacy..."

Nominalization: Using "exhibits," "displays," and "transmits" as nominal forms both subordinates the actions to the performers of the action and gives the sentence a more impersonal and formal sense.

3) **Chapter Three - Offences against the Modesty of a Natural Person and Minor Article #21:**

Text: "Whoever, intentionally and publicly displays, shows, transmits information of the kind... which violates the personal right or privacy of a natural person.."

Nominalization: As with Article 20, the actions are nominalized to discuss reputational or privacy harm as though they are abstract concepts - rather than the impact on specific behaviors.

4) **Article#23: Communication Equipment tampering**

Text: - Who is dishonestly connects or disconnects or reconnects, tampers with, alters or reprograms any communication equipment in a manner that causes wrongful loss to any other person to (...)."

Nominalization: Connects; disconnects; reconnects; tampers with; alters; and re-programs are nominalized, thereby underscoring the acts themselves, and the possibility of resulting wrongful loss, as opposed to the intents or conduct of the persons involved.

5) **Article #24: Cyber Stalking**

Article#21a) related to" whoever with the intent to make the person feeling fear, intimidate or harass a person uses a communication device to.....punish or threaten or harass a person.."

Nominalization: The process of nominalization is used, in which the terms "coerce," "intimidate," and "harass" are changed into nominal forms to abstract the actions and draw attention to the harmful impact of cyberstalking at large.

6) **Article #25: Spamming**

Text: "Anyone who disseminates, disseminates beneficial, misleading or unsolicited information to anyone without the prior consent of his addressee..."

Nominalization: The infinitive verb phrase of transmitting "harmful, fraudulent, misleading, or unsolicited information" is nominalized as a concept, describing only the material of the information and the transmission of it as a harmful abstraction.

4.1.2.4 Analysis and Discussion of Use of Nominalization Strategy in PECA 2016:

Nominalization is a discursive strategy identified by Ruth Wodak. It involves transforming verbs or actions into nouns, which can obscure agents and actions, thus affecting clarity and agency. In the Prevention of Electronic Crimes Act (PECA) 2016, nominalization is used to depersonalize and abstract actions, making it challenging to attribute responsibility and intent. For instance, terms like "unauthorized access" and "glorification of an offence" are nominalized, focusing on the act rather than the actors. This shift from concrete actions to abstract nouns dilutes the perceived agency and hides the actors behind these actions.

The use of nominalization in PECA 2016 serves several key functions such as converting verbs into nouns, the Act abstracts actions, making them appear as generalized concepts rather than specific behaviors. This abstraction adds a layer of formality and authority to the legal text.

The use of this strategy shifts the focus from individual actions to the offenses themselves, depersonalizing the crimes and emphasizing their seriousness. This helps in creating a perception of impartiality and objectivity in the law. Its use contributes to the formal tone of legal language, enhancing the perceived legitimacy and weight of the Act's provisions. It often highlights the consequences of actions, such as "harm," "loss," and "intimidation," drawing attention to the impact of cybercrimes on victims and society. This strategy impacts free speech by creating a legal framework where broad and vaguely defined terms can be interpreted subjectively. As a result, individuals may self-censor to avoid potential accusations and legal consequences, limiting open and critical expression. The ambiguity introduced by nominalization thus indirectly curtails freedom of expression. Hence, provisions in PECA 2016 show the violation of Jack Balkin's theory of Information Fiduciaries which implies that online platforms and internet sources have a fiduciary duty to protect users interests by preventing them from the free use of these forums and giving the authority to control and surveillance to the hidden power sources.

4.1.2.5. Use of Predicative Strategy in PECA 2016:

Ruth Wodak's Discourse-Historical Approach (DHA) involves the prediction technique, a method for assigning features or actions to discourse participants. This method facilitates the assessment and characterization of social agents, events, and

sometimes objects in a manner that is consistent with the speaker's or writer's intentions (Van Londen et al, 2009). A person makes or breaks the traits of good and bad, that's why predictions matter. Forecasting in a legislative analysis can provide perspective on not only what the law intends but how widely the law might impact. It may shape public narratives, encourage compliance, and set standardsbased settings. Practice examples from PECA 2016 when a prediction is operationalized like defining dishonest intention through means of unauthorized access to data or information systems, characterizing cyberwarfare as a menace rather than a crime, and crimes against individual dignity. Nevertheless, predication is a critical component for the critical evaluation of legislative texts as well as a tool that implies broader meanings of legal terminology.

It is one of the discursive strategies given by Ruth Wodak in her Discourse Historical Approach (DHA). It involves giving participants in a discourse certain characteristics, behaviors, or qualities. Prediction often allows for the evaluation and description of social actors, events, or objects in a way that enhances the intended meanings of the speaker or author. It frames things by expressing certain viewpoints or ideas. Predictions are important because they help individuals develop their positive and negative tendencies. It has some key aspects such as characterization, evaluation and contextualization. Which are shortly defined as under in the context of analysis of a document:

- i) Characterization is to assign positive or negative traits to persons
- ii) Evaluation is the process of making decisions based on predefined criteria.
- iii) Contextualization is the process of putting a subject into a certain context to affect how one perceives it.

Legislation Analysis and Prediction's Effects The use of the predication strategy in legislative analysis has profound implications for understanding the intent, scope, and impact of the legislation based on the following important issues in the legislation:

1. Lawmakers, law enforcement, and the general public may see legal issues through a certain lens by using predictions. Calling anything "fraudulent" or "harmful" highlights the need for control and sends the wrong impression.
2. Legislative justification for stringent laws might be provided by linking certain behaviors or activities to undesirable characteristics. The severity of

cybercrimes is increased when terms like "malicious" or "destructive" are used to characterize them, which supports the imposition of severe penalties.

3. The way that laws require certain behaviors has an impact on public perception and social norms. For instance, promoting the notion that breaking into computer systems is fundamentally "dishonest" presents such behavior in an unfavorable light from a legal and moral point of view.
 4. The regulations included in legislation serve as a guide for law enforcement and judicial authorities. Clearly defined behavioral norms facilitate the consistent application of the law. For instance, phrases like "intentional" and "reckless" help determine how serious an offense is and how much punishment is appropriate.
 5. Legal normative frameworks, which determine what behavior is acceptable and unacceptable, are shaped in part by the predication process. This helps to create a moral and legal code that is consistent and represents the community's values.
- Some evidences of use of Predicative Strategy in PECA 2016 are as below:

In this legislation, the predication strategy given by, Ruth Wodak (in the Discourse-Historical Approach, DHA) is employed to mean adding specific properties or values or any action to a subject in the text. This is a common method to describe and determine people and activities in a manner that matches the intent of the author or the legal purpose of the text. A key term used in the Pakistan Cyber Crimes Law 2016, is predication used to define cybercrimes and what an individual commits includes, highlighting the seriousness of such an offense and making it sound as if it gives a reason behind its legality. Detailed examples of predication within PECA 2016: - Inclusion in PECA 2016 with references to specific articles.

1. In Article 3 titled as "Unauthorized Access to Information System or Data"- 2) The term "with dishonest intention" predicates the disfavored attributes to unauthorized access by essentially labeling it as necessarily deceptive and hence torment.
2. In Article 5 titled as "Unauthorized Reproduction or Transmission of Data" the use of predication strategy is obvious in the expressions such as "dishonest intention and without authorization predicates formal use of the act of copying or transmitting as malicious and illegal

3. Article 6 “Interference with Information System or Data”: The use of “dishonest intention” here predicates the act of interference as intentionally harmful and illegitimate.
4. Article 10 titled as “Cyber Terrorism” makes use of the term of imprisonment (besides life imprisonment) was increased from seven years to 14 years in the above clauses and also in other clauses by specifying that a person committing that offence or threatening to commit it with the intent to cause the government or the public to feel fear or panic or insecurity be subject to a term of imprisonment of up to 14 years. The typical predictions of cyber terrorism are referred to the outcomes based on the arguments of the terms "fear," "panic," and "insecurity," which are portrayed as events that have the intention of wreaking havoc on society and government.
5. Article 18 And 19 regarding” Crimes against the Human Will and Honour” uses the the predication strategy implies that the action would have been characterized as a violation as long as it will harm the reputation or privacy.
6. Article 20 titled as “Malicious Code” in which examples of a code is "malicious" (a predication -- the code is "spiteful" by design and has been bred to harm and destroy)
7. In Article 21 titled “Cyber Stalking” predication is evident in the following words such as "coerce," "intimidate," and "harass" which predicate the actions of cyberstalking as abusive and harmful, evidencing the intent to cause harm to victims.
8. Article 25 titled “Spamming” Uses adjectives like harmful, fraudulent, misleading, and unsolicited to predicate the nature of the spam as being illegitimate.
9. Article 26 “Spoofing”. In this article, the phrases "dishonest intention" and "counterfeit source" are used as predication strategy tools for fooling and forgiveness.

