Social Sciences Spectrum

A Double-Blind, Peer-Reviewed, HEC recognized Y-category Research Journal

E-ISSN: 3006-0427 **P-ISSN:** 3006-0419
Volume 03, **Issue** 04, 2024
Web link: https://sss.org.pk/index.php/sss

Balancing Censorship and Cybersecurity: A Case of Internet Freedom and Security in Pakistan

Robina Khan
Assistant Professor, Department of Political Science, Gomal University, Dera Ismail Khan, Pakistan
Correspondence: dr.robina@gu.edu.pk

Maryam Siddique
Assistant Professor/ Head of Department of Psychology, Gomal University, Dera Ismail Khan, Pakistan
Email: maryam@gu.edu.pk

Zafar Abbas
Assistant Professor, Department of Political Science, Government College No.1 Dera Ismail Khan, Pakistan
Email: zafarabbas2004@gmail.com

Article Information

Received September 02, 2024 **Revised** October 06, 2024 **Published** October 17, 2024

Citation (APA):

Khan, R., Siddique, M. & Abbas, Z. (2024). Balancing censorship and cybersecurity: A case of internet freedom and security in Pakistan. *Social Sciences Spectrum, 3*(4), 31-39.

Abstract

This article explores potential strategies for balancing online freedom and security, explores censorship and cybersecurity policies in Pakistan, and explores the impact of these policies on internet freedom. The internet's arrival has presented contemporary societies with several challenges, including the need to balance internet freedom with cybersecurity dangers. To protect against cybercrimes, promote social morality, and guarantee national security, the government of Pakistan has enacted censorship laws to monitor the content of the internet. However, these limits jeopardize the digital rights of individuals. In Pakistan, striking a balance between the openness of the internet and the protection of the nation's security is a difficult but necessary task, according to this article.

Keywords: Censorship, Internet Freedom, Cybersecurity, Cybercrimes, Challenges.

Introduction

The development of digital technology has completely transformed the world. Through the use of digital technology, civilizations have been altered, and global interaction has become simpler. One of the most important tools for communication and expression is the internet. However, the internet revolution has resulted in several difficulties for civilized countries, such as striking a balance between the openness of the internet and the hazards associated with cybersecurity (Rehmat & Alam, 2018). In Pakistan, the issue of internet freedom presents a complex challenge. The Pakistani government has imposed censorship regulations to limit the availability of online material. The government does this under the guise of safeguarding citizens from cybercrimes, upholding social morality, and safeguarding national security (Jamil, 2021).

The Pakistani government aims to protect citizens from potential dangers and dangerous content on virtual platforms through the implementation of censorship rules. However, the implementation of these rules creates risks to individuals' digital rights (Jamil, 2021). The rise in the number of crimes committed online is another cause for worry. Pakistan has seen a rise in cybercrimes. Cyberbullying, online fraud, and hacking are just examples of the crimes that fall under this category (Abbas & Zubair, 2020). The government asserts that the implementation of cyber regulations and censorship are essential to lessen the likelihood of cybercrime occurring. Moreover, the implementation of digital regulatory rules is crucial for safeguarding national security. Despite this, it is crucial to balance the implementation of these measures with the risk of violating fundamental digital rights.

Theoretical Background

"Cyberspace" is a fully digitalized, borderless, and timeless dimension. Some have even referred to it as a "consensual hallucination" (Gibson, 1984), where people can express their views and opinions and connect through a global "network of networks" (Deibert, 2003). "Cyberspace" is regarded as a notion. Castells (2009) used the term "Network society" to describe the revolutionary communication platform that gave birth to the concept. According to Peteva (2020), the word "cyberspace" has been associated with the Internet and the World Wide Web since the 1990s. Additionally, when we talk about "cyberspace", we are referring to the question of whether or not it is possible to censor content. Therefore, during our discussion, it appears that we prefer the term "Internet censorship" over the previously mentioned one.

