World Journal of Advanced Research and Reviews
eISSN: 2581-9615 CODEN (USA): WJARAI
Cross Ref DOI: 10.30574/wjarr
Journal homepage: https://wjarr.com/

(REVIEW ARTICLE)

Check for updates

E-Data protection and privacy in the digital age: Risks, ethics and regulatory challenges

Mathias Ndungu *

Kogod School of Business, American University, Washington DC, USA.

World Journal of Advanced Research and Reviews, 2026, 30(01), 2193-2196

Publication history: Received on 15 March 2026; revised on 20 April 2026; accepted on 23 April 2026

Article DOI: https://doi.org/10.30574/wjarr.2026.30.1.1081

Abstract

The rapid expansion of digital platforms has fundamentally altered how personal data is generated, collected, stored, and reused. Individuals continuously produce electronic data through social media interactions, public email communications, open-access journals, online forums, and other digital services often without full awareness of the long-term implications. This study examines e-data protection and privacy challenges arising from the persistent and replicable nature of digital information. It highlights how data collected at one point in time can be repurposed or weaponized against individuals later in life, regardless of changes in opinion, maturity, exposure, or socio-cultural context. The paper explores ethical concerns, legal frameworks, technological vulnerabilities, and governance mechanisms surrounding electronic data protection. Findings suggest that while regulatory efforts have improved awareness and compliance, gaps remain in enforcement, cross-border data handling, and protection against misuse of publicly available data. Strengthening privacy-by-design approaches, legal harmonization, and digital literacy is essential to safeguarding individual rights in an increasingly data-driven society.

Keywords: E-Data Protection; Privacy; Digital Footprint; Social Media Data; Public Information; Cyber Ethics; Data Governance

1. Introduction

The digital age has ushered in unprecedented access to information, connectivity, and knowledge sharing. At the same time, it has created an environment in which vast amounts of personal data are continuously generated, collected, archived, and analyzed. Data about individuals is routinely gathered through social media platforms, public email communications, open-access journals, online discussions, and free digital services. While much of this data is shared voluntarily, its long-term persistence and secondary use present significant risks to personal privacy and autonomy(Estrada-Galiñanes & Wac, 2020; Lupton, 2016).

Unlike traditional forms of personal information, electronic data is rarely temporary. In the rapidly evolving landscape of data, driven by unparalleled technological progress by way of Posts made on social media, opinions expressed in public forums, academic contributions to free journals, or statements sent through public or semi-public email systems can be stored indefinitely, duplicated endlessly, and redistributed without the original author's consent(Splichal, 2022). This permanence means that information created during adolescence, early adulthood, or periods of limited exposure can later be interpreted out of context and used against individuals professionally, socially, politically, or legally despite natural changes in beliefs, values, and understanding over time(Park, 2022; Wisniewski, Vitak, & Hartikainen, 2022).

A critical concern in e-data protection is that digital records do not evolve with the individual. Human opinions change with age, education, cultural exposure, and life experience; however, digital artifacts remain static and

* Corresponding author: Mathias Ndungu

searchable(Cheryl & Ng, 2022). Employers, institutions, governments, and malicious actors may retrieve historical data to judge present behavior, often without considering context, intent, or personal growth(Bhadouria, 2022). This creates ethical dilemmas where individuals are effectively denied the right to evolve beyond their digital past.

The widespread availability of "free" platforms further complicates privacy protection. Many services monetize user data through profiling, behavioral analysis, and targeted advertising, often under opaque terms and conditions. Publicly accessible data while legally shared can be aggregated, correlated, and exploited in ways that were never anticipated by the data subject(Mileros & Forchheimer, 2025; Yannopoulos, 2024). As digital ecosystems become more interconnected, the boundary between private and public data continues to erode, increasing exposure to identity theft, reputational harm, surveillance, and discrimination(Mushtaq & Shah, 2025).

