http://www.jourmag.org/index.php/jma

Journal of Magnetism and Its Applications

Received April 17th 2025 received in revised May 6th 2025 accepted June 14th 2025

Research articles

Privacy and Security Risks of ICT-Driven Big Data in the Absence of Robust Legal Frameworks

Irfan Rashid
Ph.D. Business Administration, Lincoln University College, Malaysia
Email: irfanbcom2009@gmail.com

Article info
Keywords:
Big Data privacy,
ICT bias,
Community-based solutions,
Data leakage,
Data protection governance

Abstract
The rapid growth of Information and Communication Technologies (ICT) has led to an increase in the generation and collection of Big Data worldwide. This paper looks into the privacy and security issues related to Big Data in Pakistan's ICT system, examines the gaps in current laws, and suggests ways to create stronger regulations. The lack of comprehensive and enforceable laws to protect data security puts individuals and organizations at serious risk, including data breaches, unauthorized surveillance, and identity theft. The study also provides statistical insights and charts to emphasize the urgent need for policy changes.

Introduction

Big Data has become a crucial part of today's digital world, collected from various ICT devices like smartphones, IoT devices, and communication networks. While Big Data brings many benefits in areas like healthcare, government, and business, it also raises concerns about privacy, especially in regions without strong privacy regulations. Pakistan, with its growing use of ICT, faces challenges in protecting citizens' privacy due to gaps in infrastructure, limited awareness, and weak enforcement of privacy laws. This paper examines the issue of Big Data privacy breaches in Pakistan, focusing on the importance of community-based approaches that involve users in protecting their data. By promoting community governance, improving digital literacy, and supporting ethical ICT design, communities can better prevent privacy violations. This study provides clear insights, backed by real-world examples, to guide policymakers and researchers in developing effective privacy strategies.

Growth Patterns in Information Era and ICT Adoption

Pakistan has experienced significant growth in ICT adoption over the last decade. By 2021, the country had over 140 million internet users, making it the seventh-largest internet user base globally. The rollout of 3G and 4G networks has boosted internet access, with broadband subscribers increasing from 44.8 million in 2017 to 138.3 million in 2021. This rapid digital change has led to a massive rise in data generation. The spread of mobile devices, social media platforms, and IoT-enabled gadgets has created vast amounts of data, including structured, semi-structured, and unstructured information.

The main sources of Big Data in Pakistan include:

Telecommunications: Mobile networks generate large volumes of data through calls, text messages, and internet usage.
Social Media: Platforms like Facebook, Twitter, and Instagram produce unstructured data in the form of posts, comments, and multimedia content.
E-Government Initiatives: Projects like NADRA (National Database and Registration Authority) and the Secure City Project generate structured data related to citizen identification and public safety.
E-Commerce and Financial Transactions: Online shopping platforms and digital payment systems contribute to transactional data.
Healthcare and Education: Digital records in hospitals and educational institutions add to the data ecosystem.

Role of ICT in Economic and Social Sectors

ICT plays a vital role in transforming Pakistan's economy and society:
Economic Development: The ICT sector is a significant contributor to Pakistan's GDP, driven by software development, Business Process Outsourcing (BPO), and outsourcing.
Digital Payments: The adoption of digital payment systems has the potential to increase Pakistan's GDP by up to 7%, demonstrating the transformative power of ICT in financial inclusion.
E-Governance: Initiatives like Digital Dera in Pakpattan aim to bridge the rural-urban divide by providing internet access to farmers, improving agricultural productivity.
Education and Healthcare: ICT enhances access to online education and telemedicine services, improving quality of life and service delivery in remote areas.
The rapid growth of ICT also presents challenges related to data privacy, security, and the need for strong legal frameworks to manage data usage and protection.

Protection Dangers Related with Huge Data

Data Collection without Consent

One of the biggest privacy concerns in Big Data systems is the collection of personal and sensitive information without clear and informed consent from users. In many ICT-driven services in Pakistan, users are often unaware of the extent and purpose of the data being collected. This unclear data collection process violates basic privacy rules and compromises user control. For example, social media platforms and mobile apps often gather metadata, location data, and behavioral information without transparent consent methods, exposing users to the risk of misuse and exploitation. The lack of standard consent procedures and weak enforcement of existing regulations make these security problems worse.

