GARP INTERNATIONAL JOURNAL OF NATURAL AND APPLIED SCIENCES

https://garp.org.ng/gijnas

Vol. 1, Issue I, Pp.25-29; Apr., 2026

DATA PROTECTION AND PRIVACY IN THE ERA OF BIG DATA

[1]OMOROGBE, Osasu Harry PhD., [2]URIRI, Omena Ofajemu &

[3]AMENAGHAWON, Vincent Airuoyuwa PhD.

[1]Department of Cybersecurity, Igbinedion University, Okada. Edo State, Nigeria;

[2&3]Computer Science and Information Technology. Igbinedion University Okada, Nigeria

[1]omorogbe.harry@iuokada.edu.ng ; [2]uriri.omena@iuokada.edu.ng

[3]vincent.amen@iuokada.edu.ng https://orcid.org/0000-0002-6864-3665

ARTICLE INFO

Received Date: 24th Mar. 2026
Date Revised Received: 10th Apr. 2026
Accepted Date: 28th Apr. 2026
Published Date: 13th May. 2026

Citation: Omorogbe, O. H; Uriri, O. O. & Amenaghawon, V. A (2026): Data Protection and Privacy in the Era of Big Data; GARP INTER J. of Natural & App. Sci. Vol. 1, Issue I, Pp.25-29, Apr. 2026.

Abstract

The rapid advancement of digital technologies, cloud computing, artificial intelligence, and big data analytics has transformed the global information landscape. Organizations across sectors increasingly rely on data-driven systems to improve operational efficiency, enhance decision-making, and deliver personalized services. However, the widespread collection, storage, and processing of personal information have raised significant concerns regarding privacy, cybersecurity, and unauthorized data access. Data breaches, cyberattacks, identity theft, and misuse of personal information have become common challenges in the digital age. This article examines the concept of data protection and privacy within the context of big data environments. It explores the importance of data protection, major threats to information security, relevant regulatory frameworks, and best practices organizations can adopt to safeguard sensitive information. The study concludes that effective data protection requires strong legal frameworks, technological safeguards, organizational accountability, and continuous public awareness to ensure privacy and trust in digital systems.

Keywords: Data Protection; Big Data; Cybersecurity; Cloud Computing; Digital Privacy

Introduction

The rapid expansion of the digital economy has fundamentally transformed the ways information is created, collected, processed, stored, and disseminated across the globe. Technological innovations such as high-speed internet connectivity, smartphones, social media platforms, cloud computing, the Internet of Things (IoT), blockchain systems, and artificial intelligence have contributed to an unprecedented increase in digital data generation. Individuals, organizations, and governments now produce enormous volumes of data daily through online transactions, social networking activities, electronic health systems, financial services, e-commerce platforms, and smart devices. This continuous flow of information has led to the emergence of what scholars describe as “big data,” a concept characterized by massive, rapidly generated, and highly diverse datasets that exceed the processing capabilities of traditional data management systems (Mayer-Schönberger & Cukier, 2013).

Big data is commonly defined using the “5Vs” framework: volume, velocity, variety, veracity, and value. Volume refers to the enormous quantity of data generated every second; velocity describes the speed at which data is produced and processed; variety represents the different forms of structured and unstructured data; veracity concerns the reliability and accuracy of data; while value emphasizes the usefulness of data in decision-making processes (Khan et al., 2021). The integration of advanced analytics, machine learning, and artificial intelligence technologies has enabled organizations to extract meaningful insights from large datasets for strategic planning, predictive analysis, and service improvement.

In recent years, big data technologies have become central to the operations of governments, healthcare institutions, educational organizations, financial institutions, and multinational corporations. For example, healthcare organizations utilize big data analytics to improve disease diagnosis, patient monitoring, and medical research, while financial institutions apply predictive analytics to detect fraudulent transactions and assess customer behavior (Agarwal & Dhar, 2023). Similarly, social media companies collect and analyze user-generated content to personalize advertisements and enhance user experiences. Educational institutions also rely on learning analytics and student data systems to monitor academic performance and improve educational outcomes.

Despite its numerous benefits, the rapid growth of big data has raised serious concerns regarding privacy, cybersecurity, and ethical data usage. The large-scale collection and storage of personal information expose individuals and organizations to risks such as data breaches, unauthorized access, surveillance, identity theft, and cyberattacks. According to Dwivedi et al. (2023), the increasing dependence on digital technologies has intensified global concerns about data governance, consent management, and the responsible use of personal information. Consequently, governments and regulatory bodies worldwide are introducing stricter data protection laws and cybersecurity frameworks to ensure that organizations manage personal information responsibly and transparently.

