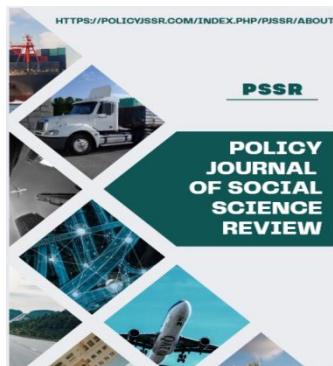


Policy Journal of Social Science Review



ISSN Online:3006-4635

ISSN Print: 3006-4627

CYBERCRIME AND DATA PROTECTION LAWS IN PAKISTAN: CHALLENGES, LEGAL FRAMEWORK, AND THE NEED FOR EFFECTIVE DIGITAL RIGHTS PROTECTION

¹Zaheer Iqbal Cheema, ²Muhammad Azeem Farooqi, ³Gul Sher Butt

¹Assistant Professor, University Law College, University of the Punjab, Lahore, Pakistan .
Ph.D.National University of Malaysia

²Ph.D. Scholar, LL.M., M.A. (English) Assistant Professor, Department of Law,
Government College University, Lahore, Pakistan

³Assistant Professor, Department of Law, University of Sargodha

zaheer.law@pu.edu.pk azeem.farooqi@gcu.edu.pk gull.sher@uos.edu.pk

Article Details

Received on 10 Feb, 2026

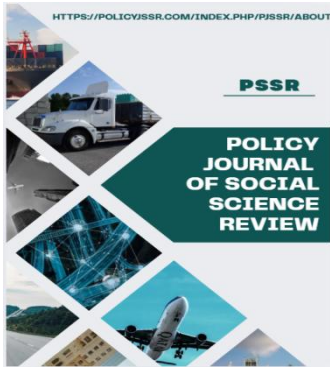
Accepted on 19 March, 2026

Published on 21 March, 2026

ABSTRACT

Digital technologies have revolutionized social, economic and governmental activities in Pakistan. The expansion of the internet, smart phones, online banking, e-commerce sites and digital communication networks have provided positive opportunities for economic development and social interaction. The digital transformation, however, has also yielded new manifestations of criminality, such as those involving cyber fraud, unauthorized use of information systems, ID theft, online harassment, data breach and other crimes that are technology-based. With the rising trend of dependence on digital platforms and low

Policy Journal of Social Science Review



ISSN Online:3006-4635

ISSN Print: 3006-4627

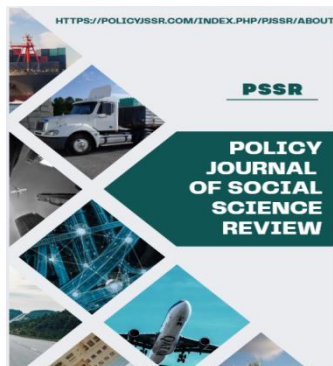
Copyright @Author

Corresponding Author: *

awareness among the public on cybersecurity practices, cybercrime is becoming a major problem for Pakistan. To confront these problems, Pakistan enacted the Prevention of Electronic Crimes Act (PECA), 2016, which is an all-embracing legislation to combat electronic crimes and digital offences. While PECA has laid a solid ground for the regulation of cybercrime, there are also some issues that need to be addressed in relation to enforcement mechanisms, institutional capacity, privacy protection, and balancing cybercrime security measures with basic human rights. The study analyzes the existing legislation related to cybercrime and data protection in Pakistan, highlighting the effectiveness of the laws, implementation challenges, and the need for more robust protection of digital rights. The study calls for a comprehensive data protection regime in the country, enhancement of institutional capacities and a rights-based approach to cybersecurity regulation. Good cyber governance should not only safeguard against digital risks faced by individuals and institutions, but also respect privacy, freedom of expression and due process in compliance with constitutional and international human rights principles.