4.1.2.6 Analysis of Use of Predicative Strategy in PECA 2016

The method offered by Ruth Wodak to predict the laws is an interesting analysis method to be applied to legislation. It sets conceptual, empirical, and normative framing, shaping public opinion as well as contestation of legitimacy, provoking a process as legislative action. The purpose of making this distinction is to be able to read

critically, particularly statutory texts, and to understand the larger implications of legal nomenclature.

The use of predication strategy in PECA 2016 is a rational lingual weapon employed in characterizing cybercrimes and their actors. If crimes are written in such a way that they are associated with a particular set of negative properties and results, the Act will position these actions to be serious threats and thus warrant harsh legal responses, shaping public opinion in these actions as cyber threats against future cyber threats.

4.1.2.7. Use of Argumentative Strategies in PECA, 2016

The argumentative strategy focuses on how arguments are made to support viewpoints, actions, or policies, is a part of Ruth Wodak's Discourse-Historical Approach (DHA). This tactic uses argumentation frameworks, or topoi, which serve as a foundation for reasoning. It focuses on how arguments are made to support viewpoints, actions, or policies. Using topoi (commonplaces) or argumentation schemes to serve as a foundation for reasoning and justification within a text is the application of the argumentation strategy. Convincing the audience of the need for certain actions and the legitimacy of particular points of view is aided by argumentation. It provides rationale from inside a text. The legislation under study i.e. PECA, 2016 makes use of some topos (common places) that are used to make authoritative powerful arguments in a discourse. These topos claim to be arguable. It refers to the justification of positive and negative attributions through "topoi." The following is a detailed examination of the topoi, using examples found in the text of PECA 2016. There are different kinds of topoi, such as:

- i) **Topos of Burdening:** When an institution or a state is burdened, they legitimize an activity. For instance, in the case of PECA 2016, article #9 spread of information via any system or device data shall be punished, which is an indirect attack on freedom of speech. Hence an action that is an open violation of human rights has been legitimized as the authority was burdened via free speech. In Article 10# "Cyber Terrorism", topos of burden has been used. The article calls cyberterrorism a "burden", as it is a major source of fear, panic, and insecurity for the government and public. This duty is a justification for harsh

punishments, and preventative precautions, in order to keep society safe and to continue to function smoothly and peacefully.

- ii) **Topos of Reality:** It logically refers to some action that has to be performed. For instance, all articles in PECA (2016) implement punishment and fines using language such as: individuals or groups shall be punished with imprisonment, or fine may be extended. The topos of reality deal with real or practical problems, and thus it often justify measures by the fact that they change things. For example, Article #19: Crimes against Human Honour, presents the use of topos of reality it focuses on the repercussions to one's name and privacy, referencing real-life implications. The practical implications for a person's identity and privacy are emphasized. This background only explains the necessity for legal protection of the dignity of individuals.
- iii) **Topos of Numbers:** Some specific statistical evidence is given to legitimize certain actions. The topos of numbers mean the use of statistical data or numerical evidence in support of an argument, illustrating the magnitude or importance of an issue. For example: In Article 15: Cyber Terrorism and Financing of Terrorism. The use of topos of numbers refers to additional numbers such as when speaking of imprisonment for a certain period that emphasize the gravity of what has been criminalized and brings out the scope of the legal penalty and therefore highlight the gravity of the problem. As in PECA (2016), the action to tackle cybercrimes via punishments is legitimized through the use of numbers which have added to its authenticity, such as five years imprisonment, ten million rupees fine, the numbering in the Acts from #1 to #51 as well as the sub numbers. Article#23 also uses topos of numbers by referring "wrongful loss" entails the quantification of the damage, amount which can be numeric which indicates how the punishable act could leave adverse effects.
- iv) **Topos of History:** It means learning from past mistakes to avoid repetition of such errors in the present. In the case of ETO, PECA, and PECA Ordinance, an attempt has been made to amend these legislations to avoid cybercrimes. This article examines three example topics to explore how the Prevention of Electronic Crimes Act (PECA) 2016 uses authority and history.

History topos uses previous occurrences or precedents to justify the current situation. It provides background information so we may comprehend the significance of this measure. The opening section refers to a complex history of prohibitions stating "while it is necessary to criminalize unauthorized actions in relation with information systems, and provide for corresponding crimes by using modern electronic implements, whereas the territory of Pakistan's laws don't cover commissioning offences with new technologies." This relatively complex historical topos is used here because it places cybercrime in perspective and demonstrates the inadequacy of past laws.

Provides background information and explains why this legislation always follows a transparent legal procedure. It helped to comprehend how legal requirements have evolved in response to technological advancements and emerging risks. It ensures that the laws are valid and enforced since they are based on information from designated organizations.

These are crucial concepts in the development of a solid and convincing legal theory that addresses contemporary problems, maintains continuity with earlier theories, and works within the framework of pre-existing institutions.

- v) **Topos of Authority:** The concept of authority refers to authorities (experts, institutions, to the extent that methods are created by law), who, by presenting actions derived from certain laws, provide credibility and validity to an argument. It refers to following the orders given by some authority. Such as in the legislation under study PECA,2016, all orders are promulgated by the administration for immediate implementation. Topos of Authority relies on the legitimacy and expertise of some entities or individuals to justify a course of action or policy. For instance in Article#22” Child Pornography” The legislation relies on the authority of the designated body to oversee the removal or blocking of harmful content. This validates the Authority as the most legitimate safeguard for minors and for measuring harmful content that minors may access.

Section # 48: Rule-Making Authority states: “The Federal Government may establish rules to carry out the objectives of this Act by notifying them in the official Gazette; The Pakistan Telecommunication Authority, for example, is described as "the

Pakistan Telecommunication (Re-organization) Act 1996 (XVII of 1996) established under the Pakistan Telecommunication Authority" in Section 2. In an attempt to provide the impression of professional backing for its positions, this act makes appeals to a reputable organization.

In summary, this analysis of PECA shows that, by resurrecting an appeal to a tradition rooted within various discourses surrounding history, authority, and how they are utilized, it seeks to legally situate itself within a specific point in time as well as space and to historically define cybercrimes. The two topoi accomplish the vital tasks of providing context, legitimacy, and coherence in their informative argument that new cybercrime laws are required.

Federal Government's authority and standing to support people conduct as a valid, authorized organization. The Act leverages recognized power for the implementation of its requirements, in addition to citing the Federal Government's competence to make laws and the Pakistan Telecommunication power. Topos of authority reinforces the credibility of the legislation as the reputable organizations and established depend on legal frameworks, which guarantees the Act's validity and credibility.

Another usage of the topos of authority is Enforcement which demonstrates that the Act has State-enforcing agencies to carry out the terms of the Act, hence increasing its effectiveness.

It also builds trust that helps to develop public confidence in the application of law by showing people that it is backed by reputable regulatory agencies which are entrusted with monitoring and enforcing it.

Topos of Definition: It means specific action has to be done concerning definitions provided in the concerned document. The Prevention of Electronic Crimes Act (PECA) 2016 employs the topos of definition to provide a clear legal framework for prosecuting various cybercrimes and offences. This method ensures accurate definitions, preventing ambiguity and setting the law apart from misinterpretation. The first section defines unauthorized access to data or information systems, stating that anyone with dishonest intentions gains such access must be punished with imprisonment for up to three years or with a fine of up to one million rupees. . In PECA

(2016), Act#2 gives detailed definitions of all the terms used in the entire document has been provided.

The second section defines unlawful copying and transmission of data, stating that anyone without authorization copies or transmits data without permission will face imprisonment for up to six months or with a fine of up to one hundred thousand rupees.

The third section defines cyberterrorism, stating that anyone who commits or threatens to commit any offence with the intent to coerce, intimidate, create fear, panic, insecurity, or intimidation in the government, public, community, sect, or society, advance interfaith, sectarian, or ethnic hatred, advance the objectives of organizations or individuals or groups, or create a threat to Pakistan's security or defense will be punished with imprisonment for up to fourteen years or with a fine of up to fifty million rupees.

The fourth section defines electronic forgery, stating that anyone with the intent to cause damage or injury to the public or any person, makes, generates, or creates false electronic records with the intention of misleading, will be punished with imprisonment for up to three years or with a fine of up to two years.

Lastly, the fifth section defines unauthorized interception, stating that anyone with dishonest intention commits unauthorized interception by technical means of transmissions not intended for public consumption and technological methods. This precise description outlines the parameters of the offense and the related penalty.