E-data protection and privacy, therefore, are no longer purely technical issues; they represent socio-technical and ethical challenges that affect human rights, freedom of expression, and digital equity. This paper explores the foundations of electronic data protection, the risks associated with publicly available personal data, and the effectiveness of existing legal and technological safeguards in addressing privacy threats in a rapidly evolving digital landscape.

2. Understanding E-Data and Digital Footprints

Electronic data (e-data) refers to any information created, transmitted, or stored in digital form. This includes structured data such as database records and unstructured data such as emails, social media posts, images, videos, and academic publications(Abdallah, 2023). Every digital interaction contributes to a digital footprint, which can be categorized as either active data deliberately shared by users or passive data collected automatically through tracking technologies, cookies, and metadata(Abdallah, 2023).

Digital footprints are cumulative and difficult to erase. Even when users delete content, copies may persist on third-party servers, backups, or data aggregation platforms. The aggregation of multiple data sources enables detailed profiling, allowing organizations to infer sensitive attributes such as political views, religious beliefs, or behavioral tendencies, even when such information was never explicitly disclosed(Mbah, 2022).

3. Privacy Risks Associated with Publicly Available Data

Publicly accessible data is often perceived as harmless due to its open nature. However, when combined across platforms and over time, such data can be weaponized. Old social media posts may be resurfaced to discredit individuals, academic opinions may be misused to imply fixed ideological positions, and email leaks can expose private contexts to public scrutiny(Tran, 2022).

One major risk lies in contextual collapse, where information intended for a specific audience is interpreted by a different one. Additionally, data permanence undermines forgiveness and personal growth, creating a digital environment where past mistakes or outdated views remain perpetually accessible. This raises questions about fairness, proportionality, and the right to be forgotten.

4. Legal and Regulatory Frameworks for E-Data Protection

Governments and international bodies have introduced data protection regulations to address privacy concerns. Frameworks such as the General Data Protection Regulation (GDPR) emphasize principles of consent, data minimization, purpose limitation, and user rights(Labadie & Legner, 2023). However, enforcing these principles becomes challenging when dealing with publicly shared data, cross-border platforms, and decentralized data storage systems(Judijanto, Solapari, & Putra, 2024).

Jurisdictional differences further complicate enforcement, as data collected in one country may be processed or stored in another with weaker protections. This fragmentation limits individuals' ability to seek redress and places disproportionate power in the hands of large digital platforms.

5. Technological Approaches to Privacy Protection

Technological solutions play a vital role in e-data protection. Encryption, anonymization, access control mechanisms, and privacy-by-design architectures help reduce exposure to unauthorized data use. Emerging technologies such as

differential privacy and decentralized identity systems aim to give users greater control over their personal data(Alanzi & Alkhatib, 2022).

However, technology alone cannot solve privacy challenges. Poor implementation, user negligence, and economic incentives to exploit data often undermine technical safeguards. Effective protection requires aligning technological solutions with ethical design and regulatory oversight(Haber & Carmeli, 2023).

6. Ethical Dimensions of Data Use and Retention

Beyond legality, ethical considerations are central to e-data protection. Organizations must consider whether it is morally justifiable to store and reuse data indefinitely, especially when it can harm individuals who have changed over time. Ethical data governance calls for proportionality, contextual awareness, and respect for human development(Dhirani, Mukhtiar, Chowdhry, & Newe, 2023).

There is growing recognition that individuals should not be permanently defined by historical digital expressions. Ethical frameworks increasingly advocate for contextual integrity, where data use aligns with the original context in which it was shared(Wong, 2023).

7. Future Directions in E-Data Protection and Privacy

The future of e-data protection lies in stronger global cooperation, improved regulatory harmonization, and enhanced digital literacy. Users must be educated about the long-term consequences of data sharing, while platforms must be held accountable for transparent data practices. Advances in artificial intelligence and big data analytics further increase the urgency of proactive privacy safeguards(Wong, 2023).

Developing mechanisms that allow individuals greater control over data lifecycle management—including modification, contextualization, and deletion will be essential in balancing innovation with fundamental rights.