Keywords: Cybercrime, Data Protection, Prevention of Electronic Crimes Act 2016, Digital Rights, Privacy, Cybersecurity, Pakistan, Information Technology Law

Policy Journal of Social Science Review



ISSN Online:3006-4635

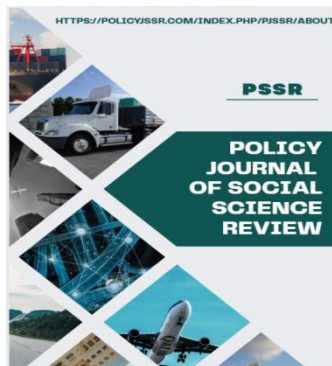
ISSN Print: 3006-4627

1. Introduction

The digital revolution has been like no other in history, and is redefining the ways in which people communicate, do business, gain access to information and connect with government institutions. Digital landscape has also seen rapid evolution in Pakistan: internet penetration has grown, smart phone usage is prevalent, online financial services are flourishing and reliance on digital platforms is increasing in the everyday life of the citizens. The digital revolution has opened up ample opportunities for the economic and social growth of Pakistan. Online businesses, digital banking systems, freelancing platforms and electronic government services have made things more convenient and efficient. In addition, the development of the information technology industry has helped provide jobs and to advance the economy. (Saleem et al, 2025) But with greater reliance on digital devices have also come new vulnerabilities. As technology systems have become the instruments through which cybercrimes are committed, they are the prime targets of the cybercriminals. Cybercriminals exploit technological systems to perpetrate offences that traditional criminal laws were not intended to handle. Cybercrime doesn't respect borders, often is committed by anonymous perpetrators, and requires technical skills to be investigated and prosecuted. Cybercrime encompasses a

variety of illegal activities that are carried out using digital networks. These comprise unauthorized access to computer systems and electronic fraud, identity theft, cyber harassment, online financial frauds, data theft, and attacks on critical information infrastructure. (Masudi, J. A., & Mustafa, N. 2023) Governments, businesses and individuals all around the world have been facing challenges as a result of the growing sophistication of cyber threats. The abuse of the internet has emerged as a significant issue in Pakistan given the rapid adoption of the internet and a lack of awareness about internet security and institutional issues. People are more vulnerable to online financial fraud, misuse of personal information, harassing messages and messages or stealing personal information online than ever before. To tackle these emerging challenges, the government of Pakistan has passed Prevention of Electronic Crimes Act (PECA), 2016. The law contains definitions of different kinds of cybercrime and outlines how the crimes would be investigated and prosecuted. It also makes provisions for the responsibilities of relevant institutions towards combating cybercrime. (Noorani, G. M. 2025) Although PECA is regarded as very important, there are debates on its effectiveness and implementation. Some critics say the law needs to be updated to reflect new technology risks, others point to the issues of privacy and freedom of

Policy Journal of Social Science Review



ISSN Online:3006-4635

ISSN Print: 3006-4627

expression or the potential for misuse of legal authority. Data protection also has become significant in Pakistan. Today, with the digitalization of the economy, personal data is a resource that governments, businesses, financial institutions, and online platforms are acquiring. If there are no appropriate protection mechanisms in place, personal data can be used inappropriately, shared and used for unlawful purposes. In contrast to other countries which have comprehensive privacy legislation, Pakistan is in the process of forming a full-fledged data protection framework. With no clear data protection regime, there are questions about how personal data should be collected, processed, stored and protected. The present research investigates the linkage between regulation of cybercrime and data protection in Pakistan. It reviews current laws and legal structures, identifies implementation issues, considers human rights questions, and recommends amendments to the current law to promote a secure and rights-based digital space. (Saleem et al, 2024)

2. Research Objectives

The objectives of this research are:

- 1.To examine the existing legal framework governing cybercrime in Pakistan.
- 2.To analyze the effectiveness of the Prevention of Electronic Crimes Act, 2016.
- 3.To identify major challenges in cybercrime investigation and enforcement.

4.To examine data protection issues within Pakistan's digital environment.

5.To evaluate cybercrime regulation from a human rights perspective.

6.To suggest legal and institutional reforms for stronger digital rights protection.

3. Research Methodology

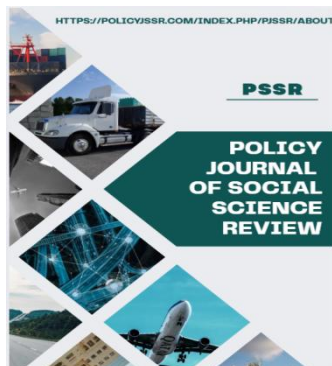
This study is a qualitative and analytical research using the legal and interdisciplinary analysis approach. The research methodology adopted by the researcher in the study is mainly secondary sources which are related to the Pakistani laws and policies, international reports, research articles, comparative legal sources and constitutional provisions etc. The legal provisions, including the Prevention of Electronic Crimes Act, 2016, constitutional rights and new data protection frameworks, are examined using a doctrinal legal research approach. The study also includes a comparative analysis, with examples of other international approaches to cybersecurity and privacy regulation. This research addresses identifying gaps between legal provisions and practice. It analyses whether the legal framework existing in Pakistan is effective in providing protection to the fundamental rights and dealing with modern cyber threats.