Topos of Urgency: This strategy is used to show the urgency of an action to be accomplished to address an issue. In PECA 2016 emphasizes the need for immediate legal measures to combat evolving cybercrime methods. Section 10 of the law states that anyone who violates sections 6, 7, 8, or 9 with the intention of inciting fear, panic, or insecurity in society will be punished with imprisonment or fines up to fifty million rupees. This urgency is crucial as it incites widespread fear and panic.

Section 13 of the law addresses electronic fraud, which can cause harm to the public and can result in imprisonment for up to three years or both. The law also provides urgent use guidelines to prevent harm and maintain confidence in electronic records.

Section 3 covers unauthorized access to data or information systems, which can lead to damage and potential misuse. The law carries a fine of up to one million rupees or imprisonment for either offense, but not less than both.

Section 9 addresses violations of an individual's dignity, which can result in a maximum three year jail sentence and a punishment of one million rupees for transmitting, displaying, or making material that violates someone else's privacy or reputation. Cyber harassment and defamation are considered the most important factors to consider in modern society.

Lastly, Section 22 of the law allows for online stalking, where anyone using an information system to force, threaten, or harass someone else faces a maximum three-year jail sentence and a fine of one million rupees. The law believes that these offenses are detrimental to people's mental health and must be stopped immediately.

4.1.2.8. Analysis of Use of Argumentative Strategy in PECA 2016

In conclusion, the PECA 2016 highlights the importance of prompt and stringent measures to protect personal safety and the safety of the public and the nation from cybercrime. The use of argumentation in PECA 2016 has several implications. It provides justification for the existence of certain legal provisions, convincing stakeholders, framing legal discourse, and establishing agreement. Argumentation justifies the existence of certain legal provisions by citing various topoi. It also helps shape the conversation around cybercrimes and related laws by framing them within security, privacy, and human dignity settings. Furthermore, argumentation aims to establish an agreement on the importance of thwarting cybercrimes and safeguarding digital infrastructure and individual rights. Ruth Wodak argues that argumentation is an essential tool in legislative debate, used in PECA 2016 to support the Act's terms, influence stakeholders, and set the tone for the conversation about cybercrimes. However, it creates a restrictive environment for freedom of speech on digital platforms.

Topoi in the PECA 2016 build powerful arguments that rationalize the enactments of the act and remedies of the act. Invoking the cost of cybercrimes to society, the status of regulatory bodies, the quantification of monetary fines, and the tangible effects of offences, the Act constructs cybercrimes as significant risks that require harsh legal measures. They need to employ these rhetorical strategies to help

convince any stakeholders of the value of the legislation and why the bill is necessary in helping combat cyber threats and protect society. Hence, these findings support PECA,2016 to exercise provisions against free speech.

4.1.2.9. Use of Perspectivation Strategy in PECA 2016:

Ruth Wodak defines perspectivation as the act of situating the speaker or writer in a particular view or perspective to construct narratives, highlight key points, or skew one's interpretation of events or deeds." The Pakistan Electronic Crimes Act (PECA) 2016 uses perspectivation to legitimize and frame cybercrimes and their regulation in a way that emphasizes their significance and the need for strict punishments. Here are some specific examples of how Perspectivation is used in PECA 2016, along with citations to the relevant articles:

Article #17: Unauthorized Access to an Information System or Data

- (1) Whoever accesses any information system or any part thereof in contravention of the provisions of this Act, shall be punished in accordance with the second paragraph of Section 269 subsection (1) of the Criminal Code..."

This is a perspective of moral indictment, framing the lack of authorization as an act of bad faith. That perspective primes a reader to see actions like those as "wrong," and that wrong actions deserve consequences.

Article #10: Cyber Terrorism states:

"Whoever commits or threatens to commit any of the offences under this Act, intending to create a sense of fear, panic or insecurity in the government, or to the public or a section of the public..."

The partial point of view: portrays an image of National security and public safety Text []): During this period, cyberterrorism is mainly seen as a threat to the state and society stability and security so the legislative response should be the highest in order to secure both parties.

Article 19: Crimes infringing upon dignity of a person

Text: "Whoever deliberately and publicly exposes or displays or distributes any information which... detrimentally affects the good name or privacy of a human being..."

Perspective Protection of human dignity and privacy View in the article It presents these offences as severe violations of personal rights, and in doing so, it legitimates punishing reputation and privacy-related penalties.

Article 20: Malicious Code

Text: "Concerning anyone who intentionally produces or otherwise makes available malicious code with the purpose that it damages an information system or data, as a consequence that it alters, destroys, reduces the value of utility or steals data..."

Analysis: From a technical perspective, the protection of digital infrastructures M andates malicious code creation and delivery as a serious threat to information systems, with the potential for great harm, and requires prevention efforts.

Article 21: Cyber Stalking

Text: "Whoever- With the intent to coerce, intimidate, or harass any person... uses information system, information system network, internet, website, electronic mail or any other similar means of communication to harm, intimidate, or harass any person..."

This article is written from the perspective of individuals that have trust issues for being constantly harassed. By placing such an empathic focus on cyberstalking as a personal violation, we are creating a culture that escalates to legislation, emphasizing the deep emotional and psychological trauma cyberstalking creates in victims.

Article 25: Spamming

"Any transmission by any person of any electronic mail, facsimile, or other telecommunication device to any other person, with the intent to deceive or mislead the addressee or recipient about the"

The point of view on which this article is based is Consumer Protection and Privacy. It paints spam as a dangerous, invasive thing, with the recipient the put upon, innocent victim who needs to be protected from evil unwanted communications.

Analysis and Discussion of Use of Perspectivation Strategy in PECA 2016:

The implications of the perspectivation in the PECA 2016 are addressed as follows:

1. **The Act: Framing of Issues:** Specific perspectives represent cybercrimes as serious threats to security, privacy, and individual dignity. By framing the public perception in this way, it makes sense for the severe measures and penalties that are likely justified.
2. **Shaping Induction:** Perspectivation constrains readers' understanding of the magnitude and type of cybercrimes. The Act frames the discussion of these problems through the lens of particular points of view by stressing the urgency of legal intervention.
3. **Sanctioning of Actions:** The Act speaks through the practices it sanctions and the penalties it imposes. The Act thereby normalizes the view that cybercrimes inherently threaten or harm human beings, justifying draconian legal responses. As Mumahammad F. (2016) mentioned, “from holistic perspective, PECA 2016, may be serving some good purposes but due to the presence of some sections like section 11 and section 37, it will not achieve its objectives to combat cybercrimes, it will worsen the conditions of basic human rights”.

PECA 2016 has adopted perspectivation as a strategic linguistic tool to view cybercrimes from distinct vantage points to underscore the gravity of acts and the necessity of strict enforcement. It shapes the reader into certain positions and allows our understanding of cybercrimes to be influenced by the provisions and punishment it prescribes for the exact reasons of the Act. This is a good strategy to convince the reader that you care about protecting the country and its citizens, and wish to ensure security and human rights.

4.1.2.10. Use of Framing Strategy in PECA, 2016

In the context of linguistics, framing refers to the use of language as a way to manipulate the text in such a manner that its interpretations, ambiguities, and conclusions are framed to hide its real purpose. In the Prevention of Electronic Crimes Act (PECA) 2016 via the use of Ruth Wodak's Discourse-Historical Approach (DHA), its framing will be explored. Through DHA, you can analyze how discourses are formed and the socio-political & historical contexts within which they emerge. The way topics, actors, and events are presented to elicit a certain view or understanding is referred to as framing. PECA 2016 employs framing techniques to make cybercrime seem like an urgent danger and to support the necessity for strict legal actions. This paper will

explore this specific use of framing in PECA 2016 with an analysis against some characteristics identified by Wodak: Examples of Framing in PECA 2016

1. Threat Framing:

Cybercrime is being threat framed as a potentially immediate and catastrophic risk to national security, public safety, and individual privacy. This frame pushes the need for some urgency and insistence on legislation.

Text: "Whereas, it is expedient to prevent unauthorized acts to information systems and provide for related offences..."

Analysis: Cybercrime is presented as a serious and immediate danger to privacy, public safety, and national security. This characterization of the danger supports the necessity for swift and forceful legal action. The use of threat focuses on the dangers associated with cybercrime, and hence frames them as risky states in need of immediate legal solution. The act relies on portraying cyber threats as all-encompassing and metastasizing to justify its draconian remedies. Its purpose is manipulation to Re-characterize cybercrimes as a significant problem that results in the formation of forceful legislation. It distorts the narrative of national security in a way that it makes the audience to forget about potential privacy and freedom issues

2. Protection Framing:

Protection framing means defensive framing. This framing emphasizes on protecting citizens, economies and governmental infrastructure against cyber threats. It frames the law as a preventative utility.

Evidence: Text "Whoever with the intent of committing any offense gains unauthorized access to any information system or data shall be punished..."

3. Responsibility Framing:

Responsibility framing emphasizes the role of government and other authorities responsible for protecting citizens from digital threats and ensuring public order.