Organizations in sectors such as healthcare, banking, education, telecommunications, and government increasingly depend on data analytics to improve productivity, enhance customer experience, and support strategic planning. For instance, healthcare institutions use patient data to improve medical diagnosis, while financial institutions rely on customer data analytics to detect fraud and improve banking services. Educational institutions also utilize student data for learning analytics and academic performance monitoring.

Despite these benefits, the rapid expansion of digital technologies has created serious concerns regarding privacy and data security. Personal information such as financial records, biometric data, medical histories, online activities, and social interactions are constantly collected and processed by organizations. The misuse or unauthorized exposure of such information can lead to identity theft, financial fraud, reputational damage, and violations of individual privacy rights (Westin, 1967).

Data protection refers to the policies, technologies, and practices designed to safeguard personal and sensitive information from unauthorized access, disclosure, destruction, or misuse. According to Solove (2021), data protection has become a fundamental issue in modern societies because individuals increasingly lose control over how their personal information is collected and shared online. Governments and international organizations have therefore introduced legal and regulatory

frameworks aimed at protecting privacy and ensuring responsible data management practices.

Concept of Data Protection and Privacy

Data protection involves the implementation of technical, administrative, and legal measures to secure information throughout its lifecycle. It ensures that data is collected lawfully, stored securely, processed fairly, and used only for authorized purposes. Privacy, on the other hand, refers to an individual's right to control personal information and determine how such information is shared or used (Omorogbe,, 2025). The increasing adoption of big data technologies has complicated privacy management because organizations often collect massive amounts of user information without adequate transparency. Big data systems can analyze behavioral patterns, predict consumer preferences, and influence decision-making processes. While these capabilities improve organizational efficiency, they also raise ethical concerns regarding surveillance and excessive data collection (Zuboff, 2019).

Importance of Data Protection

Protection of Personal Privacy

One of the primary objectives of data protection is safeguarding individual privacy rights. Personal information such as names, addresses, medical records, and financial details must be protected from unauthorized disclosure. Individuals expect organizations to handle their data responsibly and ethically.

Prevention of Identity Theft and Cybercrime

Weak data protection mechanisms increase the risk of cybercrime and identity theft. Cybercriminals exploit security vulnerabilities to steal sensitive information for fraudulent activities. Strong cybersecurity measures such as encryption, firewalls, and multi-factor authentication help reduce these risks (Whitman & Mattord, 2021).

Regulatory Compliance

Organizations are legally required to comply with data protection laws and regulations. Failure to comply may result in heavy financial penalties, lawsuits, and reputational damage. Regulatory frameworks such as the General Data Protection Regulation (GDPR) in Europe emphasize transparency, accountability, and lawful processing of personal data.

Organizational Trust and Reputation

Consumers are more likely to trust organizations that prioritize data security and privacy protection. Effective data protection practices improve customer confidence and strengthen organizational reputation. According to Cisco (2023), organizations with strong privacy policies often experience increased customer loyalty and competitive advantage.

Challenges of Data Protection in the Big Data Era

Data Breaches

Data breaches remain one of the most serious cybersecurity challenges globally. Unauthorized access to databases can expose confidential information belonging to millions of users. Major organizations have experienced large-scale data breaches resulting in financial losses and reputational damage.

Cloud Computing Risks

Cloud computing provides scalable and cost-effective data storage solutions; however, it also introduces security concerns related to data ownership, access control, and third-party management. Improper cloud configurations may expose sensitive information to attackers (Hashizume et al., 2013).

Weak Password and Authentication Systems

Poor password practices and inadequate authentication mechanisms continue to contribute to unauthorized access incidents. Many users still rely on weak or repeated passwords across multiple platforms, making systems vulnerable to cyberattacks.

Insider Threats

Employees or contractors with authorized access to systems may intentionally or unintentionally compromise organizational data security. Insider threats can result from negligence, lack of awareness, or malicious intent.

Lack of User Awareness

Many internet users lack adequate knowledge regarding online privacy and data security practices. Users frequently share personal information on social media platforms without understanding the potential risks associated with data misuse.

Regulatory Frameworks for Data Protection

Several international and national regulations have been introduced to strengthen privacy protection and data governance.

General Data Protection Regulation (GDPR)

The GDPR, implemented by the European Union in 2018, is one of the most comprehensive data protection laws globally. It grants individuals greater control over their personal data and requires organizations to ensure transparency in data collection and processing activities.

Nigeria Data Protection Act (NDPA)

Nigeria introduced the Nigeria Data Protection Act to regulate the processing of personal data and strengthen privacy rights. The Act aims to ensure lawful handling of personal information and improve cybersecurity practices within organizations operating in Nigeria.