8. Conclusion

E-data protection and privacy are critical challenges in a world where personal information is continuously generated and preserved. Data gathered from social media platforms, public emails, and open-access sources can outlive personal growth and be misused irrespective of changes in opinion, age, or exposure. While legal and technological measures have made progress, significant gaps remain in protecting individuals from long-term digital harm.

A sustainable approach to e-data protection requires integrating legal frameworks, ethical principles, technological safeguards, and user awareness. By recognizing the human capacity for change and contextual evolution, digital systems can be designed to protect privacy while still enabling knowledge sharing and innovation in the digital age. This commentary explores the complex dynamics between data, theory, and truth in the context of rapid technological advancements.

References

[1] Abdallah, A. O. (2023). The Role of E-Data Management in Enhancing Records Keeping in Primary Education in Mbeya City Council, Tanzania. The Open University of Tanzania.

[2] Alanzi, H., & Alkhatib, M. (2022). Towards improving privacy and security of identity management systems using blockchain technology: A systematic review. Applied Sciences, 12(23), 12415.

[3] Bhadouria, A. S. (2022). Study of: Impact of malicious attacks and data breach on the growth and performance of the company and few of the world's biggest data breaches. International Journal of Scientific and Research Publications, 10(10), 1-11.

[4] Cheryl, B.-K., & Ng, B.-K. (2022). Protecting the unprotected consumer data in internet of things: Current scenario of data governance in Malaysia. Sustainability, 14(16), 9893.

[5] Dhirani, L. L., Mukhtiar, N., Chowdhry, B. S., & Newe, T. (2023). Ethical dilemmas and privacy issues in emerging technologies: A review. Sensors, 23(3), 1151.

[6] Estrada-Galiñanes, V., & Wac, K. (2020). Collecting, exploring and sharing personal data: why, how and where. Data Science, 3(2), 79-106.

[7] Haber, L., & Carmeli, A. (2023). Leading the challenges of implementing new technologies in organizations. Technology in Society, 74, 102300.

[8] Judijanto, L., Solapari, N., & Putra, I. (2024). An Analysis of the Gap Between Data Protection Regulations and Privacy Rights Implementation in Indonesia. The Easta Journal Law and Human Rights, 3(01), 20-29.

[9] Labadie, C., & Legner, C. (2023). Building data management capabilities to address data protection regulations: Learnings from EU-GDPR. Journal of Information Technology, 38(1), 16-44.

[10] Lupton, D. (2016). Personal data practices in the age of lively data. Digital sociologies, 2016, 335-350.

[11] Mbah, G. O. (2022). Data privacy and the right to be forgotten. World Journal of Advanced Research and Reviews, 16(2), 1216-1232.

[12] Mileros, M. D., & Forchheimer, R. (2025). Free for you and me? Exploring the value users gain from their seemingly free apps. Digital Policy, Regulation and Governance, 27(2), 239-257.

[13] Mushtaq, S., & Shah, M. (2025). Threats to the Digital Ecosystem: Can Information Security Management Frameworks, Guided by Criminological Literature, Effectively Prevent Cybercrime and Protect Public Data? Computers, 14(6), 219.

[14] Park, R. (2022). Forgiving Without Forgetting? Privacy in an Age of Digital Permanence.

[15] Splichal, S. (2022). Datafication of public opinion and the public sphere: How extraction replaced expression of opinion: Anthem Press.

[16] Tran, J. D. (2022). Sharing truths about the self: Theorizing news reposting on social media. International Journal of Communication, 16, 20.

[17] Wisniewski, P. J., Vitak, J., & Hartikainen, H. (2022). Privacy in adolescence Modern socio-technical perspectives on privacy (pp. 315-336): Springer International Publishing Cham.

[18] Wong, W. H. (2023). We, the data: Human rights in the digital age: MIT Press.

[19] Yannopoulos, G. (2024). The price of privacy: Assessing the legality of the consent-or-pay model for personal data processing by social media platforms.