Text: "The Central Government may, by notification in the official Gazette, make rules to carry out the purposes of this Act".

This amplifies the topos of responsibility, that is this civilization has a duty towards (against) cyber security. It is emphasized that it is the duty of the government and pertinent authorities to carry out and uphold the law. The state is portrayed in this way as a proactive protector of digital security. It also underlines the importance of regulators to counter a digital terrain. It also leads to intentional misdirection, by presenting the law as appropriate governmental action, this reinforces criminalization and absolves itself of any reasonable challenge. It skews the conversation making it easier to pass and enforce this law with little oversight.

4. Modernization Framing:

Modernization framing refers to the capability to modernize existing, legal frameworks emphasizing how rapid innovation means that both our laws and the threat environment has changed. These kinds of steps can only be possible by reforming the existing laws in Pakistan which do not cater for offences with new tech help

It is emphasized that legal frameworks must be updated to keep up with technological changes. This sort of framing suggests how cyber risks are constantly emerging and hence in order to tackle the crimes how updated essential it is to have the updated laws. This construction suggests that the law must be upgraded to catch up with technological development. It paints the legislation as a positive reform of an outdated legal system. The aim of such framing is manipulation. It reforms the law as an inevitable modernization process, thus countering resistance to change and capturing support from stakeholders linked to technological advancement and new abstraction.

4.1.2.11 Analysis and Discussion of Use of Framing in PECA 2016

Through the use of the manipulation of objectives and perception in cybercrime legislation. It suggests three main strategies: developing urgency and commitment through threat and protection framing, instituting authority and control through responsibility framing, and modernization framing. The former suggests that the law is urgent and necessary to address cybercrime, while the latter portrays opposition as a threat to state security. The text also highlights the importance of modernization framing, which deflects criticism about overreach or misuse by focusing on the law's role in updating and improving the legal framework.

Finally, the text suggests that presenting the law as protective and required can lead to less opposition without promoting public safety or technological advancement.

Protection framing according to Lamont and Ho argues that anti-intensive captivity' legislation was the answer to welfare usage as by focusing on individual rights this new ideal could say it was necessary for security. This caricatures the law as a cyber-troll. By defining the law as a protector, it generates public and political support. This in turn shifts the focus from overreach or misuse of the law to its benefits, ensuring its necessity and security. It further emphasizes its importance to safeguard people against online dangers. According to this interpretation, the law serves as a safeguard to protect people from damage and to protect society as a whole.

The results from the PECA 2016 text, analyzed using Ruth Wodak's Discourse-Historical Approach (DHA) demonstrate an ideological framing that suggests how the act in the legislation uses discourse and framing techniques to create a convincing story about cybercrime and the need for judicial action. This framing emphasizes urgency, authority, and progress alongside four substantive symbols: threat arguments promoting change; protection spilling over into responsibility to highlight unseen costs as a consequence of not adapting to promote further modernization. These framings not only frame the public perception of laws in a way that justifies their strict measures and minimizes opposition. It ensures its successful execution by establishing its authority, validity, and ethical base via thoughtful discourse presentation.

4.1.2.12. Discourse Presentation in PECA (2016)

In PECA, 2016 discourse has been Presented is a persuasive way tool to portray the legislation as essential, authoritative, and all-encompassing. It employs various discursive techniques to persuade the audience with language, reasoning, and rhetoric. These techniques include nomination and prediction strategies, which involve naming and identifying players such as authorities, offenders, and victims, and predicting them as dangerous criminals, innocent victims, or dedicated officers. This helps draw moral lines and support the need for strict regulations.

4.1.2.13 Evidence of Discourse Presentation in PECA 2016

1. Criminalization of Expression: Discourse strategies in PECA 2016 frame particular forms of the expression online as criminal acts, without passing specific individuals. For example, Section 20 has a broad interpretation, for example, by the use of phrases like "intentionally" and "without lawful justification," whereby only "spreading false information" is penalized.

2. **Threat to Public Order and Morality:** This is also frequently the case, as the act uses expressions such as: 'disruption of public order' and 'protection of morality' to justify the restriction of online content¹. These terms are nowhere defined clearly and through broad enforcement they effectively chill legitimate free expression in the name of upholding moral standards.
3. **Ambiguity in Cybercrimes:** Words like “cyber terrorism” and “electronic forgery” are used to construct a story in which those online activities are part of something much bigger. PECA 2016 mixes the discourse by not specifying the exact nature of these threats, thereby contributing to creating a climate of fear in which people are constantly looking over their shoulders, seeking to voice yet fearing to dissent.

Through these discourse presentation strategies, PECA 2016 effectively curtails free speech by creating a legal and societal environment where the boundaries of permissible speech are blurred and may be enforced arbitrarily.

4.1.2.14 Analysis and Discussion of Use of Discursive Strategies in PECA 2016

PECA 2016 uses various discursive strategies to shape its narrative and regulatory framework, effectively restricting free speech. By using Nominalization strategy, the law reduces and dehumanizes actions by turning them into nouns (e.g., "unauthorized access," "glorification of an offence"), which helps obscure accountability and understand exactly participating in what behaviors is prohibited. Use of Argumentation strategies focus on the threat and security of cybercrime, emphasizing the immediate hazard to public safety and the necessity of legislation to mitigate this harm. Legitimation strategies include appealing to authority by citing reputable organizations and court decisions, and reassuring stakeholders and the general public about the dependability and enforcement of the legislation.

Historical and intertextual references highlight the need for new legislation by pointing out the inadequate earlier laws. Ethical and moral arguments appeal to morality by portraying cybercrimes as morally repugnant acts that injure both people and society as a whole. The importance of discourse presentation and framing lies in their ability to affect public perception, gain legitimacy and authority, conform to social norms, and ensure accurate policy implementation. The language of the legislation affects how the public views it, emphasizing its need and urgency, increasing public support for the

law. By presenting the law in a discourse-based manner, it gains legitimacy and authority, increasing public acceptance and the ability of authorities to enforce it.

Vague general terms like 'spreading false information' and 'cyber terrorism' mean that it's a vague grey area in law, allowing them to be applied as they like, which is a high bar for public companies to cross in open expression. By using framing and Perspectivation the law frames online behavior that the state regards as threats to public safety and morality, and frames the regulatory action of the state as protective, to maintain order. The use of mitigation by law aims to play down issues of government overreach by stressing the law enforcer's responsibility in maintaining public order, and the advantages of cybercrime prevention in order to justify increased surveillance and controls on digital communications. Criminalization of Expression in PECA 2016 criminalizes all manner of thought and speech online from sharing opinions to sharing information through the simple act of dissemination, which could be construed as harmful or threatening.

Each discursive strategy embeds these embedded ideologies and power dynamics that enable the justification of regulatory control over digital spaces. PECA 2016 prohibits freedom of speech by abstracting actions, presenting regulations as protective, and criminalizing wide varieties of communication rights, and assists self-censorship in Pakistan, damaging the right to free speech.

4.2. Analysis of PECA Ordinance 2022

The Committee considered the PECA 2016 clause by clause and made the following amendments in the Bill: Clause Number 1, 2, and 4 were amended by the Committee. The Title of the Bill has been changed to "Prevention of Electronic Crimes Act, Ordinance (Amendment)", 2022." Insertion of following new paragraphs in section #2 of PECA, 2016 was made. The amended Bill by the Committee is as under:

(vi-a) "Child" means any person who is not more than eighteen years" Amended by the Committee as under

(vi-b) "Child sexual abuse content" means the representation, by whatever means, of a child engaged in' real or simulated sexually explicit conduct or representation of the sexual part§ of a child for primarily sexual purposes."

(vii-a) Not agreed by the Committee

(xxiv-a) Not agreed by the Committee (xxvii-a) Not agreed by the Committee

(xxviii-a) Not agreed by the Committee Amendment of existing section 22 of PECA, 2016. Amended by the Committee as under: Child • pornography.

(1) Whoever intentionally produces, offers or intakes available, distributes or transmits through an information system or procures for himself or for another person or without lawful justification possesses material in an information system, that visually depicts,

- (a) a minor engaged in sexually explicit conduct '
- (b) a person appearing to be a minor engaged in sexually explicit conduct; or
- (c) realistic images representing a minor engaged in sexually explicit conduct; or
- (d) discloses the identity of the minor, shall be punished with imprisonment for a term which may extend to fourteen years but shall not be less than three years, or with fine which may extend to five million rupees or with both.
- (e) Insertion of new section 22-A in PECA, 2016: solicitation and cyber enticement not agreed by the Committee, Online insertion of new section 22-B in PECA, 2016

4.2.1. Linguistic Co -Text in PECA Ordinance 2022

The Prevention of Electronic Crimes (Amendment) Ordinance, 2022 (PECA Ordinance 2022) contains several key terms and phrases that are crucial for understanding its scope and implications. Here are some examples of linguistic context used in the ordinance, along with their meanings and suggested interpretations:

1. **Electronic Communication:** Refers to any communication transmitted in electronic form, such as emails, text messages, and social media posts. This term is used to define the scope of the ordinance in regulating digital interactions.
2. **Cybercrime:** Encompasses illegal activities conducted through digital means, including hacking, identity theft, and online fraud. The ordinance aims to address and penalize such activities to enhance cybersecurity.
3. **Defamation:** The act of making false statements that harm someone's reputation. Under PECA, defamation is criminalized, and the ordinance specifies penalties for those found guilty of defaming others online.