"Net Utopians", who believe it is nearly impossible to censor the Internet, have evolved over the last two decades and have not supported themselves against more restrictive policies. For many years, the debate between libertarianism and paternalism has surrounded the concept of Internet censorship (Jewkes & Yvonne, 2010). For instance, Spinello (2002) observes that the origins of cyberspace are unquestionably libertarian. Additionally, he defends the classical liberal perspective that Mill embraced, which means that he supports an Internet that is free from censorship. On the other hand, a paternalistic perspective may justify censorship by arguing that it aims to avert potential harm. This, in turn, justifies the strengthening of state meddling and surveillance, as well as the restriction of free expression to some degree. The fact, however, is that in strictly practical terms, the Internet is not totally "censorship-proof", and there are a variety of censorship tactics that have been deployed in many settings to support this notion. This remains true regardless of one's stance on the matter.

Understanding Censorship and its Consequences

There are several different approaches that governments use to censor the internet. These approaches include banning websites, filtering information, and monitoring activities on the

internet. There are various reasons to censor the internet, such as safeguarding national security and preventing access to harmful content like pornography or hate speech. Some people think that censorship of the internet is a violation of people's rights to freedom of speech and expression, while others claim that it is important to filter the internet to protect citizens and preserve social order. There are two different ways that censorship of the internet may take place: Top-down censorship happens when a government or other entity directs service providers to prohibit specific information. Legislation may mandate the blocking of particular information in various instances. Users cannot choose what they can access and have no control over the situation. Self-imposed censorship, on the other hand, refers to the practice of people or organizations establishing their self-censorship by selecting which information to avoid.

Media censorship is a global issue that has long preceded the establishment of information sources. One of the most prevalent justifications for censorship is the need to preserve order in the state; nevertheless, the underlying motivation is to ensure that the general population is unaware of information that may pose a danger to the authorities. The global connectedness of the Internet in the modern day makes it possible for information to travel quickly across national boundaries and even across international borders. As a result, a rising number of people who consume media rely on the Internet to get a broad range of information. In Pakistan, the government sustains its existence by implementing strict Internet surveillance measures. These apparatuses efficiently block websites and discreetly filter information, allowing only selected news to pass through the gate (Abbasi & Al-Sharqi, 2015).

It is possible to use censorship to control and suppress any expression that could threaten state order. People have used censorship throughout human history to monitor public morality, control public knowledge, and silence resistance. Socrates faced censorship for the first time in 399 B.C. For his recognition of divinities not considered conventional, he received a death sentence (Newth, 2010). In theory, the most recent technical breakthroughs make it difficult, if not impossible, to limit the flow of information that is accessible to users of the internet. Digital censorship swiftly emerged after the introduction of journalism to the Internet, employing technologies like filtering, blocking, hacking, and redirection. Despite this, the government of Pakistan has been able to catch up with more advanced technology, which has enabled them to monitor material that is found online and to divert the flow of information when necessary.

The need to maintain the state's security and stability frequently justifies censorship in Pakistan. There is censorship going on all around the world. The enforcement of censorship aims to uphold the existing social order. According to Abbasi and Al-Sharqi (2015), the PTA and other government entities play a significant part in the enforcement of censorship restrictions. When it comes to matters of security, the government often blocks websites and internet services, which ultimately constitutes a violation of digital rights. Several civil society groups and human rights advocates have expressed their concerns about how censorship impedes democratic participation and online discourse (Abbas & Zubair, 2020).

Internet Freedom

It is possible to trace the origins of the distinction between positive and negative Internet freedom back to the time before the Internet when academics were developing what they meant by the term “press freedom”. A beneficial example of this is Picard (1985), who made a distinction between negative press freedom, which is freedom from censorship, and positive press freedom, which refers to the capacity of the people to make use of the media. The conceptual framework that incorporates both positive and negative aspects of Internet freedom reflects the human rights

approach to Internet freedom, which holds that international human rights rules are relevant to freedom of thought and expression on the Internet (Shen, 2017).