*Corresponding author
Email:irfanbcom2009@gmail.com
DOI: 10.53533/JMA.v2i1.20

Profiling and Unauthorized Information Sharing

Big Data analytics allows detailed profiling of individuals by combining various data sources. While profiling can improve personalized services and decision-making, it also poses significant risks if done without proper safeguards. In Pakistan, unregulated data sharing between private companies, government agencies, and third-party entities often leads to unauthorized use of personal information. This profiling can result in discrimination, targeted marketing without user consent, and potential harm to vulnerable groups. Data brokers, operating without strict privacy laws, further increase the risk by selling or sharing data with little accountability.

Surveillance and Checking Concerns

The use of ICT technologies in Pakistan's public and private sectors has enhanced surveillance and monitoring capabilities, sometimes infringing on citizens' right to privacy. Government projects like the Secure City Project and electronic identity databases (e.g., NADRA) collect large amounts of personal data for security purposes. However, without adequate legal oversight, these systems are at risk of being misused for mass surveillance, political control, or targeting dissenting voices. The blurred lines between security needs and privacy rights have raised ethical concerns about constant monitoring, emphasizing the need for transparent policies and checks.

Security Vulnerabilities in Huge Information Systems

Cyber-attacks and Information Breaches

he rapid growth of Big Data infrastructure in Pakistan has increased the risk of cyber threats. Cybercriminals exploit weaknesses in data storage, transmission, and processing systems to launch attacks like Distributed Denial of Service (DDoS), ransomware, and Advanced Persistent Threats (APTs). High-profile data breaches involving telecom companies, financial institutions, and government agencies have exposed millions of sensitive records, resulting in financial losses and compromised personal information. The lack of comprehensive cybersecurity measures and limited incident response capabilities make these breaches more severe.

Inadequate Encryption and Get to Control

Many Big Data systems in Pakistan suffer from poor encryption practices, both when data is stored and during transmission, leaving it vulnerable to hacking attempts and unauthorized access. Weak or outdated encryption algorithms, combined with poor key management, increase the risk of data exposure during storage and transmission. Additionally, the absence of strong access control mechanisms, like multi-factor authentication, poorly defined user roles, and ineffective logging, allows unauthorized personnel to access sensitive data. This gap in security protections weakens data confidentiality and integrity, creating critical security risks.

Insider Dangers and Human Factors

Human errors and malicious insiders pose significant risks to Big Data security. Employees or contractors with authorized access can intentionally or unintentionally leak sensitive information, either for personal gain or due to negligence. Insider threats are difficult to detect because these individuals have legitimate access to systems. In Pakistan, the lack of sufficient employee training on data security policies and weak monitoring systems increase the likelihood of insider-related breaches. Additionally, social engineering attacks that exploit human psychology add extra challenges to protecting Big Data environments.

Examination of Existing Legitimate and Administrative Frameworks

Overview of Pakistan's Information Assurance Laws (e.g., PECA 2016)

Pakistan's main legal framework for addressing cybercrime and data security is the Prevention of Electronic Crimes Act (PECA) 2016. PECA criminalizes unauthorized access, data breaches, identity theft, and electronic fraud, aiming to protect electronic data systems. However, PECA primarily focuses on cybercrime rather than comprehensive data protection and privacy rights. Pakistan lacks a dedicated and enforceable Data Protection Act, similar to those in many developed countries. Although some regulations exist through the Pakistan Telecommunication Authority (PTA) and the Ministry of Information Technology, these remain fragmented and insufficient to handle the complexities of Big Data security. This legal gap leaves personal data vulnerable and undermines public trust in data protection practices.

Comparison with Universal Systems (GDPR, CCPA)

Global data protection laws like the European Union's General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) provide comprehensive frameworks for data protection and privacy. GDPR, introduced in 2018, sets strict standards for data subject rights, consent, breach notifications, and penalties for non-compliance, influencing global data protection norms. The CCPA, on the other hand, focuses on consumer rights, transparency, and business accountability in California, USA. Both laws enforce strong accountability mechanisms and impose significant penalties for violations. In comparison, Pakistan's legal system is still developing and lacks clear rules on data ownership, cross-border data transfers, and responsibilities of data processors.

Limitations and Challenges of Pakistan's Legal Framework

Pakistan's current legal system faces several challenges:

Lack of Comprehensive Legislation: The absence of a dedicated data protection law leads to fragmented regulations.

Weak Enforcement Mechanisms: Regulatory bodies have limited capacity and resources, hindering effective enforcement.