4. **Public Figure:** Refers to individuals holding public office or those who are prominent in public life. The ordinance extends the scope of defamation laws to include public figures, aiming to protect their reputations from false accusations.
5. **Non-Consensual Sharing of Intimate Images:** The unauthorized distribution of private or intimate images of individuals. This term is included to address the issue of "revenge porn" and protect individuals from such violations.
6. **Cognizable Offense:** A serious crime for which a police officer can arrest without a warrant. The ordinance categorizes certain offenses, such as cyber terrorism and child pornography, as cognizable offenses to ensure swift action.
7. **Non-Bailable Offense:** Crimes for which bail is not granted as a matter of right. The ordinance designates certain offenses, including online defamation, as non-bailable to emphasize their severity.
8. **Content Moderation:** The process of monitoring and regulating user-generated content on digital platforms to ensure compliance with legal and ethical standards. The ordinance addresses the role of content moderation in preventing cybercrimes.
9. **Cyber Terrorism:** The use of digital means to conduct terrorist activities, such as spreading propaganda or coordinating attacks. The ordinance includes provisions to combat cyber terrorism and protect national security.
10. **Child:** means any person who is not more than eighteen years of age.
11. **Child Pornography:** The illegal creation, distribution, or possession of explicit images of minors. The ordinance includes stringent measures to prevent and punish such activities to protect children from exploitation.
12. **"Child sexual abuse content"** means the representation, by whatever means, of a child engaged in real or simulated sexually explicit conduct or representation of the sexual parts of a child for primarily sexual purposes."

These terms and phrases are integral to understanding the legal framework established by the PECA Ordinance 2022. They reflect the ordinance's focus on regulating digital spaces, protecting individuals from online harm, and ensuring cybersecurity.

4.2.2. Use of Discursive Strategies in PECA Ordinance 2022

To evaluate the use of referential strategies based on the framework of Ruth Wodak, a helps to identify and analyze certain ways of building up social realities and power relations among communities. The five major reference strategies include: nomination, predication, argumentation and intensification.

Ruth Wodak's Discourse-Historical Approach is recursive of social processes, historical background, and practices of discourse. Since the pillars of Wodak 's DHA are historical context, social processes and discursive practices therefore these three dimensions are used to analyze the Prevention of Electronic Crimes Act (PECA) Ordinance 2022. The first dimension under analysis is its content. The Second is to see the modes of discursive formation or discursive interpretations that the document has contained. Third is to see how it is related to common affairs or the world around it at a particular time in a particular place. The detailed analysis is as follows:

4.2.2.1. Use of Predication Strategy

Predication involves attributing qualities to social actors, actions, and phenomena. In PECA Ordinance 2022, the terms "offenders" and "cybercriminals" are predicated with negative attributes such as "malicious" and "harmful." This framing helps to justify the stringent measures and penalties imposed to protect public safety. Predication Strategy is the linking of an element with a social actor quality of a trait of an attribute The use of this strategy can be easily noted in the kin descriptions of who the wrongdoers are and what they have done consider the following text as example from PECA Ordinance 2022: Consider the following example from the text of PECA Ordinance 2022.

“Any person who [commits the offence of cyber terrorism and interferes or threatens to interfere] knowingly with the operation of an asset or facility of major significance or with access to it shall be liable to imprisonment for a term not exceeding fourteen years.

4.2.2.2. Use of Referential Strategy

Referential strategies define, construct, and represent social actors. PECA uses referential terms like "aggrieved person," "public figure," and "holder of public office"². These terms draw on positive associations, suggesting that the ordinance aims

to protect the rights and reputation of these figures, while implicitly framing dissent as potentially unlawful.

4.2.2.3. Use of Perspectivation Strategy

This strategy involves positioning, opinions, and attitudes. PECA Ordinance 2022 portrays the government as a guardian of public order and morality, emphasizing the need for digital surveillance. Phrases like "ensuring public safety" and "maintaining public order" perspectivize the state's role as protective, justifying the ordinance's strict control over digital communication.

4.2.2.4. Use of Argumentation Strategies

PECA Ordinance 2022 uses argumentation strategies to legitimize its provisions. By arguing that cybercrimes disrupt public order and harm national security, statements like "unauthorized access" and "spreading false information" are constructed as serious threats requiring severe penalties and a tight control framework. The ordinance's themes include cybersecurity and prevention of cybercrimes like cyberstalking, cyberbullying, cyber radicalization, and fake news/hate speech; the correlation of Freedom of Speech in Pakistan, specifically the limitations to the freedom of speech and its possible abuse against opponents of the current establishment; avenues for Legal Regulation and Execution- investigative agencies, legal channels to deal with electronic crimes.

Examples of use of Argumentation Strategies in PECA Ordinance 2022:

1. Legitimization: The ordinance legitimizes itself as cyber threats increase and Citizens ' rights as a group to life and liberty are infringed upon. Authority**: By appealing to legal precedents, international norms & experts ' opinions, this ordinance seeks to make itself law in the eyes of everyone involved.
2. Fear and Threat: It stresses the hazards cybercrimes pose and how they can put national security or public order at risk.
3. Security versus Freedom: In such discourse, computer security is portrayed as a trade-off needed to maintain order — some people's liberty must inevitably be suppressed for the protection of society as a whole.
4. Whether defenders of the law named and shamed you as a criminal mastermind, or quite different kinds of people were split apart to take sides thus conforming

themselves into victims and persecutors will determine this TV drama's rating in future years.

5. Based on the provisions of the PECA Ordinance 2022 which says:
6. "If businesses wish to have their data safe and unchanged, then, there should be higher control mechanisms in place and organizations should not allow any access or threats from the cyber world". The argumentation here is that this Topos of Security shields data honesty with proper measures.

4.2.2.5. Mitigation and Intensification in PECA Ordinance 2022

Intensification strategies amplify certain elements to emphasize their importance. PECA Ordinance 2022, intensifies the threats posed by cybercrimes by using phrases like "increasing punishment" and "severe consequences." This creates a sense of urgency and necessity for stringent measures. Whereas the use of mitigation strategies softens the perception of certain actions. In PECA, mitigation is evident in the language that downplays concerns about the ordinance's broad provisions. By emphasizing the importance of public safety and security, these measures are presented as necessary evils rather than oppressive regulations.

Example 1:

"A temporary measure will be in place while we explore more permanent solutions."

Here, "temporary measure" and "explore more permanent solutions" mitigate the possible concerns or fears about the permanence of a potentially unpopular decision.

Intensification strategies, on the other hand, are used to emphasize or exaggerate the impact of a statement. They can make an argument more compelling or urgent.

In this example, the phrase "to ensure the safety of citizens and to protect national interests" mitigates the potential criticism that the ordinance may be infringing on personal freedoms by emphasizing positive intentions.

Example 2:

From the PECA Ordinance 2022:

"Immediate action is necessary to counter the severe threats to national security."

The terms "immediate action" and "severe threats" intensify the sense of urgency and gravity of the situation, persuading the audience that the measures are justified.

Example 3:

"The results were undeniably catastrophic, leaving no room for doubt about the necessity of our response."

Here, "undeniably catastrophic" and "leaving no room for doubt" are used to intensify the negative outcomes and the necessity for an immediate and strong response.

In both examples from the PECA Ordinance 2022, mitigation and intensification strategies are used to shape the audience's perception and reaction. By mitigating, the text seeks to downplay potential negative reactions or criticisms, while intensification aims to strengthen the argument and evoke a stronger emotional response.

These strategies are essential tools in political and legal texts where the authors need to balance between justifying their actions and controlling public perception.

Mitigation implies the effect of the ordinance on free speech in a minimalist presentation while including checks and balances in it. Whereas, intensification helps emphasize the range of threats that affect the majority of targets and their extremity, those are in a position to gain public support for strict measures against cyber threats.

