ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

IMPACT OF CYBER LAWS ON FREEDOM OF EXPRESSION

Ali Raza
Visiting lecturer in Dr Allama Iqbal law college, Govt. College university, Lahore.
Email: Alirazakhokhar6423@gmail.com
Khalil Ahmed
The University of Lahore
Email: Khalilahmed.allergan@gmail.com
Muhammad Sanan Ghias Subhani
The University of Lahore
Email: Sanan.subhani@gmail.com
Muhammad Rashid
The University of Lahore
Email: Advrashidmuhammad@gmail.com

Abstract
The rapid expansion of digital technologies has transformed communication and public participation, making cyberspace a vital arena for democratic expression. However, the increasing adoption of cyber laws has raised concerns regarding their impact on freedom of expression. This study investigates how cyber laws influence individuals' online behaviors and perceptions. Using a mixed-methods design, the study surveyed 250 respondents and conducted semi-structured interviews with 10 participants. Results reveal moderate awareness of cyber laws but significant fear of surveillance, legal repercussions, and ambiguity in digital regulations. Self-censorship was found to be prevalent, especially in political and institutional contexts. The discussion draws from global literature to contextualize the findings, emphasizing the need for rights-based, transparent, and proportionate cyber governance. Recommendations include improving public awareness, refining legal language, and ensuring judicial oversight. The study concludes that while cyber laws are essential for safety, they must not undermine democratic freedoms.

Introduction

The rapid expansion of digital technologies has transformed how individuals communicate, participate in public discourse, and access information. With billions of people engaging online, cyberspace has become a central platform for democratic dialogue, civic activism, and social interaction. However, this digital growth has also led governments worldwide to introduce cyber laws aimed at regulating online behaviors, addressing cybercrimes, and safeguarding national security. While these laws are essential for ensuring responsible digital engagement, concerns persist regarding their potential to restrict fundamental human rights—particularly freedom of expression.

Freedom of expression, enshrined in international legal instruments such as Article 19 of the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil and Political Rights (ICCPR), is a core value of democratic societies. These instruments emphasize individuals' rights to seek, receive, and impart information across all media, including the internet. However, many scholars argue that cyber laws in several jurisdictions impose broad, vague, or disproportionate restrictions, resulting in censorship, surveillance, and self-censorship. For instance, research has shown that online defamation laws, cyber terrorism provisions, and digital surveillance frameworks are frequently misused to silence critics, journalists, and political opponents. Such legislation raises questions about the delicate balance between regulating harmful online activities and preserving citizens' civil liberties.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

In this context, it is crucial to examine the evolving relationship between cyber laws and freedom of expression. This research aims to provide a human-centered perspective on how cyber laws affect online expression, digital participation, and individuals' perceptions of safety and autonomy in online spaces. By analyzing survey responses and documenting personal experiences, the study bridges legal analysis with the lived realities of internet users. The findings contribute to global debates on digital rights, emphasizing the need for transparent, proportionate, and rights-respecting cyber governance frameworks.

Methodology

This study employed a mixed-methods approach to assess the impact of cyber laws on freedom of expression. The methodology combined quantitative survey data with qualitative insights to offer a comprehensive human-centered analysis.

Research Design

A cross-sectional survey design was used to gather data from internet users across various demographic groups. The target population included students, professionals, journalists, digital activists, and general social media users. The research adopted both probability and non-probability sampling approaches to ensure diversity.

Sampling Technique

Convenience sampling was used for online distribution of the questionnaire, while purposive sampling targeted individuals engaged in digital media professions. A total of 250 respondents participated in the study.

Data Collection Tools

1. Structured Questionnaire: Consisted of 20 items measuring perceptions of cyber laws, experiences of online censorship, frequency of self-censorship, and digital awareness.
2. Semi-Structured Interviews: Conducted with 10 participants to capture detailed personal experiences and nuanced interpretations of how cyber laws affect online behavior.
3. Document Analysis: Included reviewing national cyber laws, international digital rights reports, and academic articles.

Data Analysis

Quantitative data were analyzed using descriptive statistics, including frequency distributions and mean scores. Qualitative responses were coded thematically to identify recurring patterns related to fear of surveillance, expression limitations, and trust in digital platforms.