Documents such as the Universal Declaration of Human Rights (UDHR) describe the fundamental concepts that underpin the freedom of the Internet, identifying the ability to receive and transmit information without interference as an inherent right. Social media platforms have emerged as one of the most significant instruments for a large number of people all over the globe to freely express themselves, engage with one another, and exchange and receive information, ideas, and news. People are now able to communicate with one another and band together for any cause, including political and social activities, thanks to the proliferation of social media. Before the emergence of social media, traditional mass media channels like newspapers, radio, and television played a major role in opinion sharing and information gathering. For the last ten years, social media platforms have established a global arena that enables individuals to search for, collect, receive, and share almost everything conceivable. Previously, it was not feasible for governments to control content that was communicated via social media; but, in recent times, authorities have begun to regulate social media platforms and have adopted censorship rules (Tambini, 2021).

The possibility that the Internet may improve people's ability to express themselves freely is without a doubt not universally accepted. The regulation of social media platforms is far more stringent in several nations than it is in other ones. China, Iran, Cuba, Syria, Turkey, and Vietnam are just a few of the countries that actively block social media websites and take measures to restrict information that is available online. Through the implementation of the "Great Firewall of China" and the practice of keyword blocking, which entails the prohibition of an enormous number of terms on the internet, the country's expression is subject to intensive censorship and control.

Security Issues in Age of Technology

Cybercrimes

The phrase “cybercrime” can carry a wide range of meanings. For instance, we refer to conduct as cybercrime when it occurs on a computer using the internet and a digital device. Moreover, another characteristic of this type of criminal activity is that the perpetrator is never required to be physically present at the crime scene (Munir & Gondal, 2017). Despite the proliferation of the internet, 3G/4G technologies, and information and communication technologies (ICTs), Pakistan is having a difficult time progressing in both the public and commercial sectors. It is crucial for developing nations to defend not just persons and companies, but also the country itself, from cybercrimes, since the rapid growth of technology poses a significant threat to the protection of the nation. Regrettably, Pakistan is not completely immune from malicious cyber activity (Zahoor & Raz, 2020).

It is crucial to have a clear understanding of cybercrime. Barn and Barn (2016) believe that one of the likely factors contributing to the difficulty of assessing cybercrime is the absence of well-formed definitions and categorization systems that can account for the variety of cybercrimes. According to Black et al. (2019), the fact that cybercrime law in different jurisdictions is not systematic nor universal is an additional factor that contributes to the complex nature of this issue. Cybercrimes have increased in Pakistan, posing several challenging issues for individuals, companies, and government officials. The growth in cybercrimes has brought about these challenges. Cybercriminals are now launching attacks on the information infrastructure. Abbas et al. (2023) have identified hacking, phishing, identity theft, online fraud, and cyberbullying as some of the most prevalent forms of cybercrime. According to Shahzad (2023), the increasing number of cybercrimes gives more proof of the weaknesses that exist inside Pakistan's digital infrastructure

and underscores the need for developing comprehensive cybersecurity measures. He also emphasizes the need to address these vulnerabilities.

Strategies for Strengthening Cybersecurity

In the current age of digital technology, there is a growing worry over cybercrimes (Ekwonwune et al., 2024). The proliferation of cybercrime is posing an ever-increasing threat to Pakistan. The laws that control cybercrime in Pakistan include categories such as cyberterrorism, online theft, and online fraud. These laws also cover the electronic devices used to commit these crimes. Several cyber laws, addressing cybersecurity concerns, have been in effect since 2002 and even before that (Rehmat & Alam, 2018).

Pakistan has implemented legal measures to address the issue of cybercrime. The government of Pakistan enacted the Electronic Transaction Ordinance (ETO) 2002 to recognize and facilitate the use of electronic forms for papers, records, information, communications, and transactions, according to Hamdani (2014). It is possible to trace a significant portion of this growth in the media sector to the implementation of the Pakistan Electronic Media Regulatory Authority (PEMRA) Ordinance 2002. In addition, the government enacted several additional laws that pertain to the media, including the Press Council Ordinance of 2002, the Defamation Ordinance of 2002, and the Press, Newspaper, News Agencies, and Books Registration Ordinance of 2002. The Newspaper Employees (Conditions of Services) Act, 1973 was another piece of legislation that was in effect at the same time as these other laws (Gul, 2017).

