Journal of Sociology & Cultural Research Review (JSCRR)
Available Online: https://jscrr.edu.com.pk
Print ISSN: 3007-3103 Online ISSN: 3007-3111
Platform & Workflow by: Open Journal Systems

CYBERSECURITY LEGISLATION AND GLOBAL STANDARDS: A COMPARATIVE ANALYSIS OF PAKISTAN'S PECA 2016 AND UN GUIDELINES ON DISINFORMATION

Jawad Ishaq Rana
Assistant Professor, Media Studies at Iqra University Islamabad Campus.
Dr. Sarwat Rauf
Associate Professor of International Relations at the National University of Modern Languages (NUML), Islamabad.
ORCID is: 0000-0003-2239-6934

Abstract
This study examines Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 through the lens of the United Nations' guidelines on countering disinformation. It focuses on the relationship between cybersecurity and human rights. By employing Finnemore and Hollis' norm construction theory, the research evaluates the selective adoption of global norms by Pakistan and how the country prioritizes state security over individual freedoms. Using a qualitative content analysis, the study assesses PECA's alignment with UN standards on freedom of expression, transparency, and proportionality. The findings reveal that while PECA demonstrates strong cybersecurity provisions, its restrictive language and broad enforcement mechanisms limit adherence to international norms. This potentially leads to self-censorship and a "chilling effect" on free expression. This selective alignment highlights the influence of Pakistan's sociopolitical and security priorities on norm adoption thereby reflecting challenges in balancing digital rights with national security. The research highlights the need for policy reforms such as clearer legal definitions, enhanced transparency, and proportionate enforcement to align PECA with international standards. The study provides insights into the intricacies of integrating international norms into national regulatory frameworks. It aims to contribute to broader discussions on governance in the digital age.

Keywords: *PECA 2016, Disinformation Regulation, Freedom of Expression, Media Governance*

Introduction
The evolution of digital platforms has revolutionized how we communicate. The added factor of globalization has led to an exponential increase in our access to knowledge. Whereas information is now much easily and readily available, so is misinformation. Misleading information

which is designed to deceive is disinformation and it poses a global danger to public trust, democratic processes and human rights (Amnesty International, 2021). For a country like Pakistan, the consequences can be much more complex as disinformation closely correlates to the country's sociopolitical nature and security issues.

To address uncertainty in the cyber domain, the Pakistan government passed the Prevention of Electronic Crimes Act (PECA) (GoP, 2016) as an internet regulation mechanism and targets offences such as hate speech, deception, or crime. However, PECA has been criticized for having strict regulations or vague terminologies open for subjective interpretations (Khan, Tehrani, & Ifthikhar, 2019). For example, Section 20 discusses acts against dignity or Section 37 on unapproved internet information both highlight how these broad provisions can grant authorities such discretion to apply their own understanding. These could lead to potential overreach thus creating a "chilling effect" (Ó Fathaigh, 2019) on the freedom of expression.

The United Nation's Secretary General's Report on Countering Disinformation for the Promotion of Human Rights and Fundamental (2022) provides guidelines for countries to regulate disinformation, and it emphasizes protecting freedom of expression, transparency, and proportionality in enforcement. Pakistan is a UN member state and therefore comes under pressure to align with international standards. However, PECA's provisions places priority for state security over protection of individual rights.

This purpose of this study is to assess how aligned PECA is with guidelines provided by UN on disinformation. This is done by applying Finnemore and Hollis' Norm Construction Theory to analyze whether Pakistan adopts those guidelines fully, selectively, or absence of adherence to international norms. According to Finnemore and Hollis, states adopt cybersecurity norms according to their local priorities. This allows the states to adopt elements which align with their own sociopolitical contexts. Applying this theory, the study investigates Pakistan's control of digital space while adopting global norms of combating disinformation.

For this study, a qualitative content analysis is used with a structured rubric. It evaluates how PECA adheres to UN standards of freedom of expression, transparency and proportionality. The findings are as follows: PECA's focus on cybersecurity is strong; however, protection of rights is limited. This reveals selective alignment. It must be noted that a developing country like Pakistan isn't alone in this selective adoption of UN standards. Democracies such as the United States and Germany also face similar

criticism from organizations like Amnesty International (2021). This also shows that balancing security and human rights is a global struggle.

Although the study analyzes Pakistan's laws, the implications for this study sheds light on the challenges faced by states to integrate international norms within their regulatory frameworks. Furthermore, studying Pakistan's approach through the lens of Finnemore and Hollis' framework, this research highlights the subtleties and complexities of norm construction in matters of cybersecurity. The study will also recommend policies which can enhance how PECA can balance security with human rights.