4.2.2.6 Analysis of Use of Discursive Strategies in PECA Ordinance 2022

These discursive strategies collectively construct PECA 2022 as a necessary law to curb cybercrimes and protect social order. When attempting to analyze the relationship between cybersecurity and fundamental rights while using the PECA Ordinance 2022, it is pertinent to apply Ruth Wodak's DHA or discursive humanistic analysis to determine the effects of cybersecurity policies on freedom of speech. The use of discursive strategies reveal how the ordinance is constructed and justified.

However, by employing predication, referential strategy, and Perspectivation strategy. The ordinance frames dissenting voices as threats. The broad and vaguely defined terms obscure agency and responsibility, leading to potential misuse and self-censorship. Ultimately, PECA's discursive strategies contribute to a climate where free speech is restricted under the veil of public safety and security. The PECA Ordinance 2022 which contains enunciates these strategies does not only define any crime concerning electronic crimes but also associates such a crime with the gravity of such offences and their proper suppression through aggressive legal interventions. This corresponds with Wodak (Discourse) in the sense that it explains how discourse intervenes with the building of the social and political worlds.

Applying Ruth Wodak's DHA to the PECA Ordinance 2022, there is a complex interplay between the need for cybersecurity and protection of fundamental rights. Content analysis via applying Ruth Wodak's DHA model highlights key themes and participants, while discursive strategies show how the ordinance is framed and defended. Analysis emphasizes the historical, social, and political factors that shape this discourse around an ordinance.

The implications of PECA Ordinance (Public Enterprises Control Act) 2022 can be better understood for social governance and individual freedom by its analysis using Ruth Wodak's discursive strategies.

CHAPTER 5

FINDINGS AND CONCLUSION

Technological advancements worldwide have made it essential for nations to come up with proper legislation on cybercrime. PECA was enacted in Pakistan in 2016. The appearance of new advanced media forms such as digital platforms requires an appropriate legal framework that can protect individuals' digital rights. However, the introduction of PECA in 2016 provoked controversy where stakeholders termed it as an 'incoherent cocktail of anti-free speech, anti-privacy and anti-internet provisions.' Concerning the Constitution of the Islamic Republic of Pakistan, this review sheds light on PECA concerning the articles where fundamental rights guaranteed by the Constitution of Pakistan 1973.

5.1. Findings of the Research

The law named PECA 2016 was introduced to combat cybercrime, control activities on social networks, and shield against electronic offences in Pakistan. It sought to address problems like cyberbullying, harassment, identity theft as well as unauthorized access to information. However, long-standing political freedom was a prospect, and controversy started to occur concerning the suppression of freedom of speech and rebellion. The textual analysis of PECA 2016, and its amendment through the PECA Ordinance 2022, revealed the following concerns related to several textual, social and discursive practices in PECA 2016 that made its amendment in the form of PECA Ordinance 2022 necessary. Applying Ruth Wodak's Discourse Historical Approach concerning PECA 2016 and PECA Ordinance have the following findings providing answer to research Question no.1.as under:

5.1.1. Textual, Social and Discursive Practices in PECA, 2016

1) Textual Practices in PECA 2016

Terms like 'hate speech,' 'offensive communication,' and 'cyber terrorism' are all very ambitiously worded. Such terms do not have definitive definitions and so are only subjectively defined and selectively enforced. By leaving this term textual vague, it has the chilling effect on free speech since people begin self-censoring in order to avoid potential liability. For example, terms like 'offensive communication' are interpreted

variably, rendering the words ambiguous in application. That the textual practices involved in PECA 2016 included sections that defined defamation of “natural persons” as a criminal offence. These provisions were rather vague and pertained to prosecution where the offence had been committed through statements made on the internet that tend to bring harm to the subject’s reputation. However, the law did not differentiate between criticism of the government bodies or institutions.

2) Social Practices in PECA 2016

The enactment of PECA 2016 was highly influenced by the socio political context in which it was enacted. Underlying power dynamics and control mechanisms are represented by disproportionate use of the law against activist, dissenting voices, journalists and political opponents. Selective enforcement of this legislation erodes the credibility of the legislation and instils fear of not protecting free speech and human rights. Socially, PECA 2016 was condemned for being oppressive and the suppression of the freedom of speech. Activists, independent journalists, human rights defenders, as well as political opponents experienced threats of being prosecuted for their work. The law was applied to give clamp down on voices of dissent under the guise of eradicating fake news and cybercriminals.

3) Discursive Practices in PECA 2016

This framing of PECA 2016 as necessary for national security and public order provides the reason to undertake extremely harsh measures and mass surveillance. The state takes up a protective role in the 'nation', on 'public order', making permissible only discourse defined within the free expression space. However, this narrative treats the government as this guardian of public welfare, which may then construct the basis for regulation over digital activities.

Among other linguistic strategies, the ordinance normalizes and mitigates. Nominalization is the naming of actions as abstract nouns; the key effect of this is to foreground the generalized threat rather than how it is acted out by specific individuals. So, for example, terms like 'cyber terrorism' are vital because they nominalize the concept and focus on perceived threat, not the individual accountable for it. Focusing on the positives the law may do and why regulation helps us collectively, as a society or a nation, mitigative language seeks to frame law as protection, not oppression.

Such practices therefore call for amendments to PECA 2016 to strike a reasonable balance between regulatory provisions and preserving fundamental rights. Selective enforcement and subjective interpretation of the law require more defined standard and stricter oversight of their enforcement predispose the right of free speech and fair application.

5.1.2. Fulfillment of Free Speech Conditions in Ordinance 2022 of PECA

Applying Ruth Wodak's Discourse Historical Approach to the text of PECA Ordinance 2022 has led to the following findings answering Question no.2 of the research as follows:

Later, on February 18, 2022, the Pakistani government approved an ordinance to amend PECA 2016. New defamatory sections were introduced broadening the critique of government bodies and the military. In its place, it brought into notice a new definition of the word person which included institutions formed by the government. An action for defamation was termed as a serious offence one with which a person could not bail out, in addition to raising the maximum years for imprisonment from the current three to the current five years. Pursuers of defamation could be anyone including an institution with criminal proceedings being set in motion.

Some of the amendments under PECA Ordinance 2022 intended to remedy the shortcomings of PECA 2016 and imply greater protection of free speech include:

- i) **Clarified Definitions:** More precise definitions are given for terms such as "hate speech," "cyber terrorism" and "offensive communication," the ordinance adds. Having a clear meaning reduces the risk of ambiguities, and subsequent misuse of the law, thereby making the law less ambiguous and more consistently and fairly applicable. For example, the term hate speech is now defined, with strict criteria, so that it is not subject to the influence of the policymakers' mood or political correctness, and cannot be enforced selectively.
- ii) **Balanced Provisions:** The new provisions seek to strike a middle ground between regulatory statutes and protecting free speech, by including explicit provisions to protect against unreasonable censorship and overreach. In these clauses, protecting fundamental rights comes first, alongside legitimate security concerns. For example, the ordinance includes provisions which protect

journalists and activists from being subjected to further legal action and protect free expression.

- iii) **Enhanced Oversight:** The PECA Ordinance 2022 set clearer oversight, accountability mechanism to prevent abuse and to ensure fair application of the law. Independent review bodies and periodic audits of enforcement practices are among these mechanisms. These choices have enhanced oversight is in service of building public trust that human rights principles are applied with few inconveniences.

Proportional Penalties: The ordinance likens punishment to crime, with penalizing cyber offenses on a proportional scale. The purpose of this proportionality is to thwart the abuse of legal measures against dissenting voices in an unduly high number. Thus, minor offenses including 'spreading false information,' have differentiated penalties from major offenses like 'cyber terrorism.'

- iv) **Focus on Rehabilitation:** The ordinance also puts more burden on rehabilitating and educating the offenders and therefore dealing with cybercrimes more holistically. They aim to focus on rehabilitation to reduce recidivism and promote a more responsible digital citizenship. They are expected to provide a more enabling environment for free expression, and a due response to legitimate security concerns. Explicit definitions and further oversight mechanisms for the use of legal provisions were especially important to prevent the illegal use of legal provisions and to protect fundamental rights.

This amendment was a breach of Pakistan's human rights conventions, especially concerning freedom of speech. Lack of consultation and public scrutiny is another aspect that faced negligence in the case of PECA, Ordinance 2022 as well. The government deliberately ignored to consult civil society groups and the private sector on the amendments. This resulted in the lack of transparency in the aforementioned legislation even before its enactment.

Cybersecurity and free speech continue to be a problem; there is a need to keep on debating.

Furthermore, the regulation of the PECA 2016 and its subsequent amendments reveals the conflict between the idea of managing the internet fiduciaries and the

protection of human rights. However, freedom of speech has been widely regarded and debated under the impact of the said amendment.

The PECA Amendment Ordinance 2022 was passed in February 2022, to address the perceived shortcomings in the 2016 Pakistan Electronic Crimes Act (PECA). Concerning its effect on freedom of speech, it has elicited some controversy. The PECA 2016 intended to fight cybercrimes, control online activities and prevent electronic offences. It covered principles like cyberbullying, harassment, identity theft, and unlawful access to data among others.