In 2004, Pakistan's Ministry of Information Technology presented the Electronic Crime Act (ECA)-2004 to the public for the first time. These changes were made to the ETO-2002, which underpinned this law. ECA-2004 is responsible for the specification of a vast number of new terms, some of which include cyberterrorism, unauthorized access, system and data damage, and electronic theft. In a nutshell, one of the key objectives of this piece of law was to provide legal protection for efforts to combat cybercrime. The Prevention of Electronic Crimes Ordinance (PECO 2007) was passed into law in 2007 to combat cybercrime in Pakistan (Daily Dawn, 2009). Remember, the Parliamentary Election Commission of Pakistan (PECO-2007) aimed to establish cyber-law rules. The legislation addressed the penalties for committing electronic fraud and falsification, as well as data destruction, cyberstalking, spoofing, and spamming behavior. Some segments of society have expressed their disapproval of this law, citing its political motivations and its intended suppression of disputes. Opponents and civil society members successfully ruled it null and invalid in November 2009 (Zafar & Ahmad, 2011).

The President of Pakistan approved the Prevention of Electronic Crimes Act (PECA)-2016 on August 18, 2016. The Act included provisions for the restriction, monitoring, and punishment of speech that occurs on the internet. The statute encompasses a wide range of offences, including but not limited to the illicit transmission of data, illegal copying, and unauthorized access to an information system. This Act established severe fines for data or computer networks related to critical infrastructure. Under the provisions of the PECA-2016, hate speech and offences connected to terrorism, including the planning, recruiting, and/or financing of terrorist activities via the use of new media, are subject to legal consequences (LOC, 2016). Not only has the definition and determination of cybercrime been the subject of intense opposition from national and international human rights organizations throughout the legislative process of the PECA-2016, but several clauses have also been subject to such opposition. The "United Nations Special Rapporteur on Freedom of Expression" expressed his concern and recommended a thorough evaluation of the Act, ensuring adherence to established international human rights norms. Several

international human rights organizations have attacked the PECA-2016 not only for infringement on the rights to freedom of expression and privacy, but also for its excessively harsh enforcement (Privacy International, 2017).

Need for Balancing Censorship, Cybersecurity and Internet Freedom

Many democratic nations have difficulty striking the appropriate balance between freedom of expression on the one hand and its proportionate restriction on the other. On the other hand, non-democratic nations frequently oppressively use censorship, in the form of what is known as "digital authoritarianism" (Shahbaz & Funk, 2019). As a result, many democratic nations struggle to find the right balance. Researchers have determined that North Korea has the highest level of Internet censorship, meaning the government controls and heavily restricts any material broadcast to the general public (Bischoff, 2020). Lee and Liu (2012) rate China in second place, highlighting its exceptionally efficient mechanism for censoring materials in cyberspace. This approach is known as the "Great Firewall," and it prevents China's "netizens" from accessing stuff that they do not find acceptable. Some other nations, such as Russia with its "blacklist law" (BBC News, 2012) and Vietnam with its Decree 72 law that criminalizes political criticism, are examples of governments that are making growing efforts to filter material and impose repressive censorship (Schmidt & Cohen, 2014).

Citizens in Pakistan have gained more power as a result of the widespread usage of the internet, which has enabled them to exercise their right to free expression, have access to a variety of information, and participate in civic debate. However, the surge in online activity also presents risks to national security. The government is aware that the dissemination of material on the internet may pose a risk to national security. Because of the proliferation of false information, the commission of cybercrime, and the use of digital platforms by terrorist groups, it is necessary to take a strategic approach to the administration of the internet to protect both internet freedom and national security. The presence of sensitive material, such as multiple films depicting military manoeuvres and strategies, postings containing confidential economic information, or other facts that might compromise our nation's security, can put our nation in jeopardy.

Notwithstanding this, there is a debate going on between a number of different schools of thought. One school of thought contends that the control of technology is a breach of international human rights norms and that it ultimately affords the government the potential to monitor the actions of the general public that take place on the internet. Governments often abuse the cyber laws, which encompass legal and political issues relating to Internet-based technologies such as freedom of expression, access to information, privacy rights, and the right to intellectual property. There is a need for a balanced strategy that respects the liberties of individuals while limiting security dangers, and this dual-use nature of the internet highlights the need for such an approach.