Problem Statement

Disinformation is one issue in a globalized world which affects political stability, public trust, and human rights. Furthermore, even the United Nations admits that "There is no clear definition of, or shared common understanding and approach to, the term "disinformation". To address this issue, many governments have adopted legal measures as to how they can manage online information and counter cybercrime. Enacted in 2016, Pakistan passed the Prevention of Electronic Crimes Act (PECA) as a measure to target misinformation and offences related to the cyber domain. Regulations often face criticism and PECA is challenged that it infringes upon the rights of people to information, free speech, and transparency. There have also been recent amendments to the law which shows the shifting of priorities where digital risks have evolved while there are concerns for the state's growing control of online platforms.

In the 77th Session of the UN General Assembly, the United Nation's Secretary General's Report on Countering Disinformation was distributed. It provides a benchmark to advocate human rights, transparency in the procedures to deal with disinformation, and proportionate measures to deal with cybercrimes. A study is required to assess how PECA aligns with the UN's recommendations in light of a theoretical framework. Looking through Finnemore and Hollis' study of norm formation, we can better understand how PECA balances state security with the fundamental freedoms of people.

Core Argument

This research argues that Pakistan's law which regulates disinformation, Prevention of Electronic Crimes Act (2016), selectively aligns with UN Standards of Countering Disinformation for the Promotion of Human Rights and Fundamental Freedoms. In light of Finnemore and Hollis' theory of norm construction, this study highlights how PECA emphasizes regulatory control and compromises on freedom of expression, transparency, and proportionality of punitive measures which show the

Pakistani law places local socio-political priorities at the cost of a balanced cybersecurity approach.

Objectives

To analyze the extent to which Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 align with the United Nation's recommendations for countering disinformation especially in light of protecting human rights.

To evaluate how effective PECA is to balance cybersecurity requirements with fundamental freedoms such as the freedom of expression, transparency, and proportionality.

To investigate through the lens of Finnemore and Hollis' norm construction theory the extent of Pakistan's sociopolitical and security priorities

Research Questions

How does Pakistan's Prevention of Electronic Crimes Act (PECA) 2016 align with United Nation's recommended standards to counter disinformation, especially to protect human rights?

How effective is PECA in balancing the need for cybersecurity with fundamental freedoms which include the freedom of expression, transparency, and proportionality with punitive measures?

How do Pakistan's socio-political and security priorities shape the adoption of international norms within PECA as seen through theoretical lens of Finnemore and Hollis' norms construction?

Literature Review

Regulating disinformation is challenging especially when there is no universally accepted definition of the term. One way to study it is through inspection of official documents such as a state's laws which outlines it or using standards recommended by international bodies on what constitutes disinformation and how to deal with this issue. The subject is closely linked to human rights in terms of freedom of expression, right to information, and transparency. In Pakistan, the relevant law is the Prevention of Electronic Crimes Act (PECA) 2016. In a globalized interconnected world, laws don't exist in a vacuum and the United Nations also has standardized cybersecurity of which disinformation is a part. To guide this evaluation, a structured approach to assess how national and international norms interact is through theoretical framework which scholars Finnemore and Hollis provide in their norm construction theory. Additionally, scholarly critique can also add a needed dimension to evaluate how PECA aligns with UN's international standards.

UN Standards for Countering Disinformation

The United Nation's approach to disinformation is outlined in the Secretary-General's report on "Countering Disinformation for the Promotion and Protection of Human Rights and Fundamental Freedoms" (2022). It emphasizes the need to curb disinformation whilst upholding the freedom of expression by establishing a legal framework and discussion on the steps states and technology enterprises take to counter various manifestations of disinformation. The document is comprised of 60 points with a comprehensive approach centered around human rights, namely freedom of expression, transparency of regulation, prohibition of hate speech, advocacy of violence. How the state approaches disinformation, responsibilities of the technology companies in content moderation i.e. data transparency, and empowering individuals with recognizing disinformation through media literacy. For example, there is a need for proportionate and transparent regulation and avoiding broad or vaguely defined disinformation policies. Moreover, these regulations should safeguard democratic values and endorse norms which ensure accountability without excessive censorship. Ultimately, the document's goal is to balance effective disinformation control with protection of fundamental freedoms.