4. Conceptual Understanding of Cybercrime

4.1 Definition of Cybercrime

Cybercrime is defined as any crime that is committed using computers, digital

Policy Journal of Social Science Review



ISSN Online:3006-4635

ISSN Print: 3006-4627

networks, electronic devices, or information systems. Cybercrime differs from traditional crimes in that the criminals are typically able to remain anonymous and victims are often located anywhere in the world. (Bhatti, A., & Afraz, T. 2025)

Cybercrime may involve computers as:

- 1.Targets of crime – such as hacking, malware attacks, and unauthorized access.
- 2.Tools for committing crime – such as online fraud and identity theft.
- 3.Platforms for communication and exploitation – such as cyber harassment and digital abuse.

Cybercrime is complex and needs expertise and specific legislation to tackle technology-driven crimes, as traditional criminal justice mechanisms are inadequate.

4.2 Major Forms of Cybercrime in Pakistan

A. Unauthorized Access and Hacking

Unauthorized access when someone accesses a computer system, network, or digital account without permission. The hackers could steal information, damage systems, or exploit for financial gain or for personal use. Due to the rising trend of digital dependency, government institutions, businesses and individuals have increasingly become targets of hacking attempts in Pakistan. (Awais, F. 2025)

B. Online Financial Fraud

In Pakistan online banking, mobile payment and ecommerce have grown in the form of digital financial services at a fast pace. But this growth has created new opportunities for cybercriminals too.

Common forms include:

- Fake online shopping websites
- Phishing attacks
- Banking scams
- Fraudulent digital transactions
- Theft of financial information

These crimes are not only a financial loss, they also inflict a loss in public trust in digital services. (Muhib et al, 2025)

C. Cyber Harassment and Online Abuse

The use of digital technologies to harass, or the harassment of others, is an important social and legal problem. Social media can be the place where you often find yourself doing:

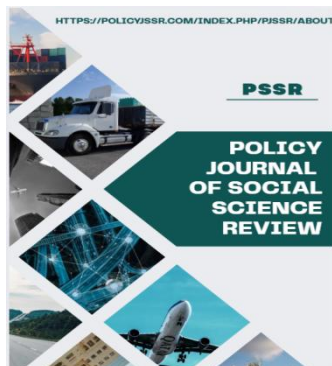
- Threats
- Blackmail
- Unauthorized sharing of personal information
- Online stalking
- Digital harassment

Women and vulnerable groups are particularly affected by online abuse, making cybercrime regulation an important human rights issue. (Khan, A. U. A. 2025)

D. Identity Theft and Data Misuse

Identity theft is the unauthorized use of someone's personal information. Identity documents, financial data or online

Policy Journal of Social Science Review



ISSN Online:3006-4635

ISSN Print: 3006-4627

accounts could be used fraudulently by criminals. With increasing personal data available online, legal systems face a big challenge in protecting digital identities. (Munir, A. 2025)

5. Evolution of Cybercrime Legislation in Pakistan

5.1 Early Legal Developments

In the absence of the comprehensive cybercrime legislation, Pakistan had to resort to general criminal laws and regulations relating to electronic transactions for dealing with technology related offences. One of the earliest attempts to give electronic documents and to recognize digital communication in the law is the Electronic Transactions Ordinance, 2002. But it didn't have enough provisions to deal with contemporary cyber crimes. Digital technologies developed at a fast pace, necessitating specific legislation that would be able to address cyber threats. (Hadi, M. J. 2024)

5.2 Prevention of Electronic Crimes Act (PECA), 2016: A Critical Analysis

PECA 2016 is the country's first-ever comprehensive law against electronic crimes. The Act had the goal of preventing unauthorized activities being used in information systems, to control use of electronic communication and to create possibilities for investigation and prosecution of cyber crimes. PECA gives legal recognition to different types of

cybercrime and empowers the relevant authorities with investigative powers. It includes offences arising from unauthorized access, electronic fraud, data theft, cyber harassment, cyberstalking and offences against the dignity and privacy of individuals. The fact that PECA was introduced was significant because it recognized that digital crimes need to be treated in a particular way, using a specialized legal approach. Despite a few years in operation, doubts have been raised about its effectiveness, coverage and interrelationship with basic rights. (Mohammed, F. 2016)