Striking a balance between the ideal of Internet freedom of speech, which allows users to act anonymously, and the need for a safe environment, where responsible governments can discover and prevent harmful users, is a challenging problem. Indeed, policymakers in the modern era are currently involved in two concurrent activities that could potentially clash with each other. To promote freedom on the internet, it is necessary to advocate for privacy and provide people with tools that allow them to conduct themselves anonymously online. Cybersecurity, on the other hand, pertains to the transparency and attribution of online activities. People often fail to understand and address the conflicts these two activities cause. One factor contributing to the issue is the isolation of discussions about cybersecurity and Internet freedom regulations from one another. The national security community has been active in the development of cybersecurity policy, while the

technology community and a small group of human rights advocates have been interested in the development of Internet freedom regulations.

Keeping a balance between preserving digital rights and maintaining order, peace, and security in a society is the most challenging challenge that the government of Pakistan must face. The requirement of finding a means to strike a compromise between safeguarding national security and maintaining internet freedom is one of the most crucial difficulties that policymakers in Pakistan confront. Other challenges include the need to find a strategy to preserve national security. Policymakers in Pakistan should adopt cybersecurity measures that respect basic rights to combat cyberattacks and protect national interests. These fundamental rights include the right to privacy, the right to freedom of speech, and the capacity to access critical information (Abbas *et al*., 2023).

Conclusion

The number of incidences of cybercrime in Pakistan is increasing, and they are affecting both people and companies. A lack of resources and available skills confronts the nation with difficulties in addressing these dangers. Improving cybersecurity and successfully combating cybercrimes in Pakistan requires several important actions, including investments in technology and the promotion of international collaboration. The article's findings conclude that Pakistan's censorship rules impede internet freedom. Through the engagement of stakeholders, the enhancement of transparency, and the refinement of legislative frameworks, Pakistan can establish a more balanced approach that respects both the basic rights of people and security as well. Striking a balance between the openness of the internet and the protection of the country is a difficult but necessary task in Pakistan. A dedication to democratic ideals, an awareness of the digital world, and a coordinated effort from all sectors of society are required to accomplish this. The findings of this research indicate that cybersecurity requires both the development of new technologies and the expansion of existing capabilities. In this post, the author emphasizes the need for precise legal definitions and openness in government policies about internet freedom. Additionally, the author encourages interaction from several stakeholders and identifies solutions to preserve this balance. Pakistan can create a digital environment that protects both internet freedom and national security using this method.

References

Abbas, Z. & Zubair, M. (2020). Freedom of Expression under Censorship is a threat to Democracy. *The Dialogue,* 15(1): 18-26.

Abbas, Z; Khan, R; Khan, M.Z; & Imran, M. (2023). Cyber Laws and Media Censorship in Pakistan: An Investigation of Governmental Tactics to Curtail Freedom of Expression and Right to Privacy. *Journal of Creative Communications,* 1-14.

Abbasi, I. S & Al-Sharqi, L. (2015). Media censorship: Freedom versus responsibility. *Academic Journals, Journal of Law and Conflict Resolution, 7*(4): 21-25.

Barn, R.; Barn, B. (2016). An ontological representation of a taxonomy for cybercrime. *In Proceedings of the 24th European Conference on Information Systems* (ECIS 2016), Istanbul, Turkey, 12–15 June 2016.

BBC News (2012, January 11). Russia internet blacklist law takes effect. Retrieved from http:// www.bbc.co.uk/news/technology-20096274

Bischoff, P. (2020). Internet Censorship 2020: A Global Map of Internet Restrictions. *Comparitech* Retrieved from, https://www.comparitech.com/blog/ vpn-privacy/internet-censorship-map/>.

Black, A.; Lumsden, K.; Hadlington, L. (2019). Why Don't You Block Them? Police Officers' Constructions of the Ideal Victim when Responding to Reports of Interpersonal Cybercrime. *In Online Othering: Exploring Violence and Discrimination on the Web; Lumsden, K., Harmer, E., Eds.*; Palgrave Macmillan: Basingstoke, UK, pp. 355–378.