UN Broader Framework on Cybersecurity and Peace

The UN's stance on cybersecurity goes beyond disinformation to encompass broader principles of peace and security in cyberspace. "The United Nations Cyberspace and International Peace and Security" report by UNIDIR (Kavanagh, 2017) outlines norms for how states should behave while safeguarding fundamental rights. Although the report recognizes that states face difficulty while enforcing international norms domestically, particularly if they conflict with political agendas, it calls for trust-building measures among international actors by developing capacity-building measures. Doing so would enable nations to effectively address cyber vulnerabilities. The report is divided into three parts: First, it highlights the efforts made by UN General Assembly to set global standards. Next it connects how human rights issues are affected by international threats. Finally, it discusses the role of the Security Council to protect critical infrastructure. This is not easy as there are challenges of complexity such as limited resources, lack of trust between nations, and inconsistencies in international laws. Overall, the focus of the report is on global security related to information and communication technologies.

Pakistan's Prevention of Electronic Crimes Act (PECA) 2016

The Prevention of Electronic Crimes Act (PECA) became law in Pakistan in 2016. Its primary goal is to address the growing threat of cybercrimes. Moreover, it exists to enhance national security in cyberspace. As internet use, social media, and digital technologies advance and evolve, Pakistan faced increasing incidents of online fraud, harassment, unauthorized data access, and even cyber terrorism. After the 2014 terrorist attack on Army Public School in 2014, Pakistan launched the National Action Plan (NAP) to counter terrorism and extremism. On the digital front, PECA was introduced as part of the lager security strategy. These would include regulation of digital activities, combatting cyber offenses, and provision of a legal framework to persecute for cybercrimes. The PECA document is comprised of 55 sections which comprehensively covers a range of cyber offenses and protocols to enforcement. It defines terminologies, penalties for cybercrimes, procedural powers for investigation, protections for infrastructure, and provision for international collaboration for cybercrime cases. Since its inception, PECA has been amended three times: Once in 2020 with minor revisions to strengthen enforcement and update some definitions. Then in 2022, stricter penalties were introduced for online defamation making it a nonbailable offense, extending potential imprisonment from three to five years, and it also required courts to decide cases within six months to expedite proceedings. The latest amendments in 2023 include issues of cyberbullying, child protection, data protection, and privacy protection in online spaces.

Critiques of PECA

One result of inception and then the subsequent increased regulations has influenced how PECA is perceived. When looking at it through the lens of human rights of expression and rights to information or privacy, it has brought criticism for the expanded scope of the law. One critique by Sheraz Khan et al. (2019) noted that the vague language in sections 3, 4, and 37 permit broad interpretation which can lead to subjective enforcement which stifles free speech. The scholars argue that PECA has been given extensive powers to the authorities sans adequate safeguards. This can lead to a climate of self-censorship among journalists and activities in Pakistan which diverges from international standards like Article 19 of ICCPR – something which Pakistan is obligated to uphold. Similarly, Yasir Aleem et al. (2021) discuss a "chilling effect" (phenomenon in which people or groups are discouraged to express themselves because they fear breaking the law) in online expression. For example, the authors state that Section 37 of PECA allows Pakistan Telecommunication Authority (PTA) to block content without judicial oversight. Their argument is that this contradicts

with UN's recommendations for transparency and accountability in digital governance. This highlights PECA's potential misuse to silence dissenting views online and therefore compromise the standards of free speech and transparency. They suggest critical need for systematic assessment of PECA's provisions so it aligns with international human rights norms. Another scholarly critic is by Nabila Jaffar (2021) who situates PECA within a broader landscape of state-sponsored disinformation and media manipulation as tools of modern statecraft. She argues that PECA can be used as a political instrument rather than genuine protection against misinformation. For example, silencing dissenting voices in the pretext of "fake news" which can diverges form UN standards advocating freedom of expression and avoidance of excessive censorship. Jaffar highlights the need for a framework to distinguish genuine disinformation from political suppression mechanisms.

Normative Theories: Finnemore and Hollis' Cybersecurity Framework

Finnemore and Hollis' theory (2016) on norms in global governance offers a framework to explore how states construct and internalize norms. The focus in on the processes by which international norms are interpreted, adopted, or modified by the states based on their own unique social and political contexts. They offer a theoretical perspective which can be used to assess how PECA aligns with international norms such as how states prioritize security over individual freedoms. Therefore, states follow a selective adoption of norms. This exclusiveness raises questions about the universality of human rights principles in digital governance. The scholars go on to contend in order to be successful in norms integration, states need to find a balance between global standards with their local priorities. This raises the concern of inherent tensions in regulation of the cyber domain.

This source used for the study not only provide information regarding the legal frameworks, but the tension that exists between a state's requirements and conforming to UN standards for disinformation such as freedom of expression, transparency, and proportionality. Hence, a research gap exists to study this phenomenon in a standardized framework to asses PECA's alignment with global norms. Fennimore and Hollis provide such a framework for this study which can guide essential reforms ensuring a balance security with human rights protection.