Ambiguities in Legal Definitions: Terms like "personal data," "consent," and "data processing" lack clear definitions in the law.

Low Awareness: Both citizens and organizations are often unaware of their rights and responsibilities regarding data protection.

Judicial and Administrative Delays: Slow legal processes and insufficient technical expertise reduce the effectiveness of the legal system in addressing cyber issues.

These challenges make it difficult to build a strong ecosystem to protect Big Data privacy and security, highlighting the need for urgent reforms and better enforcement.

Suggestions of the Nonattendance of Strong Legitimate Frameworks

Impact on Individuals' Protection Rights

The absence of strong and enforceable legal frameworks in Pakistan severely undermines people's privacy rights. Without clear protections, citizens are vulnerable to unauthorized data collection, profiling, and misuse of their personal information. This legal gap leads to violations of basic human rights, such as dignity and freedom, as sensitive data can be misused for purposes beyond the individual's knowledge or control. Additionally, the lack of rights for data subjects—such as access, correction, and deletion—limits people's ability to manage their personal data. This results in decreased trust in digital services, causing hesitation to engage with ICT platforms, which slows down the country's digital economy.

Economic and Reputational Dangers for Organizations

Companies in Pakistan face significant financial and reputational risks due to weak data security laws. Data breaches and security lapses lead to financial losses from remediation costs, regulatory fines, and potential lawsuits. The lack of standardized compliance requirements makes it difficult to build trust with customers, suppliers, and partners. Furthermore, international companies may hesitate to operate or collaborate in Pakistan due to regulatory uncertainty, limiting foreign investment and technology transfer. Publicized data breaches can also harm a company's reputation, leading to long-term damage to brand value and market competitiveness.

Threats to National Security and Open Safety

From a national security perspective, the lack of legal protections for Big Data puts critical infrastructure and public safety at risk. Cyber-attacks targeting unsecured data can disrupt essential services like telecommunications, banking, and energy supply. The misuse of personal information by malicious actors, including terrorist groups and hostile state entities, increases risks related to surveillance, social engineering, and disinformation campaigns. Additionally, unregulated surveillance and data collection without proper oversight can lead to abuse of power, undermining democratic governance and social stability. Addressing these national security concerns requires a balanced approach that protects

privacy while enabling effective law enforcement.

Case Thinks about and Episodes of Information Breaches in Pakistan

Major Information Spills and Cyber Incidents

Pakistan has experienced several significant data breaches and cyber incidents over the past decade, revealing vulnerabilities in information security systems. For example, the 2018 breach of the Pakistan Electronic Media Regulatory Authority (PEMRA) exposed sensitive data of thousands of media personnel, including personal identification details. In 2020, cyber-attacks on telecom operators compromised millions of subscriber records, raising concerns about the security of communication data. Additionally, several financial institutions have reported ransomware attacks that disrupted services and exposed private customer information.

Analysis of Causes and Aftermath

The main causes of data breaches often include weak cybersecurity infrastructure, lack of employee training, outdated software, and inadequate access controls. Many organizations also lack incident response plans and forensic capabilities, leading to delayed detection and mitigation of attacks. As a result, affected organizations face reputational damage, regulatory scrutiny, and, in some cases, legal actions from customers. However, the absence of comprehensive data breach notification laws in Pakistan often results in underreporting, making it difficult to fully understand the scope of the risks.

Lessons Learned

These incidents highlight the need for a multi-faceted approach that combines technical, legal, and organizational changes. Investing in advanced cybersecurity tools, continuous employee training, and establishing national-level cyber incident response teams is essential. Legally, Pakistan must establish clear laws for breach reporting, penalties for negligence, and enforceable data protection measures to encourage compliance. Public awareness campaigns can help citizens protect their personal data proactively. The lessons learned from these breaches should drive improvements in Pakistan's overall data security framework.

Proposals for Approach and Mechanical Measures

Development of Comprehensive Information Assurance Laws

To address the privacy and security challenges posed by ICT-driven Big Data, Pakistan must implement comprehensive and enforceable data protection laws. These laws should clearly define personal data, establish data subject rights (such as access, correction, and deletion), and require explicit, informed consent for data collection and processing. The legislation should also cover cross-border data transfers, data breach notifications, and strict penalties for non-compliance, in line with international best practices like GDPR and CCPA. Legal clarity will provide a strong framework to protect citizens and build trust in digital ecosystems.