5.3 Major Provisions of PECA, 2016

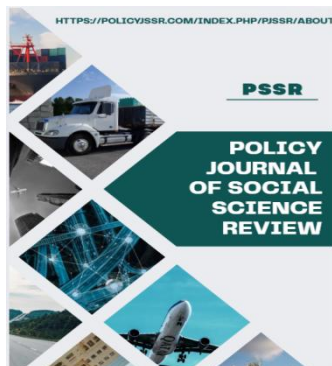
A. Unauthorized Access to Information Systems

PECA makes it a crime to hack into info systems and data. This is to ensure the security of computer networks, digital accounts and electronic information against unauthorized access. With the proliferation of online banking systems, government databases, and business information systems, unauthorized access has become more and more important. To implement these provisions, technical knowledge and up-to-date investigative skills are needed. (Ahmed et al, 2026)

B. Data Theft and Unauthorized Use of Information

The Act offers a safeguard against unauthorized access, copying, or use of electronic information. This becomes a

Policy Journal of Social Science Review



ISSN Online:3006-4635

ISSN Print: 3006-4627

crucial point especially as personal and organizational information has become a valuable asset in the digital world. But criminal penalties are not enough to achieve data protection there should be a robust system of data collection, processing and storage rules for organizations. (Dhirani, L. L. 2024)

C. Electronic Fraud

Electronic fraud provisions are for crimes committed with deceit using electronic technology. Such crimes involve fraudulent electronic transactions, manipulation of electronic information for financial gain, and online scams. In Pakistan, electronic transactions and the use of online marketplaces has become a significant issue as it allows for increasing instances of fraud. It is difficult for many victims to claim financial losses as a result of problems in investigating and identifying cybercriminals. (Ullah, S et al 2015)

D. Cyber Harassment and Cyberstalking

One of the most significant achievements of PECA is that online harassment is defined as a criminal act. The law protects against the misuse of digital platforms threatening, intimidating or harming a person. This is especially relevant for women and vulnerable groups who are victims of online violence. However, it has to be implemented in a manner that allows for easy access to complaints, the sensitive handling of complaints and the prevention

of further harm occurring to victims. (Imam, D.S, 2024)

6. Institutional Framework for Cybercrime Enforcement in Pakistan

6.1 Federal Investigation Agency (FIA) Cyber Crime Wing

The Federal Investigation Agency (FIA) has been the main body to investigate cybercrime cases in Pakistan in the past. The Cyber Crime Wing was created to investigate complaints relating to the electronic crimes and carry out technical investigations. (Bhatti, A., & Afraz, T. 2025)

The agency performs several functions, including:

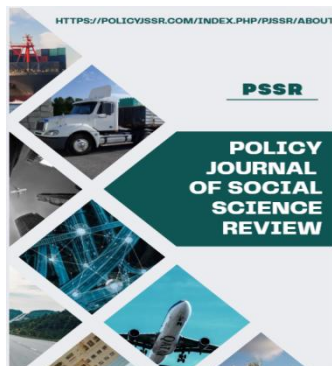
- Receiving cybercrime complaints
- Conducting digital investigations
- Collecting electronic evidence
- Identifying cybercriminals
- Assisting prosecution authorities

The FIA Cyber Crime Wing is vital but is beset with various challenges such as limited resources, a rising number of complaints, an inadequate number of technical experts and the challenge of dealing with the rapidly evolving technology. (Baloch, A., & Abid, A. 2026)

6.2 Challenges in Cybercrime Investigation

Cybercrime investigations can be quite unique and vary greatly from normal criminal investigations. Specialized collection, preservation and analysis methods are required for digital evidence. (Haque, E et al 2023)

Policy Journal of Social Science Review



ISSN Online:3006-4635

ISSN Print: 3006-4627

Major challenges include:

Technical Complexity

The cybercriminals are constantly finding new ways as well, such as new methods of fraud, encrypted communications, and anonymous digital networks. Ongoing training is essential for effective responses by law enforcement. (Ahmad, W., Asghar, U., & Afzal, M. 2025)

International Nature of Cybercrime

In many cases of cybercrime, both the perpetrators and victims are from different countries, as are the digital infrastructure. Cooperation between the international community is thus necessary for investigation and prosecution.