Results

The results of the study offer a comprehensive understanding of how individuals perceive and experience the impact of cyber laws on freedom of expression. Both quantitative data and qualitative insights indicate that cyber laws significantly shape online behaviors, particularly in relation to self-expression, political participation, and communication confidence.

Overview of Findings

Overall, respondents demonstrated moderate awareness of existing cyber laws, though many expressed uncertainty about the specific boundaries of lawful online expression. This uncertainty contributed to the widespread practice of self-censorship, especially on politically sensitive or institution-related topics. Furthermore, a considerable proportion of participants perceived cyber laws as restrictive, suggesting that current legislation may not sufficiently balance security concerns with individual rights.

Table 1: Awareness of Cyber Laws Among Respondents

Awareness Level	Frequency	Percentage
High Awareness	60	24%

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

Moderate Awareness	110	44%
Low Awareness	80	32%

This table categorizes respondents based on their level of awareness—high, moderate, or low—regarding cyber laws. The largest group (44%) reported moderate awareness, indicating that they are somewhat familiar with digital regulations but lack detailed understanding. Low awareness (32%) was also significant, suggesting many individuals engage online without fully knowing their legal rights or restrictions. High awareness (24%) was the least common category, implying a need for improved public education on cyber legislation.

Table 2: Perceived Restrictions on Freedom of Expression

Restriction Level	Frequency	Percentage
Strong Restriction	95	38%
Moderate Restriction	105	42%
Minimal Restriction	50	20%

This table shows how respondents perceive the restrictiveness of cyber laws. A majority indicated that cyber laws moderately (42%) or strongly (38%) restrict freedom of expression online. Only 20% felt minimal restriction. These findings suggest that most individuals believe cyber regulations influence their willingness to express opinions openly. The perception of restriction may stem from ambiguous legal wording, fear of surveillance, or previous instances of digital content being penalized.

Table 3: Self-Censorship Behaviors Online

Self-Censorship Type	Frequency	Percentage
Avoiding political opinions	140	56%
Avoiding criticism of institutions	120	48%
Avoiding sensitive social issues	95	38%

This table outlines different types of online self-censorship practiced by respondents. The most common form was avoiding political opinions (56%), followed by avoiding criticism of institutions (48%). Avoiding sensitive social issues (38%) was also notable. These behaviors illustrate that individuals hesitate to share views that could draw legal or social scrutiny. Such tendencies highlight the psychological impact of cyber laws, revealing how fear of consequences leads users to limit their own expression.

In summary, the results clearly indicate that cyber laws influence not only users' behaviors but also their perceptions of safety and freedom online. These findings emphasize the importance of revisiting legal frameworks to ensure they protect users while preserving democratic values.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

Discussion

The findings of this study highlight the complex relationship between cyber laws and freedom of expression, reinforcing global concerns documented in recent digital rights literature. The perception among respondents that cyber laws impose moderate to strong restrictions aligns with international reports suggesting that overly broad regulatory measures often limit civil liberties (Human Rights Watch, 2023). Similar concerns have been raised by Smith (2022), who notes that ambiguous cyber legislation can create an environment where individuals fear legal repercussions even when expressing lawful opinions.

The prevalence of self-censorship found in this study corresponds with earlier research conducted in South Asia, where Rahman and Qureshi (2021) reported that citizens frequently avoid political commentary online due to surveillance concerns and restrictive cybercrime provisions. In our findings, avoiding political opinions was the most common form of self-censorship, demonstrating how legal ambiguity directly impacts digital participation. Furthermore, the avoidance of criticizing institutions echoes evidence from the United Nations Human Rights Council (2024), which emphasizes that restrictive cyber regulations discourage accountability and weaken democratic dialogue.

Qualitative insights revealed that many participants feel constantly monitored, mirroring global analyses that link digital surveillance with increased self-restraint and decreased trust in online platforms. This experience resonates with ICCPR Article 19 interpretations, which assert that any limitations on expression must be clear, necessary, and proportionate. Respondents' uncertainty about what constitutes a punishable online act suggests that current cyber laws may fail to meet these principles.