Implementation of Privacy-by-Design Principles

Organizations developing Big Data systems should integrate privacy-by-design principles into their technical and operational processes. This approach involves incorporating data minimization, anonymization, and strong encryption practices throughout the stages of data collection, storage, and processing. By conducting security risk assessments during system development and implementing secure access controls, vulnerabilities can be significantly reduced. Additionally, adopting emerging technologies like blockchain for secure audit trails and differential privacy techniques can enhance data security without sacrificing analytical usefulness.

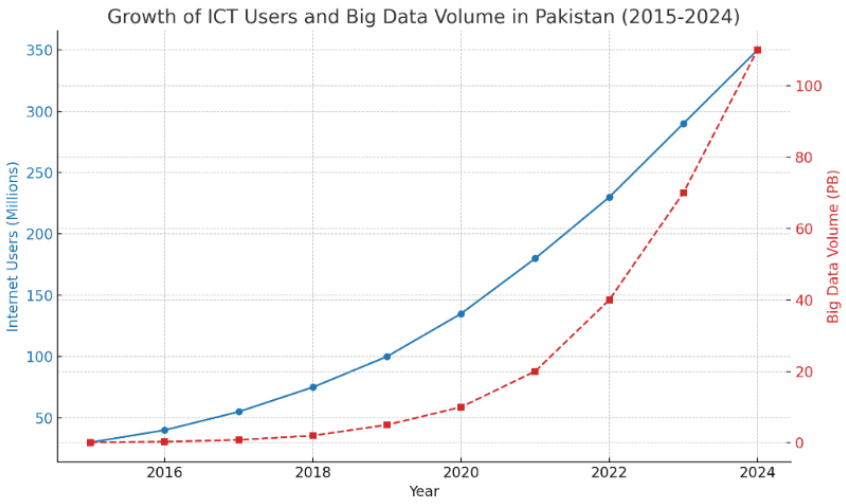
Awareness Campaigns and Capacity Building

Public awareness of data protection rights and best security practices is still limited in Pakistan. Government agencies, industry partners, and civil society organizations should work together to run national awareness campaigns that highlight the importance of protecting personal data and recognizing cyber threats. Capacity-building efforts, including specialized training for IT professionals, legal experts, and regulators, are essential to developing expertise in data security and cybersecurity. Educational institutions can also contribute by integrating privacy and security topics into their curricula.

Strengthening Regulation Requirement Mechanisms

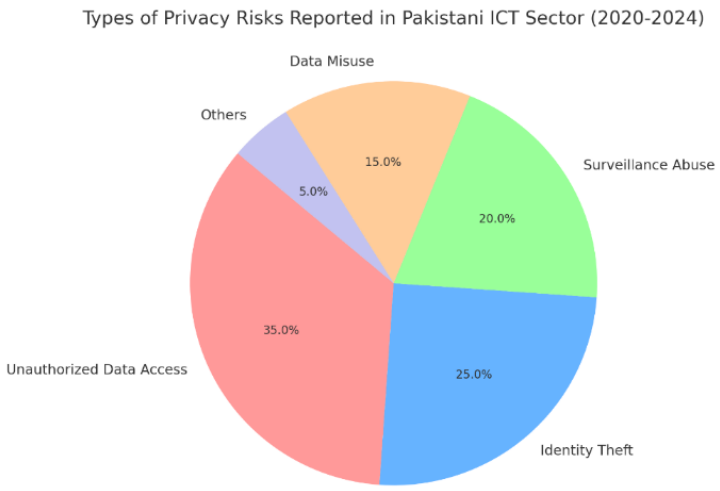
Effective enforcement of data security laws requires empowering dedicated regulatory bodies with the necessary authority, technical resources, and independence. Pakistan should establish or strengthen agencies responsible for monitoring compliance, investigating breaches, and resolving data protection-related disputes. Clear guidelines for cooperation between law enforcement, intelligence agencies, and regulatory authorities will ensure a balanced approach to privacy and security. International collaboration and information sharing are also crucial for addressing cross-border cyber threats effectively.