Digital Evidence Management

The electronic evidence is easily modified, deleted or transferred. Investigators should adhere to procedures to ensure reliability and admissibility of digital evidence in a court of law.

7. Data Protection Challenges in Pakistan

7.1 Absence of Comprehensive Data Protection Legislation

Pakistan lacks a full-fledged Data Protection Law, similar to international standards, in the current digital landscape, which is one of the key drawbacks in the country's legal system. PECA aims to tackle some types of illegal access and misuse of data, but doesn't cover the entire data lifecycle.

A modern data protection framework should address:

- Collection of personal information
- Purpose of data processing
- Consent requirements
- Data storage and security
- Rights of individuals over their information
- Responsibilities of organizations handling personal data

If there is no such law, then the person might not be legally protected against misuse of their personal information. (Azhar et al, 2025)

7.2 Personal Data and Privacy Risks

Digital platforms collect large amounts of personal information, including:

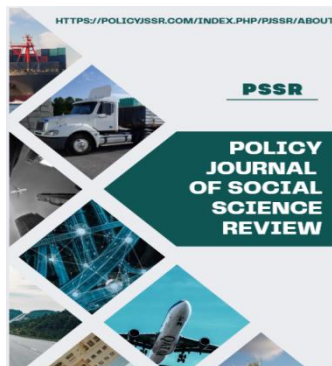
- Names
- Identification details
- Financial information
- Location data
- Online activities
- Communication records

Government departments, banks, online businesses, and social media platforms process personal data on a daily basis. (Shabbir, N., & Adnan, M. 2025)

Weak data protection mechanisms create risks such as:

- Unauthorized disclosure of information
- Identity theft
- Financial fraud
- Surveillance concerns
- Commercial misuse of personal information

Policy Journal of Social Science Review



ISSN Online:3006-4635

ISSN Print: 3006-4627

Protection of personal data is therefore directly connected with the constitutional right to dignity and privacy.

7.3 Data Protection and Businesses

Increasingly, businesses in Pakistan are depending on customer data for digital services and marketing activities. Ecommerce businesses, financial institutions and tech firms gather a lot of consumer data. But if there are no legal requirements, companies might not have enough of an incentive to implement robust data security measures. (Bint Sohrab et al, 2024) A comprehensive data protection law should put responsibilities on businesses as follows:

- Secure handling of customer information
- Notification of data breaches
- Limiting unnecessary data collection
- Ensuring transparency in data processing

8. Human Rights Perspective of Cybercrime Regulation in Pakistan

Cybercrime regulation must balance two important objectives:

1. Protecting individuals and society from digital harm.
2. Protecting fundamental rights in the digital environment.

Excessive regulation or misuse of cyber laws may negatively affect freedom, privacy, and democratic participation. (Ahmad, M. T., & Habib, R. I. 2026)

8.1 Right to Privacy

The right to privacy is a fundamental human right, which is recognized all over the world and enshrined in the constitution of Pakistan. The dignity and privacy of home is guaranteed under Article 14 of the Constitution of Pakistan. In the digital era, privacy goes beyond boundaries of physical space and extends to safeguarding personal information and online identities. The individual's right to privacy and dignity can be adversely affected by unauthorized access, data breaches and misuse of their personal information. Thus, cybercrime legislation should provide adequate safeguards against digital privacy breaches. (Abbas et al, 2023)

8.2 Freedom of Expression

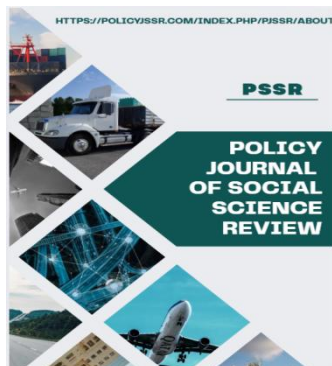
Digital platforms have been a part of the political, educational, and social life. The Constitution of Pakistan guarantees the freedom of speech and expression of every individual (Article 19) with reasonable lawful restrictions. Cybercrime legislation needs to strike a balance between detection of online abuse and the protection of free expression. Excessively general limits could deter legal communication and public involvement. (Aftab, s. 2024)

A rights-based approach demands restrictions to online expression must be:

- Clearly defined by law
- Necessary for legitimate purposes
- Proportionate to the harm being addressed

8.3 Due Process and Fair Investigation

Policy Journal of Social Science Review



ISSN Online:3006-4635

ISSN Print: 3006-4627

Those suspected of committing cybercrimes should be treated fairly based on the principles of justice and due process. Important safeguards include:

- Transparent investigation procedures
- Protection against arbitrary action
- Right to legal representation
- Independent judicial review

Cybersecurity should not become a justification for violating fundamental legal protections.