Theoretical Framework

"Constructing Norms for Global Cybersecurity" by Finnemore and Hollis (2016) provides a comprehensive framework to understand how norms form in the cyber domain. They argue that cyberspace is not static: It evolves through social processes and interactions between diverse actors

which can be states, the private sector, and/or the civil society. Their fundamental argument is that norms are cultivated and reinforced through the process of socialization, persuasion, and stakeholders who make strategic choices. Whereas many norms which can be straightforward and can be established through treaties or legal definitions, the scholars argue that 'cybernorms' must be adaptable considering the change nature of the technological landscape. Furthermore, they have to accommodate various (often conflicting) goals of their stakeholders. With changing dynamics of technology, states must be adaptable in cybersecurity and redefine the stakes or who the stakeholders are.

Considering the flexible nature and context-driven approach makes the norms construction theory aptly relevant to assess Pakistan's Prevention of Electronics Crimes Act 2016. Using Finnemore and Hollis' theory, we can evaluate how PECA aligns with global norms set by international bodies – namely the United Nations' Standards for Countering Disinformation. Using this approach of a structured analysis of PECA's provisions, we can assess weather the law aligns with UN's recommended principles such as freedom of expression, transparency, proportionality. We can use this lens to evaluate not only on the formal contents of the law, but also on the socio-political contexts which drives its enforcement. Looking at PECA's flexibility, scope, and adaptability, the norms construction framework can offer a comprehensive understanding how national legislation fares in adoption of global norms. It should provide an assessment whether PECA aligns with or deviates from international standards for potential reform.

Methodology

Converting a subjective matter into an objective study requires a structured methodology. This will allow for an accurate assessment of how Pakistan's Prevention of Electronics Crimes Act (PECA) 2016 aligns with international standards. A systematic approach will provide clarity, consistency in identifying how PECA aligns with or diverges from UN's recommended standards on digital rights and disinformation regulation.

Research Design

This study is conducted with a qualitative content analysis methodology. This method is suitable to examine legal texts against a structured rubric made from international norms. Systematic evaluation of PECA's text for content analysis can focus on how the outlined provisions in the law align with United Nations Standards for Countering Disinformation (UNSGCD Report 2022) and protection of human rights – especially in regards to cyberspace.

Data Collection

Primary Data
Full text of Pakistan's Prevention of Electronics Crimes Act (PECA) 2016 including three amendments.
United Nations Report on Countering Disinformation for the promotion and Protection of Human Rights and Fundamental Freedoms (providing a benchmark to evaluate PECA)
Supplementary and Secondary Data
Critiques from studies evaluating PECA
Assessments by credible international organizations
Rubric-based Content Analysis
A custom rubric is designed into themes based on UN recommended standards which mentions the category, its description, and the justification of the category and its terminology for this rubric.
Freedom of Expression Protections
Assessing any language within PECA which protects or restricts freedom of expression
Section 20 of UNSGCD Report 2022: "…State responses to disinformation must themselves avoid infringing on rights, including the right to freedom of opinion and expression."
Section 56 of UNSGD Report 2022: "56. States bear the primary responsibility to counter disinformation by respecting, protecting and fulfilling the rights to freedom of opinion and expression, to privacy and to public participation.
Section 57 of UNSGD Report 2022: "To be effective in countering disinformation, responses need to be multifaceted and context-specific, and should be grounded in respect for the right to freedom of expression. In particular, strategies to counter disinformation should be clear about what is information they are seeking to tack le and identify the key players and obstacles in a particular context…"
Article 19 of the Universal Declaration of Human Rights and the ICCPR which prioritizes freedom of expression specifically stating: "Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice."
Transparency and Accountability
Examining procedural clarity, transparency measures, and public accountability (in regards to content regulation)

Section 27 of UNSGCD Report 2022: "Maximizing transparency and access to information is a central requirement for building trust in public institutions, governance and processes."
Section 60e of UNSGCD Report 2022: "Ensure a greater degree of transparency regarding measures to counter disinformation…"
Section 51 of UNSGCD Report 2022: "…take the actions necessary to protect against harms from disinformation, including conducting regular human rights impact assessments, enhancing transparency and accountability…"
Section 60f of UNSGCD Report 2022: Establish independent oversight to ensure accountability for enterprises' actions in terms of implementing any transparency and other obligations and commitments and redress for users."
Proportionality and Enforcement
Evaluate PECA's penalties and restrictions to determine whether they align with proportionate measures advocated by the United Nations.
Section 45C: "Disproportionate punishment, especially when coupled with the overbroad scope of many disinformation laws, creates a serious risk of discouraging speech…"
Section 26: "regulatory bodies need to ensure overall coherence with other enforcement structures…"
Each category is scored on a scale of 0 – 3 as with assignments as follows:

Rubric	**Score**
Full alignment with UN norms	3
Partial alignment with UN norms	2
Limited alignment with UN norms	1
No alignment with UN norms	0

Analytical Process
Coding and Scoring
Sections of PECA are coded according to categories given in the rubric
Each section is scored according to its language and provisions
Interpretation and Justifications are documented for transparency
Comparative Analysis

PECA's scores are compared against UN Standards
Determine areas of strong alignment and identify gaps
Any deviations will be analyzed in relation to Pakistan's socio-political context using Finnemore and Hollis' norm construction theory.

Limitations

Subjectivity in Coding
Despite the rubric, there may be an interpretative bias especially where PECA or UN Standards language is ambiguous.
Transparency can be enhanced by documenting the justification
Scope of Analysis
This study is limited to PECA's text; it does not examine the implementation or enforcement outcomes which can affect practical alignment with UN norms.

Findings and Analysis

In the analysis a qualitative content analysis method was used to evaluate PECA's text against United Nations Standards for Countering Disinformation. A rubric-based approach was applied by awarding of points for the level of alignment in light of Finnemore and Hollis' norm construction theory. The study demonstrates that PECA is partially aligned with UN norms in areas of proportionality and cybersecurity while the alignment with the freedom of expression and transparency remains limited. This shows that prioritization of state security causes divergence from global norms on transparency and individual freedoms. It also shows a regulatory approach which aligns the local need for control over digital content and cyberthreats. The details are as follows:

Freedom of Expression Protections

PECA has extensive restrictions on speech shown in the following sections:
Section 20: This section addresses "offenses against the dignity of a person" and criminalizes content that harms personal dignity. However, this section lacks specific definitions which allow for broad interpretation. For example, what constitutes dignity? Does the same rule apply to public figures (which should also be defined) as private citizens?
Section 37: This section grants Pakistan Telecommunications Authority (PTA) the power to block or remove content which it deems unlawful "in the interest of the glory of Islam or the integrity, security, or defense of Pakistan." However, without clear procedural protections for freedom of expression. Furthermore, "integrity" is ambiguous if taken as general term. PECA defines integrity as "the means, in relation to an electronic document, electronic signature or advanced electronic signature… has not

been tampered with…". This definition is not in context and, again, open for interpretation.
The use of broad language and lack of oversight. It exposes PECA to potentially overreach and limits its alignment with UN recommendations which emphasize freedom of expression as a fundamental right.
Score awarded: 1/3
Interpretation: Section 20 criminalizes content which can allegedly harm the "dignity of a person". This is vaguely defined and allows for broad interpretation. It could restrict legitimate speech. Section 37 grants PTA the power to block content with ambiguous wording. For example, there are no set boundaries or protections for "glory of Islam" and "national security".

Justification: The provisions in Sections 20 and 37 lack specific safeguards to protect free speech. This allows for significant discretionary power without immediate judicial review. The ambiguity does raise concern of how the law has the potential to infringe upon the freedom of expression which is a core principle in UN norms to preserve individual rights and diversity of opinions.
Comparative Insights: In contrast to UN norms upholding the freedom of expression despite within disinformation regulations, PECA's restrictive approach shows that the law prioritizes state control. According to Finnemore and Hollis' theory, this selective adoption is a result of Pakistan's focus on state security over protection of rights. Therefore, it shows that local security concerns internalize international norms.

Transparency and Accountability

PECA has components which show a vague process of transparency in decision-making.
Section 37 gives authority to PTA to restrict access to content which it deems unlawful without requiring judicial oversight. This gives PTA broad discretion to remove content for vague rationales such as those related to national interest, decency, or morality.
Although the law allows the Federal Government to formulate rules and safeguards, and mentions "transparent process" and "effective oversight mechanism", it leaves it up to the government which can allow for selective socio-political reasoning. Furthermore, it states that absence of any rules will empower the Authority. A plea may be filed and aggrieved parties can appeal to the High Court within thirty days.
Score awarded: 1/3

Interpretation: Section 37 authorizes with PTA with 'necessary' authority to remove content. It can refer matters to the Federal Government to prescribe rules. There is a process for aggrieved parties and the process of appeal is stated. However, considering the rapid nature of today's online content, there is no provision for the courts to decide the matter before, for example, the information becomes irrelevant.