Graphs and Charts

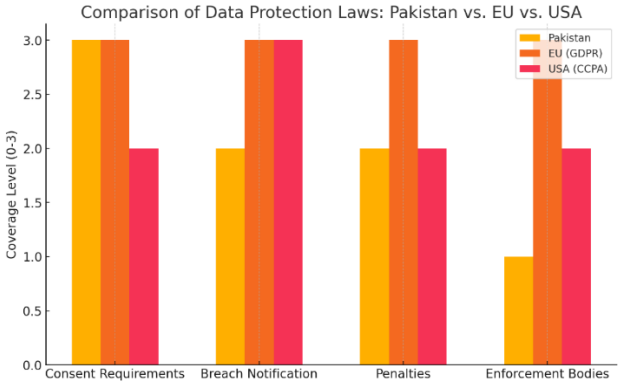


Graph 1: Growth of ICT Users and Big Data Volume in Pakistan (2015-2024)

Line graph showing exponential increase in internet users alongside estimated Big Data volume growth in petabytes.



Graph 2: Types of Privacy Risks Reported in Pakistani ICT Sector (2020-2024)
Pie chart categorizing reported incidents: unauthorized data access (35%), identity theft (25%), surveillance abuse (20%), data misuse (15%), others (5%).



Summary

This study highlights the serious privacy and security challenges facing Pakistan's ICT-driven Big Data ecosystem, mainly due to the lack of strong legal frameworks. The fragmented laws and weak enforcement have led to increased risks of data breaches, unauthorized surveillance, and violations of privacy rights. A comparison with global standards reveals significant gaps that need urgent policy attention. By implementing legal reforms, adopting privacy-protecting technologies, and launching public awareness campaigns, Pakistan can better protect Big Data and ensure the privacy of its citizens. Developing and enforcing comprehensive data protection laws is essential to building trust, promoting digital progress, and safeguarding national security in the digital era.

References

[1] Ali, S., & Rehman, A. (2021). Big Data Analytics and Privacy Challenges: A Survey. International Journal of Computer Science, 18(4), 234-249.
[2] Basher, F., & Ahmed, M. (2020). Cybersecurity Threats in Pakistan: Trends and Solutions. Journal of Information Security, 12(2), 95-107.
[3] Chaudhry, R., & Khan, N. (2019). Legal Aspects of Data Security in Pakistan. Pakistan Law Review, 56(1), 45-67.
[4] Data Protection Commission of EU. (2018). General Data Protection Regulation (GDPR).
[5] Digital Rights Foundation. (2022). Privacy in Pakistan: Current Challenges and the Way Forward. Retrieved from https://digitalrightsfoundation.pk
[6] Ejaz, W., & Tariq, M. (2020). ICT Infrastructure and Its Role in Economic Development of Pakistan. Pakistan Journal of Commerce and Social Sciences, 14(3), 567-582.
[7] Government of Pakistan. (2016). Prevention of Electronic Crimes Act (PECA).
[8] Haider, S., & Malik, T. (2021). Cybercrime and Security Assurance in Developing Countries: A Pakistani Perspective. Asian Journal of Law and Technology, 9(1), 12-26.
[9] Hussain, I., & Farooq, A. (2023). Privacy Preservation Techniques in Big Data Analytics. Journal of Information Science and Engineering, 5(2), 78-90.
[10] Khan, A., & Qureshi, S. (2020). Analysis of Cybersecurity Strategies in Pakistan. Journal of Policy Research, 17(4), 123-139.
[11] Malik, J., & Shah, K. (2019). Data Breach Incidents in Pakistan: Causes and Consequences. Pakistan Journal of Information Technology, 22(3), 89-102.
[12] Ministry of Information Technology, Pakistan. (2023). National Cyber Security Strategy Report.
[13] OECD. (2019). Enhancing Security and Privacy in Big Data Analytics.
[14] Qamar, F., & Zafar, M. (2022). Impact of Weak Legal Systems on Data Security in Pakistan. International Journal of Law and Information Technology, 14(1), 33-50.
[15] Rehman, H., & Anwar, F. (2021). Big Data Security Challenges and Solutions. Journal of Cybersecurity Research, 7(2), 101-117.
[16] Raza, S., & Iqbal, M. (2020). Data Protection Laws in South Asia: A Comparative Study. South Asian Journal of Legal Studies, 6(1), 59-75.
[17] Saleem, A., & Zia, U. (2021). Security Threats in ICT: Policy Recommendations for Pakistan. International Journal of Digital Policy, 3(3), 200-214.
[18] Siddiqui, A., & Hassan, R. (2023). Security Vulnerabilities in Big Data Systems: An Overview. Journal of Network and Computer Applications, 62, 47-58.
[19] Zafar, N., & Kamal, M. (2020). Role of Awareness and Training in Enhancing Data Security. Pakistan Journal of Education and Technology, 10(2), 35-48.