9. Comparative Analysis: International Approaches and Lessons for Pakistan

9.1 European Union: General Data Protection Regulation (GDPR)

The European Union General Data Protection Regulation (GDPR) is one of the most robust data protection laws in the world.

GDPR emphasizes:

- Individual control over personal data
- Transparency in data processing
- Strong organizational responsibilities
- Rights to access and delete personal information
- Accountability of data controllers

Pakistan can learn from GDPR principles by developing a framework that places individuals at the center of data protection. (Hoofnagle et al, 2019)

9.2 India's Digital Data Protection Framework

With the rise in digital transformation, India's government has enacted laws

regarding personal data protection. India's response shows how vital it is to define clear responsibilities for organizations dealing with personal information and provide enforcement mechanisms. The technological and social context in both Pakistan and India is comparable and lessons can be learned from it for Pakistan's future regulations. (Burman, A. 2022)

10. Recommendations for Legal and Institutional Reform

Based on the analysis, the following reforms are recommended:

10.1 Enact Comprehensive Data Protection Legislation

Pakistan requires a dedicated data protection law that clearly defines:

- Rights of individuals
- Duties of organizations
- Data processing standards
- Penalties for violations
- Independent regulatory mechanisms

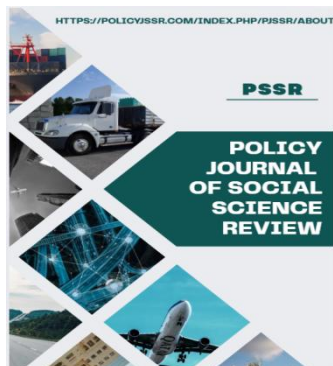
Such legislation should align with international privacy standards while considering Pakistan's social and legal environment.

10.2 Strengthen Cybercrime Investigation Institutions

Law enforcement agencies require:

- Advanced digital forensic facilities
- Specialized training programs
- Increased technical experts
- Better coordination with international agencies

Policy Journal of Social Science Review



ISSN Online:3006-4635

ISSN Print: 3006-4627

Cybercrime cannot be effectively controlled without improving investigative capacity.

10.3 Establish Public Cybersecurity Awareness Programs

Many cybercrime victims lack knowledge about digital safety.

Government institutions, educational organizations, and private companies should promote:

- Online safety education
- Responsible digital behavior
- Awareness regarding financial scams
- Protection of personal information

10.4 Develop Specialized Cybercrime Courts

Cybercrime cases often involve complex technical evidence. Specialized judicial mechanisms may improve:

- Understanding of digital evidence
- Speed of case resolution
- Quality of legal decisions

Judges and prosecutors should receive specialized training in technology-related legal issues.

10.5 Maintain Balance between Security and Rights

Cybersecurity policies must protect both national interests and individual freedoms. Pakistan should adopt a human-centered approach where digital security measures respect:

- Privacy
- Freedom of expression
- Equality
- Due process

11. Conclusion

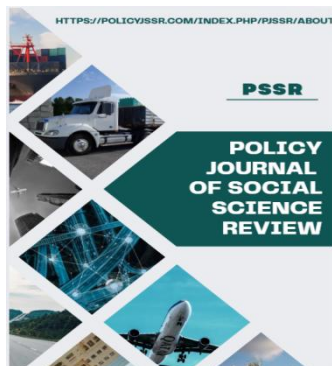
The swift advancement of digital technology has reshaped the social and economic landscape of Pakistan both in terms of opportunity and challenges such as cybercriminal activities and data security issues. Online fraud, identity theft, hacking and digital harassment are all emerging types of cyber offences which have become widespread and which need a strong legal and institutional response.

Prevention of Electronic Crimes Act, 2016 is a step towards combating cybercrime in Pakistan. It sets a legal framework for the investigation and prosecution of electronic crimes. Still, technology is changing at a rapid pace and associated legal changes are needed for this.