Justification: The Act gets marks for outlining the process and lays out categories for offenses, but many are vague and open for interpretation. A small error in content or a malicious campaign would both get treated the same for content removal. PTA gets discretion the incumbent government can decide the rules of constitution of offenses. Referral of appeal to the High Court also comes at a cost of time for which some information may be time-bound for which there is no accountability for the loss incurred of the content's removal.

Comparative Insights: UN promotes transparency in disinformation regulation. However, PECA's enforcement mechanisms are opaque and include referrals and even authority in the absence of defined cases "for the time being". Finnemore and Hollis' norm construction theory suggests that Pakistan's focus remains on maintaining administrative control over digital content which shows state-centric regulatory practices over clearly defined governance.

Proportionality in Enforcement

PECA outlines severe penalties for various cyber offences which can range from imprisonment, fine, or both in sections its Chapter 2, Sections 6 to 28. In regards to disinformation, the following sections can be applied:

Section 9 deals with the dissemination of information which can glorify an offense related to terrorism, person or crime related to terrorism, or activities of any 'proscribed' organization/individuals/groups. It defines "glorification" to include any form of praise or celebration in a desirable manner. Although much of terminology can be subjective, but it shows the law take effort to define some terms. Violation can incur prison up to seven years or fine up to 10 million Rupees, or both. Because the punishment can be severe, there is no outlined criteria for applying maximum versus minimum penalties.

Section 10 discusses cyberterrorism and other clauses leading to cyberterrorism. It discusses creating a sense of fear, panic or insecurity, advance hatred of ethnic, sectarian, or interfaith hatred. Punitive measures include fines up to fifty million Rupees or imprisonment up to 14 years, or both. "Fear, panic, or insecurity", "advancing hatred" make enforcement

challenging because these terms aren't standardized and open to discretion by authorities, especially to assess severity.

Section 11 spells out an undefined fine and a prison sentence up to seven years, or both for hate speech which it defines as information which can 'likely' advance interfaith, sectarian, or racial hatred. Undefined fines can create inconsistency and leave room for variable enforcement. Although Resemblance to the definition of modesty is hinted upon in Section 63 of Pakistan Penal Code Act XLV (1860) defines "Amount of fine" as "Where no sum is expressed to which a fine may extend, the amount of fine to which the offender is liable is unlimited, but shall not be excessive". This too leaves room for interpretation.

Section 12 also deals with terrorism and one point is to curtail the recruitment process by disseminating information by an undefined fine, imprisonment up to seven years, or both. Similar to Section 11, it is open for variable interpretation and enforcement.

Section 16 discusses that any unauthorized use of identity information can be punished by a fine of up to five million Rupees, imprisonment up to three years, or both. Since "unauthorized use" is broad without specifying any criteria, it leaves the crime open for interpretation in terms of enforcement. Would self-posted pictures on social media be counted as authorized? Similar factors in regards to digital media can be defined better.

Section 20 discusses offenses against dignity of a natural person. This section specifically mentions "false" information to intimidate, harm the reputation or privacy of a natural person. Violation can bring a prison sentence up to three years with a fine that may extend to one million Rupees, or both. For broadcast media, people can apply for removal, destruction, or blocking access to such information and gives the Authority to "direct any of its licensees to secure such information". It doesn't state what the judicial oversight is regarding the licenses.

Section 21 discusses offences against modesty of a natural person and minor which deals with unwarranted use of sexually related content such as superimposition of images, intimidation, or enticement. This is a sensitive matter and punitive measures include imprisonment up to five years and fine up to five million Rupees, or both. In case of a minor, the punishment can be extended. Although the resemblance to the definition of modesty is hinted upon in Section 509 of Pakistan Penal Code (1860) which states "…intrudes upon her privacy", Modesty should be better defined and although it covers photographs, modern technologies such as Ai generated content, videos, deepfakes should also be included for enforcement.

Section 24 discusses cyberstalking by using any information system to coerce or harass another person, spying, or distribution of someone's picture without consent which harms a person. Punishment includes a prison sentence up to three years and fine up to one million rupees, or both. Section 24a goes on to discuss cyberbullying. However, words like "intimidate" and "coerce" are subjective. The language around cyberbullying could be better clarified instead of leaving it open for interpretation.

Section 25 discusses spamming as transmission of harmful, fraudulent, misleading, illegal, or unsolicited information which can incur a prison sentence starting around three months and 50,000 Rupee fine to repeated or bigger violations up to one million Rupees. While the section mentions increase in penalties for repeat violations, there could be better set parameters for words like "harmfulness" or "misleading information" which may open litigation gateways if taken in their ambiguous form.