Nevertheless, controversy began over whether it would hinder freedom of speech and freedom of dissent. The amendment agenda of the PECA was in response to a new form of emerging threats and challenges to technological advancements by balancing the freedom of speech and the security of cyberspace. The amendment increased the coverage of defamation laws to incorporate the criticism of government organs such as the military and judiciary. It outlawed all cases of cyber-bullying of political and other powers by the public, and severe consequences were enacted.

The public officials and state entities have less protection for defamation as compared to the past while the private persons can get prepared for not being discussed or slandered in the public domain. It was intended to improve the protection of cyberspace, but it provoked criticism concerning the limitation of freedom of speech. As far as Constitutional considerations of the legislation (2022) is concerned, it is worth mentioning that renowned Justice of Pakistan Athar Minallah of Islamabad High Court (IHC) has declared the PECA Ordinance as unconstitutional.

Article #19 of the constitution addresses freedom of speech; fundamental rights are provided by articles #9 and #14. It provided special emphasis on the fact that the right to free speech and the right to receive information is an important requisite for societal progress and prosperity.

Such suppression of rights was also considered outlawed under the PECA ordinance due to the violation of democracy. It rendered to practically criminalize, defame and safeguard reputations through arrest and imprisonment carried negative consequences. Citizens including journalists, human rights defenders, and political opponents were at risk of being prosecuted for speaking out.

To strengthen its campaign, media associations moved to court to challenge the constitutionality of the PECA ordinance 2022, especially on the grounds of infringement of press freedom.

The Islamabad High Court quashed the PECA Amendment Ordinance 2022 and the Ministry of Information put a succinct message across stressing that the former was null and void beyond any reasonable doubt. The court directed an inquiry against the FIA's Cyber Crime wing and the police for torturing the suspects. This verdict was seen as a landmark in Pakistan's history to have people their freedom of speech back.

5.2. Conclusion

Freedom of media and independence of media are vital in the process of developing democracy as well as the rule of law. The weighing of cybersecurity and freedom of speech is to date an area of contention, and thus it will always be a topic of discussion and further policy changes. Therefore, it is quite evident that the PECA Amendment Ordinance 2022 sought to achieve the mean between cybersecurity and freedom of speech. However, theoretical provision for it was seen as having precarious effects on the protection of expression. The recent court verdict meant that protecting rights and guaranteeing freedoms must be applied together with countering cyber threats. Conclusively, Pakistan has to move forward on the path of a sound democracy, where both, security and civil liberties are upheld. Legislative language has, and continues to be, shaped out of, and in turn, helps shape the socio political context of ETO 2002, PECA 2016 and PECA Ordinance 2022 through a critical discourse analysis of their text. Fundamentals of these findings are that they underscore that legal frameworks need to be continuously refashioned while remaining relevant and effective in the evolving digital landscape. With the passage of PECA Ordinance 2022, free speech protection is moving towards better protection of rights with the removal of past oversights. But vigilance will need to continue and some further amendments may need to be made in order to retain that balance between regulation and freedom.

5.3 Suggestions for Future Researchers

Following the completion of a critical discourse analysis (CDA) of the Electronic Transactions Ordinance 2002 (ETO 2002), the Prevention of Electronic Crimes Act 2016 (PECA 2016), and PECA Ordinance 2022 using Ruth Wodak's Discourse-Historical Approach (DHA) some possible avenues can be identified to

explore for the future researchers The goal of these recommendations is to direct future researchers in furthering this study in future, exploring other dimensions of free speech and digital governance in Pakistan and adding upon the existing knowledge. For instance,

1) Comparative Inter-Subject Studies

Future researchers can go on to compare the laws of various countries and do more discourse analysis to this end. This will give a more general view on perceptions of how different legal systems meet digital communication and freedom of expression issues, demonstrating not only where Cross-cultural distinctions exist in implementation but also connecting similar policies with others elsewhere in more detail.

An investigation of the evolution of electronic crime laws over an extended period can provide insight into how socio-political changes are reflected in legal texts. Going forward, it might be possible to follow amendments and modifications to the ETO, PECA 2016, and subsequent ordinances over time—gaining ideas into the dynamic relationship between changes in policy and emerging digital threats. Scholars need to carry out research on how these laws affect digital rights and civil liberties. Empirical research in this field might include case-law analysis, interviews with victims of law enforcement investigation and public opinion survey results. Such work is essential for gaining insight into just what these regulations do to free speech or privacy in practice.

2) Alignment with International Human Rights Norms

By comparing Pakistan's act of cybercrime law to right to freedom of expression and privacy standards under international human rights law, new research can provide insight into the global significance of one country's domestic laws. This research might generate policy proposals that serve in the cause of international law.

3) Technological Advances Meet Legal Innovation:

As technology changes swiftly now is the time to study how regulatory frameworks keep up with new electronic realities. Future research should focus

on regulatory readiness calibrated to keep pace with technological environments such as artificial intelligence.

4) Public and Media Discourse Analysis

Study of the public and media discourse that surrounds the enactment and enforcement of these laws is an important way to get to know society's attitudes toward and response this time around. This approach can help us understand its bigger ripples on society as well as how right the media has been playing a role in formation of law on digital legislation.

5) Focus on Marginalized Groups

Future researchers should explore how these cybercrime laws impact marginalized groups, including minorities, activists and journalists. This can reveal potential bias and disproportionate effects, paving the way for better policy recommendations.

6) Policy Recommendations and Advocacy

Building on the research results, future studies should work to forge specific policy ideas that develop information security solutions compatible with free speech protections. Support from decision makers, legal scholars and civil society organizations will help these research findings become practical policy change.

By working through these options, future researchers can continue to promote understanding of the nature of dialogue between electronic crime laws and freedom of speech, and contribute towards a more balanced judge for digital age laws.

7) Ethnographic Studies on Digital Practices

The study of how people and communities use digital spaces in the face of these laws under the lens of digital governance via ethnographic studies of such places of actual human interaction with digital governance can provide a more grounded perspective of the lived lives with digital governance. Ethnographic methods enable researchers to capture the practices, problems and problem solving users face as they go about using the law and digital technology to solve their problems.

5.4 Conclusion

These recommendations for future researchers will contribute to a better view of the legislation under study on free speech and digital governance in Pakistan. The following research avenues provide both avenues to new dimensions of digital and regulations to address new challenges and reform the policy making in a balanced and just manner, the legislative space of the cybercrimes in Pakistan is evolving rapidly. The application of Ruth Wodak's Discourse Historical Approach, which offers a nuanced analysis regarding the impact of these laws on free speech and digital governance. The results confirm the need to strike a delicate balance between the respective regulatory measures in place and protecting fundamental rights. Future researchers can add to the existing research, by using more dimensions as a point of interest to explore, and partake in a legal practice that is more equitable and effective in relation to supporting security and freedom by incorporating the proposed recommendations.

REFERENCES

- Ahmadvand, M. (2014). Critical discourse analysis: An introduction to major approaches. *Dinamika Bahasa Dan Budaya*, 5(1), 82–90.
<https://www.unisbank.ac.id/ojs/index.php/fbib1/article/view/382>
- Amoussou, F., & Allagbe, A. (2018). Principles, theories and approaches to Critical Discourse analysis. *International Journal on Studies in English Language and Literature*, 6(1). <https://doi.org/10.20431/2347-3134.0601002>
- Baker, P., Gabrielatos, C., KhosraviNik, M., Krzyżanowski, M., McEnery, T., & Wodak, R. (2008). A useful methodological synergy? Combining critical discourse analysis and corpus linguistics to examine discourses of refugees and asylum seekers in the UK press. *Discourse & Society*, 19(3), 273–306.
<https://doi.org/10.1177/0957926508088962>
- Brooks, P. (2005). *Narrative and law: The risks of storytelling in legal discourse*. Yale University Press.
- Brooks, R., & Gewirtz, S. (2005). *The narrative turn in social research: Implications and challenges*. Palgrave Macmillan.
- Buetow, S. (2018). Apophenia, unconscious bias and reflexivity in nursing qualitative research. *International Journal of Nursing Studies*, 89, 8–13.
<https://doi.org/10.1016/j.ijnurstu.2018.09.013>
- Bukhari, N. H. (2013). Critical discourse analysis and educational research. *IOSR Journal of Research & Method in Education (IOSRJRME)*, 3(1), 09–17.
<https://doi.org/10.9790/7388-0310917>
- Campbell, C. (2008). Foucault, psychology and the analytics of power. *Journal of Community & Applied Social Psychology*, 18(6), 645–646.
<https://doi.org/10.1002/casp.994>
- Chiluwa, I. (2012). Citizenship, participation, and CMD. *Pragmatics and Society*, 3(1), 61–88. <https://doi.org/10.1075/ps.3.1.03chi>
- Chomsky, N. (1992). Explaining language use. *Philosophical Topics*, 20(1), 205–231.
<https://doi.org/10.5840/philtopics19922017>
- Corridor, J., & Gilroy, P. (1990). *Language and trial: The dynamics of written and spoken communication in legal settings*. Cambridge University Press.