California Consumer Privacy Act (CCPA)

The CCPA provides California residents with rights regarding the collection, use, and sharing of personal information by businesses.

- Best Practices for Data Protection
- Data Minimization
- Organizations should collect only the information necessary for specific operational purposes. Excessive data collection increases privacy risks and storage vulnerabilities.

Encryption Technologies

Encryption converts readable data into coded formats that can only be accessed using authorized decryption keys. Encryption is essential for protecting sensitive information during storage and transmission.

Access Control Mechanisms

Organizations should implement strict access control systems to ensure that sensitive information is accessible only to authorized personnel.

Employee Training and Awareness

- Cybersecurity awareness programs help employees recognize phishing attacks, suspicious activities, and unsafe online practices. Human error remains a major contributor to cybersecurity incidents.
- Backup and Disaster Recovery Systems
- Regular data backups enable organizations to recover critical information following cyberattacks, hardware failures, or accidental data loss.

Regular Security Audits

Periodic security assessments help organizations identify vulnerabilities and strengthen their cybersecurity infrastructure.

Conclusion

Data protection and privacy have become critical concerns in the era of big data and digital transformation. While data-driven technologies provide numerous economic and social benefits, they also expose individuals and organizations to cybersecurity threats, privacy violations, and ethical challenges. Effective data protection requires a combination of legal compliance, technological safeguards, organizational accountability, and public awareness. Governments, businesses, and individuals must collaborate to ensure responsible data management and protect privacy rights in increasingly digital societies. As technology continues to evolve, data protection will remain an essential component of cybersecurity and digital governance.

References

Agarwal, R., & Dhar, V. (2023). Big data, data science, and analytics: The opportunity and challenge for IS research. *Information Systems Research, 34*(1), 1–16.

Cisco. (2023). *Data privacy benchmark study*. Cisco Systems.

Dwivedi, Y. K., Hughes, L., Baabdullah, A. M., Ribeiro-Navarrete, S., Giannakis, M., Al-Debei, M. M., Dennehy, D., Metri, B., Buhalis, D., Cheung, C. M. K., Conboy, K., Doyle, R., Dubey, R., Dutot, V., Felix, R., Goyal, D. P., Gustafsson, A., Hinsch, C., Jebabli, I., ... Wamba, S. F. (2023). Metaverse beyond the hype: Multidisciplinary perspectives on emerging challenges, opportunities, and agenda for research, practice and policy. *International Journal of Information Management, 66*, 102542.

Hashizume, K., Rosado, D. G., Fernández-Medina, E., & Fernandez, E. B. (2013). An analysis of security issues for cloud computing. *Journal of Internet Services and Applications, 4*(1), 1–13.

Khan, N., Yaqoob, I., Hashem, I. A. T., Inayat, Z., Mahmoud Ali, W. K., Alam, M., Shiraz, M., & Gani, A. (2021). Big data: Survey, technologies, opportunities, and challenges. *The Scientific World Journal, 2021*, 712826.

Mayer-Schönberger, V., & Cukier, K. (2013). *Big data: A revolution that will transform how we live, work, and think*. Houghton Mifflin Harcourt.

Omorogbe, O. H. & Amenaghawon, V.A. (2026) Development of an Embedded Artificial Intelligence Framework for Intelligent E-Learning Management Systems GAIJIST Vol.1.1.2026 pp.20-24

Omorogbe, O. H., Eduje, A. I., Anyanwu, L., Obande, B.O, Ukaoha, K. C., Izevbuwa, O. G., Ighotuweyin, A. F., & Arenvbaguehita, O. D. (2025). The impact of artificial intelligence (AI) on fraud detection in banks in Edo State. GAS Journal of Engineering and Technology (GASJET), 2(9), [26-35)

Omorogbe, O. H., Obande, B. O., Amoforitse, F. I., Eduje, A. I., & Omoregie, D. A. (2025). Ensuring a secure future by insuring against cybercrime: A study of Okada Micro Finance Bank, Okada, Edo State. GAS Journal of Engineering and Technology, 2(5), 27–31

Solove, D. J. (2021). *Understanding privacy*. Harvard University Press.

Tavani, H. T. (2016). *Ethics and technology: Controversies, questions, and strategies for ethical computing* (5th ed.). Wiley.

Westin, A. F. (1967). *Privacy and freedom*. Atheneum.

Whitman, M. E., & Mattord, H. J. (2021). *Principles of information security* (7th ed.). Cengage Learning.

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Public Affairs.