Section 26 discusses 'spoofing' or establishing a website or information source with dishonest intention and can be punished for imprisonment up to three years and find up to 500,000 Rupees, or both. Although "dishonest intention" is defined as "…to cause injury, wrongful gain or wrongful loss or harm to any person or to create hatred or incitement to violence", the variability in interpretation and the low fine with broad application could be a weak deterrence.

Score awarded: 2/3

Interpretation: PECA incorporates critical measures to address cyber offences. Many align with international goals to strengthen digital security. However, as noted in the previous section point-by-point, there is a lack of specificity in many cases which can lead to subjectivity in enforcement. Fines and punitive measures are well defined for the most offenses yet the range and details are open for interpretation without a set criterion. In some cases, the fines are either not defined or the punishments cannot be measured to justify the severity of the offences.

Justification: Despite many ambiguities, PECA demonstrates partial alignment with UN norms. This is addressed through a structured framework to address cybercrimes including disinformation and cybersecurity. The Act provides a comprehensive outline of offences and the penalties associated with the crime which shows strong commitment to manage online threats. Procedural integrity and work towards accountability can be seen in the list of specific cybercrimes and procedures. Although there is room for improvement, the structured approach of PECA shows it is partially aligned with international standards outlined by the

United Nations. It emphasizes national security while acknowledging the freedom of expression in a regulated framework.

Comparative Insights: Viewed from the lens of Finnemore and Hollis' theory on norm construction, PECA demonstrates selective internalization of international norms. It shows Pakistan adapting cybersecurity principles to its socio-political landscape. Islamic values also may play a role in variance with worldwide norms especially when considering terms like "modesty" or dealing with extraordinary dangers of terrorism. This reflects strong punitive measures for cyber threats showcasing how Pakistan prioritizes state security. Even in this scenario, application of cybersecurity principles also showcases the country's efforts to integrate international norms with national security requirements while selectively incorporating elements of proportionality and transparency.

Discussion and Implications

The findings of this study show that PECA 2016 demonstrates a partial and selective alignment with United Nations approach to disinformation as outlined in the Secretary-General's report on "Countering Disinformation for the Promotion and Protection of Human Rights and Fundamental Freedoms". While the law incorporates vigorous cybersecurity provisions which are well aligned with international standards in infrastructure protection, in regards to disinformation, it compromises on freedom of expression, transparency, and proportionality. The selectiveness of alignment suggests that state security and control of digital content is prioritized over individual freedoms. One can see this interrelation as PECA 2016 emerged from the National Action Plan (NAP) which is Pakistan's broader strategy to combat terrorism and strengthen its national security. Supporting NAP's goals to counter extremism and boost national resilience against the many security threats, PECA provides a legal framework for addressing cybercrimes, cyberterrorism, hate speech, and disinformation – all which could incite violence or undermine national security.

With a priority for security, the selective adopting of UN norms reflects the influence of Pakistan's socio-political environment as theorizers of norm construction, Finnemore and Hollis, point out that states internalize global norms to align with local identities and interest. For a state which has faced, and faces threats of terrorism and extremism, there is a heightened focus on national security and maintenance, deterrence, and public order over freedoms of expression. The restrictive provisions on content are exacerbated by weak procedural transparency. This is recipe for a 'chilling effect' or the fear of people to freely express themselves without fear of

facing punitive measures. This can lead to suppression of legitimate speech and self-censorship undermining the freedom of expression.

UN standards on cybersecurity advocate that regulatory approaches should be carefully balanced with disinformation control. By being selective in implementation of security-oriented norms, digital rights are overlooked and PECA can be critiqued for limited integration of international human rights standards in cybersecurity legislation. Moreover, when terms, crimes, or categories are not well defined, broad interpretations are left to discretion of authorities. Besides the "what", the "how" is also called into question. For example, PECA gives some broad discretionary powers to Pakistan Telecom Authority (PTA) or other frameworks that can be influenced by the incumbent government's will rather than the law in its spirit. Referral to other agencies and courts can also hamper information flow, especially when information in the digital age can have a short life span. As another example, if PTA removes content and the case is referred to the high court which takes weeks to process, timebound information becomes moot by the time the process can be fully addressed and therefore, free expression is suppressed. Addressing such matters into law can help with transparency of the process, accountability of the parties, and a balanced approach towards aligning with international standards.