Castells, M. (2009). *The Rise of the Network Society: The Information Age: Economy, Society, and Culture*. Wiley-Blackwell.

Daily Dawn. (2009, October 30). Traders term e-crime law anti-people. Retrieved from https://www.dawn.com/news/889238

Deibert, R.J. (2003). *Black Code: Censorship, Surveillance, and the Militarisation of Cyberspace*. 32 Millennium.

Ekwonwune, E.N., Eduroha, A., Dennis, M.C., & Chigozie, U.C. (2024). Internet Censorship and its Implication on Personal Privacy. *International Journal of Research Studies in Computer Science and Engineering*, *10*(2): 22-30.

Gul. A. (2017, November 14). Study: Internet Freedom Worsens in Pakistan. *Voice of America,* [Retrieved from https://www.voanews.com/a/internet-freedom-worsens-pakistan-study/4114815.html].

Hamdani, Y. (2014). Major Challenges to Fundamental Right of Freedom of Speech in Pakistan. *Media Defense*.

Jamil, S. (2021). The rise of digital authoritarianism: Evolving threats to media and Internet freedoms in Pakistan. World of Media. *Journal of Russian Media and Journalism Studies*, 3(1): 5-33.

Jewkes, Y & Yvonne, M. (2010). Introduction: The Internet, cybercrime and the challenges of the twenty-first century, [in:] Y. Jewkes, M. Yvonne (ed), *Handbook of Internet Crime.* Willan Publishing.

Lee, L & Liu, C. (2012). Forbidden City Enclosed by the Great Firewall: The Law and Power of Internet Filtering in China. *Minnesota Journal of Law, Science and Technology, 13*(1): 125-135.

LOC. (2016, September 21). Pakistan: National Assembly passes a new cybercrime law. *Library of Congress*. https://www.loc.gov/item/global-legal-monitor/2016-09-21/pakistan-national-assembly-passes-newcybercrime-law/

Munir, A., & Gondal, M.T. (2017). Cyber Media and Vulnerability: A discourse on cyber laws and a probe on victimization of cybercrimes in Pakistan. *Global Media Journal: Pakistan Edition, 10*(2).

Newth, M. (2010). The long history of censorship. Retrieved from http://www.beaconforfreedom.org/liste.html?tid=415&art_id=475

Peteva, P. (2020). The nature of censorship and regulation of the darknet in the Digital Age. PRAWO, Retrieved from https://repozytorium.uni.wroc.pl/en/dlibra/publication/129046/edition/118462/the-nature-of-censorship-and-regulation-of-the-darknet-in-the-digital-age-peteva-petya.

Privacy International. (2017). *The right to privacy in Pakistan*. Privacy International: Human Rights Committee 120th Session.

Rehmat, A. & Alam, M. A. (2018). The State of Digital Rights in Pakistani Cyberspace. *Freedom Network.*

Schmidt, E.E. & Cohen, J. (2014, March 11). The Future of Internet Freedom. *The New York Times.* Retrieved from http://www.nytimes.com/2014/03/12/opinion/the-future-of-internet-freedom.html?_r=0

Shahzad, M. (2023). Emerging Cyber Crimes in Pakistan: A Case Study of Online Fraud through Digital Microloan Apps. *Global Digital & Print Media Review, 6*(2): 411-421.

Shen, F. (2017). Internet Use, Freedom Supply, and Demand for Internet Freedom: A Cross-National Study of 20 Countries. *International Journal of Communication*, 11(2); 2093–2114.

Tambini, D. (2021). A theory of media freedom. *Journal of Media Law, 13*(2); 135-152, DOI: 10.1080/17577632.2021.1992128.

Zafar, F., & Ahmad, S. (2011). *The challenges of internet rights in Pakistan*. Global Information Society Watch. https://www.giswatch.org/en/country-report/internet-rights/challenge-internet-rights-pakistan.

Zahoor, R & Raz, N. (2020). Cyber-Crimes and Cyber Laws of Pakistan: An Overview. *Progressive Research Journal of Arts and Humanitie*, 2(2): 134-143.