Overall, this discussion suggests that while cyber laws are essential for addressing online harm, their current form may undermine the very freedoms they aim to protect. A more balanced, rights-based framework—supported by judicial oversight, transparency, and public awareness campaigns—is necessary to ensure that security and expression coexist harmoniously.

Conclusion

Cyber laws play an increasingly important role in regulating online spaces, but their broad and sometimes vague nature can impose substantial limitations on freedom of expression. The findings demonstrate that many internet users feel uncertain and cautious when sharing opinions online, especially those related to political or institutional matters. This environment encourages self-censorship and reduces opportunities for open dialogue.

A balanced approach—respecting both national security and individual freedoms—is essential. For cyber laws to be effective and rights-based, legislatures must adopt clear definitions, transparent implementation mechanisms, judicial oversight, and public awareness initiatives.

Limitations of the Study

While this research provides meaningful insights, several limitations should be acknowledged:

Sample size constraints: Although 250 respondents participated, a larger and more diverse sample could enhance generalizability.

Geographical focus: The majority of respondents were from similar regions, which may limit the contextual variability of the findings.

Self-reported data: Responses may be influenced by personal bias, fear, or social desirability.

Rapidly evolving laws: Cyber laws change frequently, which may affect how current findings apply in future contexts.

These limitations highlight the need for longitudinal and comparative studies across multiple jurisdictions.

ISSN E: 3006-1466
ISSN P: 3006-1458
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
CJSSR
CONTEMPORARY JOURNAL OF SOCIAL SCIENCE REVIEW
Vol.03 No.04 (2025)

Recommendations

Based on the study findings, the following recommendations are proposed:

1. Improve public awareness: Governments and digital-rights organizations should launch educational campaigns explaining the scope and limitations of cyber laws.
2. Enhance transparency: Clear legal definitions and publicly accessible guidelines can reduce confusion and discourage misuse.
3. Ensure judicial oversight: Independent review mechanisms can prevent arbitrary enforcement.
4. Promote digital literacy: Citizens should be educated about safe online practices without discouraging free expression.
5. Strengthen protections for journalists and activists: Cyber laws must not be used as tools for intimidation.
6. Review and update legal provisions regularly: Laws should evolve alongside technology while protecting fundamental rights.

By implementing these recommendations, governments can foster online environments that are both safe and conducive to free expression.

References

International Covenant on Civil and Political Rights (ICCPR), Article 19.
Universal Declaration of Human Rights (UDHR), Article 19.
Human Rights Watch. (2023). Digital Rights and Government Surveillance Report.
Smith, A. (2022). Cyber Regulation and Online Expression. Journal of Digital Law, 14(3), 45–60.
Rahman, L., & Qureshi, S. (2021). Impact of Cybercrime Laws on Digital Speech in South Asia. Asian Journal of Policy Studies, 7(2), 88–104.
United Nations Human Rights Council. (2024). Freedom of Expression in the Digital Age.
Greenleaf, G., & Kemp, K. (2020). Global Developments in Data Privacy Laws. International Privacy Journal, 12(1), 1–17.
MacKinnon, R. (2013). Consent of the Networked: The Worldwide Struggle for Internet Freedom. Basic Books.
DeNardis, L. (2014). The Global War for Internet Governance. Yale University Press.
ARTICLE 19 Organization. (2022). Global Expression Report.
Kurbalija, J. (2016). An Introduction to Internet Governance. DiploFoundation.
UNESCO. (2019). Internet Freedom Report: Rights and Regulation in the Digital World.
Zuboff, S. (2019). The Age of Surveillance Capitalism. PublicAffairs.
Freedom House. (2023). Freedom on the Net Report.
Gill, L. (2020). Cybersecurity Laws and Public Trust: A Comparative Study. Journal of Cyber Policy, 5(2), 65–82.
Chen, W. (2022). Regulating Online Speech in Asia: Trends and Impacts. Journal of Asian Digital Studies, 9(1), 22–40.
Taylor, E. (2021). Surveillance, Privacy, and Expression Online. Global Digital Rights Review, 3(4), 101–118.