It must be noted that balancing disinformation control with free speech is not just an issue for Pakistan and developing countries, developed nations such as the United States and Germany face similar challenges (Helm & Nasu, 2021). While Pakistan's laws can be more restrictive, Amnesty International and other human rights organizations' criticisms of disinformation laws highlight a global struggle in crafting regulation frameworks which are effective and respect human rights. Therefore, although adopting of international norms is a complex undertaking given national cybersecurity frameworks, indigenous needs, varying contexts, evolving nature and technologies related to information and dissemination, and definitions which can satisfy multiple stakeholders. PECA's partial alignment with UN standards on disinformation can be drastically improved even it cannot be fully aligned.

Pakistan's PECA 2016 provides an insightful case study as to how national security concerns shape selective adoption of international norms on cybersecurity. Though challenging, improvements can be made towards protection of human rights towards freedom of expression while curtailing disinformation – not just for Pakistan, but for other countries across the world.

Policy Recommendations

To better align PECA with international standards and address the identified gaps, several policy recommendations emerge:
Enhance Judicial Oversight and Transparency: Introducing more clearly defend judicial review for PTA decisions on content removal could ease concerns about arbitrary censorship and increase public accountability.
Clarify Legal Definitions: Better definitions, especially in Sections 20 and 37 would reduce the potential for overreach by government and authorities to ensure that enforcement targets content which is genuinely harmful but won't suppress legitimate speech.
Implement Proportionate Penalties: Revising penalties to reflect the severity of offenses such as by outlining a range, particularly for some terms which are vaguely defined such as "dishonest intention" or "modesty" or "glorification" would align PECA's enforcement approach more closely with UN norms on proportionality.
Strengthen Privacy Protections: Putting in rigorous privacy safeguards into PECA's cybersecurity provisions would improve its alignment with digital rights standards. This could help balance national security measures with individual freedoms.
Consider trends in technology: Information and Communication Technology is evolving fast. Staying abreast of trends and forecasting use could offer a proactive way to incorporate laws dealing with emerging technologies such as artificial intelligence and their impact on human rights violations. Future research in a comparative analysis of other countries with similar sociopolitical contexts and how their laws are constructed in alignment with international norms and standards for cybersecurity, especially in regards to disinformation.

References

Aleem, Y., Asif, M., Khaliq, M., Imtiaz, I., & Ashraf, M. U. (2021). The Prevention of Electronic Crimes Act 2016 and shrinking space for online expression in Pakistan. Ilkogretim Online - Elementary Education Online, 20(2), 1019-1026.
Amnesty International. (2021). A human rights approach to tackle disinformation: Submission to the Office of the High Commissioner for Human Rights. Amnesty International. Retrieved from https://www.amnesty.org/en/documents/pol30/3477/2021/en/
Finnemore, M., & Hollis, D. B. (2016). Constructing norms for global cybersecurity. The American Journal of International Law, 110(3), 425-479.
GoP. (1860). Pakistan Penal Code (Act XLV of 1860). Government of Pakistan. Retrieved from

https://pakistancode.gov.pk/english/UY2FqaJw1-apaUY2Fqa-apaUY2Npa5lo-sg-jjjjjjjjjjjj
GoP. (2016). Prevention of Electronic Crimes Act. Government of Pakistan. Retrieved from https://pakistancode.gov.pk/
Helm, R. K., & Nasu, H. (2021). Regulatory responses to 'fake news' and freedom of expression: Normative and empirical evaluation. Human Rights Law Review, 21(2), 302-328. Retrieved from https://doi.org/10.1093/hrlr/ngaa060
Jaffer, N. (2021). Fake news and disinformation in modern statecraft. Regional Studies, 39(1), 3-33. Retrieved from https://regionalstudies.com.pk/wp/wp-content/uploads/2022/11/1.-Fake-News-Nabila-Jaffer.pdf
Kavanagh, C. (2017). The United Nations, cyberspace and international peace and security: Responding to complexity in the 21st century. United Nations Institute for Disarmament Research.
Khan, S., Tehrani, P. M., & Ifthikhar, M. (2019). Impact of PECA-2016 provisions on freedom of speech: A case of Pakistan. Journal of Management Info, 6(2), 7-11. Retrieved from https://readersinsight.net/jmi/article/view/566/737
Ó Fathaigh, R. (2019). Article 10 and the chilling effect: A critical examination of how the European Court of Human Rights seeks to protect freedom of expression from the chilling effect. Ghent University. Retrieved from https://biblio.ugent.be/publication/8620369
Secretary-General, U. N. (2022). Countering disinformation for the promotion and protection of human rights and fundamental freedoms: Report of the Secretary-General (A/77/287). United Nations. Retrieved from https://digitallibrary.un.org/record/3987886