- Cotterill, J. (2003a). Language and power in court. In *Palgrave Macmillan UK eBooks*. <https://doi.org/10.1057/9780230006010>
- Cotterill, J. (2003b). Macro-, micro- and multiple narratives: Storytelling in court. In *Palgrave Macmillan UK eBooks* (pp. 19–64).
https://doi.org/10.1057/9780230006010_3
- Coulthard, M., & Johnson, A. (2007). *An introduction to forensic linguistics: Language in evidence*. Routledge. https://pasca.uns.ac.id/s3linguistik/wp-content/uploads/sites/44/2016/10/Malcolm_Coulthard_Alison_Johnson.pdf
- Crystal, D. (2003). *The language of authority: How language conveys power in law and legislation*. Oxford University Press.
https://culturaldiplomacy.org/academy/pdf/research/books/nation_branding/English_As_A_Global_Language_-_David_Crystal.pdf
- Daudpota, F. (2016). An examination of Pakistan's cybercrime law. *SSRN Electronic Journal*. <https://doi.org/10.2139/ssrn.2860954>
- Jenks, C. J. (2020). *Researching classroom discourse: A student guide*. Routledge.
<https://doi.org/10.4324/9780429264023>
- Earley, C. L. (2009). *Popular political participation in the late Roman Republic* [PhD Dissertation, Victoria University of Wellington].
<https://doi.org/10.26686/wgtn.16968259.v1>
- Eboibi, F. E. (2017). A review of the legal and regulatory frameworks of Nigerian Cybercrimes Act 2015. *Computer Law & Security Review*, 33(5), 700–717.
<https://doi.org/10.1016/j.clsr.2017.03.020>
- Fairclough, N. (1989). *Language and power*. Longman Group UK Limited.
https://www.okehamptoncollege.devon.sch.uk/uploads/6/1/4/4/61443371/ebooksclub.org_language_and_power_language_in_social_life_.pdf
- Fairclough, N. (1994). *Critical discourse analysis: The critical study of language* (2nd ed.). Longman. <https://www.felsemiotica.com/descargas/Fairclough-Norman-Critical-Discourse-Analysis.-The-Critical-Study-of-Language.pdf>
- Fairclough, N. (2009). A dialectical-relational approach to critical discourse analysis in social research. In R. Wodak & M. Meyer (Eds.), *Methods of critical discourse analysis* (2nd ed., pp. 162–187). Sage.
https://www.researchgate.net/publication/285130079_A_dialectical-relational_approach_to_critical_discourse_analysis_in_social_research

- Firestone, W. A. (1987). Meaning in method: The rhetoric of quantitative and qualitative research. *Educational Researcher*, 16(7), 16–21.
<https://doi.org/10.3102/0013189x016007016>
- Flowerdew, J., & Richardson, J. E. (2017). *The routledge handbook of critical discourse studies* (1st ed.). Routledge. <https://doi.org/10.4324/9781315739342>
- Fowler, C. A., Levy, E. T., & Brown, J. M. (1997). Reductions of spoken words in certain discourse contexts. *Journal of Memory and Language*, 37(1), 24–40.
<https://doi.org/10.1006/jmla.1996.2504>
- Gibbons, J. (2008). Questioning in common law criminal courts. In J. Gibbons & M. T. Turell (Eds.), *Dimensions of Forensic Linguistics* (pp. 115–130). John Benjamins Publishing Company. <https://doi.org/10.1075/aals.5.09gib>
- Haque, J. (2013). Pakistan's internet landscape. In *Bytes for All*. Bytes For All. Retrieved May 18, 2025, from <https://www.bytesforall.pk/publication/internet-landscape-pakistan-2022>
- Kamal, D. (2017, January 18). *A comparative analysis of the Prevention of Electronic Crimes Bill*. Jinnah Institute. <https://jinnah-institute.org/publication/policy-brief-a-comparative-analysis-of-the-prevention-of-electronic-crimes-bill/>
- Kattakayam, J. J. (2006). Power and knowledge: Some reflections on contemporary practices. *Sociological Bulletin*, 55(3), 449–467.
<https://doi.org/10.1177/0038022920060306>
- Khaghaninejad, M. S. (2015). Political practice of literary analysis: How to read literature more closely. *International Letters of Social and Humanistic Sciences*, 49, 92–105. <https://doi.org/10.18052/www.scipress.com/ilshs.49.92>
- Khan, S., Tehrani, P. M., & Iftikhar, M. (2019). Impact of PECA-2016 provisions on freedom of speech: A case of Pakistan. *Journal of Management Info*, 6(2), 7–11. <https://doi.org/10.31580/jmi.v6i2.566>
- Kundi, G. M., Nawaz, A., & Akhtar, R. (2014). Digital Revolution, Cyber-Crimes and Cyber legislation: A challenge to governments in developing countries. *Journal of Information Engineering and Applications*, 4(4), 61–70.
<https://www.iiste.org/Journals/index.php/JIEA/article/view/12430>
- Mailland, J. (2000). Freedom of speech, the internet, and the costs of control: The French example. *SSRN Electronic Journal*, 33, 1179–1234.
<https://papers.ssrn.com/sol3/Delivery.cfm?abstractid=1578402>

- Majumder, A. (2017). Gayatri Spivak, planetarity, and the labor of imagining internationalism. *Meditations*, 30(2), 15–28.
https://mediationsjournal.org/files/Meditations30_2_02.pdf
- Ramazan, M., Javaid, K., Iqbal, T., & Buksh, I. (2019). Freedom of speech: Infringement of women rights in Pakistan. *SAUSSUREA*, 9(1), 28–38.
https://www.researchgate.net/publication/330713373_Freedom_of_Speech_Infringement_of_Women_Rights_in_Pakistan
- Rogers, R., Malancharuvil-Berkes, E., Mosley, M., Hui, D., & Joseph, G. O. (2005). Critical discourse analysis in education:: A review of the literature. *Review of Educational Research*, 75(3), 365–416.
<https://doi.org/10.3102/00346543075003365>
- Saeed, R. (2020). Role of media of Pakistan in “Freedom of Speech”: A survey of Lahore District. *Global Multimedia Review*, 3(1), 39–51.
[https://doi.org/10.31703/gmmr.2020\(iii-i\).04](https://doi.org/10.31703/gmmr.2020(iii-i).04)
- Said, E. W. (2016). *Orientalism: Western Conceptions of the Orient*. Penguin UK.
- Sajjad, F., Malghnai, M., & Khosa, D. (2017). Language, social media and Political Identity (Re)presentation:: A new theoretical framework for the analysis of social media political discourse. *International Journal of English Linguistics*, 8(2), 199. <https://doi.org/10.5539/ijel.v8n2p199>
- Schlesinger, A. M., & Wilentz, S. (2007). *The Politics of hope and the bitter heritage: American liberalism in the 1960s* (Vol. 5). Princeton University Press.
<http://ci.nii.ac.jp/ncid/BA84985714>
- Siddique, O., & Hayat, Z. (2008). Unholy speech and holy laws: Blasphemy laws in Pakistan-controversial origins, design defects, and free speech implications. *SSRN Electronic Journal*, 17(2), 303–385.
https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2207002#
- Van Dijk, T. A. (1993). Principles of critical Discourse analysis. *Discourse & Society*, 4(2), 249–283. <https://doi.org/10.1177/0957926593004002006>
- Weiss, G., & Wodak, R. (Eds.). (2007). *Critical discourse analysis*. Palgrave Macmillan.
- Whitaker, B. E. (2005). Citizens and foreigners:: Democratization and the politics of exclusion in Africa. *African Studies Review*, 48(1), 109–126.
<https://doi.org/10.1353/arw.2005.0047>

- Wodak, R. (2009). The semiotics of racism: A critical discourse-historical analysis. In *John Benjamins Publishing Company eBooks* (pp. 311–326).
<https://doi.org/10.1075/z.148.29wod>
- Wodak, R. (2011). Language, power and identity. *Language Teaching*, 45(2), 215–233. <https://doi.org/10.1017/s0261444811000048>
- Wodak, R. (2014). Critical discourse analysis. In G. Hornberger & R. N. Anderson (Eds.), *The Routledge companion to English studies* (pp. 302-316). Routledge.
<https://doi.org/10.4324/9781315852515-22>