One of the key challenges is the lack of a comprehensive data protection framework that can safeguard individuals' personal data in the digital world. A strong cybersecurity strategy involves criminalization as well as prevention, privacy and accountability measures, which are all necessary.

Building trust amongst citizens, businesses, and government institutions is crucial for the future of Pakistan's digital development. A robust and progressive cybercrime framework, in line with good data protection measures, can foster innovation in digital technologies and ensure the protection of fundamental rights.

Policy Journal of Social Science Review



ISSN Online:3006-4635

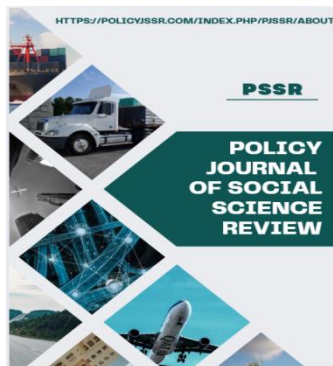
ISSN Print: 3006-4627

The objective of cyber law should not only be controlling digital threats but also creating a secure, fair, and rights-based digital society. Pakistan needs to create a balance between cybersecurity and freedom of expression through enhancing institutions, strengthening legislation and implementing international best practice.

References

- 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*, 09732586231206913.
- Aftab, S. (2024). Right to Privacy and Freedom of Expression in the Constitution of Pakistan. In *Comparative perspectives on the right to privacy: Pakistani and European experiences* (pp. 99-126). Cham: Springer Nature Switzerland.
- Ahmad, M. T., & Habib, R. I. (2026). The Prevention of Electronic Crimes Act, 2016: Balancing Cybercrime Control and Freedom of Online Expression in Pakistan. *Pakistan Journal of Humanities and Social Sciences*, 14(1), 368-375.
- Ahmad, N. M., & Asghar, M. S. (2025). Privacy as a Legal Right: A Comparative Study Between Pakistan and Malaysia. *Journal of Arts and Linguistics Studies*, 3(1), 839-858.
- Ahmad, W., Asghar, U., & Afzal, M. (2025). An analysis of the effectiveness of FIA cyber crime laws in preventing and investigating online fraud in Pakistan: Challenges and recommendations. *Research Consortium Archive*, 3(2), 836-852.
- Awais, F. (2025). Enhancing legal frameworks to address cybercrime in the digital age: A critical perspective. *UCP Journal of Law & Legal Education*, 3(2), 56-82.
- Azhar, S., Rizvi, S. A. A., & Asghar, U. (2025). Criminal procedure code in Pakistan: Evaluating the process and challenges in investigating crimes. *The Critical Review of Social Sciences Studies*, 3(2), 789-799.
- Aziz, O., Siraj, M. A., & Rehman, A. (2021). Privacy challenges in cyber security against cybercrime in digital forensic. *A systematic literature review in Pakistan. Journal of Computing & Biomedical Informatics*, 2(02), 158-164.
- Baloch, A., & Abid, A. (2026). Cybercrime Regulation in Pakistan: An Assessment of the Prevention of Electronic Crimes Act, 2016 and the Role of Law Enforcement Agencies in Comparative Perspective. *Social Science Review Archives*, 4(2), 2825-2845.
- Bhatti, A., & Afraz, T. (2025). Digital Innovation, Data, And Rights:

Policy Journal of Social Science Review

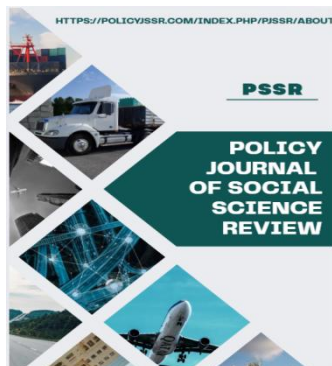


ISSN Online:3006-4635

ISSN Print: 3006-4627

- Reassessing Pakistan's Intellectual Property and Cyber Law Framework. Data, And Rights: Reassessing Pakistan's Intellectual Property and Cyber Law Framework (November 28, 2025).
- Bint Sohrab, L., Shah, K., & Nawaz, B. (2024). Bridging The Gap: Cross-Border Data Flows & Data Protection Harmonization In Pakistan. *Journal Of Social Sciences Development*, 3(3), 232-247.
- Brenner, S. W. (2010). *Cybercrime: Criminal Threats from Cyberspace*. Praeger.
- Burman, A. (2022). Will India's Proposed Data Protection Law Protect Privacy and Promote Growth?. *Carnegie Endowment for International Peace*.
- Council of Europe. (2018). *European Ethical Charter on the Use of Artificial Intelligence in Judicial Systems*.
- European Union. (2016). *General Data Protection Regulation (GDPR), Regulation (EU) 2016/679*.
- Government of Pakistan. (2016). *Prevention of Electronic Crimes Act, 2016*.
- Government of Pakistan. *Constitution of the Islamic Republic of Pakistan*.
- Hadi, M. J. (2024). *Safeguarding Critical Infrastructures Through Data Protection Laws: A Comparative Study with a Focus on Pakistan*. Available at SSRN 4730720.
- Haque, E. U., Abbasi, W., Murugesan, S., Anwar, M. S., Khan, F., & Lee, Y. (2023). Cyber forensic investigation infrastructure of Pakistan: an analysis of the cyber threat landscape and readiness. *Ieee Access*, 11, 40049-40063.
- Hoofnagle, C. J., Van Der Sloot, B., & Borgesius, F. Z. (2019). The European Union general data protection regulation: what it is and what it means. *Information & communications technology law*, 28(1), 65-98.
- Imam, D. S. (2024). *Cyber bullying in Pakistan: The silent menace*. Centre for Governance Research.
- Khan, A. U. A. (2025). *Cyber Crime in Pakistan: Trends, Challenges, and Legal Responses*: <https://doi.org/10.55966/assaj>. 2025.4. 1.080. *ASSAJ*, 4(01), 1358-1366.
- Kshetri, N. (2019). Cybercrime and cybersecurity in developing countries. *Journal of Global Information Technology Management*.
- Masudi, J. A., & Mustafa, N. (2023). *Cyber security and data privacy law in Pakistan: Protecting information and privacy in the digital age*. *Pakistan Journal of International Affairs*, 6(3), 1-11.

Policy Journal of Social Science Review



ISSN Online:3006-4635

ISSN Print: 3006-4627

- Mohammed, F. (2016). PECA 2015: A Critical Analysis of Pakistan's Proposed Cybercrime Bill. *UCLA J. Islamic & Near EL*, 15, 71.
- Muhib, M., Muhib, K., & Muhib, Z. (2025). Pakistan's Cyber Laws and International Legal Standards on Digital Rights. *Policy Journal of Social Science Review*, 3(3), 151-165.
- Munir, A. (2025). Cybercrime Laws and Digital Privacy in Pakistan. Available at SSRN 5950694.
- Noorani, G. M. (2025). Data protection laws in Pakistan: challenges and opportunities. *Pakistan Journal of Law and Technology*, 6, 364-374.
- OECD. (2013). Privacy Guidelines: OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data.
- Saleem, B., Ahmed, M., Zahra, M., Hassan, F., Iqbal, M. A., & Muhammad, Z. (2024). A survey of cybersecurity laws, regulations, and policies in technologically advanced nations: A case study of Pakistan to bridge the gap. *International Cybersecurity Law Review*, 5(4), 533-561.
- Saleem, H. A. R., Bukhtiar, A., Zaheer, B., & Farooq, M. A. U. (2025). Challenges faced by the judiciary in implementing cybersecurity laws in Pakistan. *The Critical Review of Social Sciences Studies*, 3(1), 1052-1066.
- Shabbir, N., & Adnan, M. (2025). Cyber Security: A Growing Challenge to Pakistan. *Annals of Human and Social Sciences*, 6(1), 372-384.
- Solove, D. J. (2004). *The Digital Person: Technology and Privacy in the Information Age*. New York University Press.
- Ullah, S., Amir, M., Khan, M., Asmat, H., & Habib, K. (2015, November). Pakistan and cyber crimes: Problems and preventions. In *2015 First International Conference on Anti-Cybercrime (ICACC)* (pp. 1-6). IEEE.
- United Nations. (1948). *Universal Declaration of Human Rights*.
- United Nations. (1966). *International Covenant on Civil and Political Rights*.
- Wall, D. S. (2007). *Cybercrime: The Transformation of Crime in the Information Age*. Polity Press.
- Zahoor, R., & Razi, N. (2020). Cyber-crimes and cyber laws of Pakistan: An overview. *Progressive Research Journal of Arts & Humanities (PRJAH)*, 2(2), 133-143.