The Ethical and Social Issues in Information Systems from Data Use, Surveillance, and Artificial Intelligence

Siti Zuhaini Abd Samah[1], Maslin Masrom[2]

[1,2]*Faculty of Artificial Intelligence*
Universiti Teknologi Malaysia,
Jalan Sultan Yahya Petra, 54100 Kuala Lumpur, Malaysia

sitizuhaini@graduate.utm.my, maslin.kl@utm.my

Article history

Received:
14 April 2026

Received in revised form:
24 April 2026

Accepted:
5 May 2026

Published online:
15 June 2026

*Corresponding author
maslin.kl@utm.my

Abstract

Digital technologies are rapidly transforming organizational operations, with Artificial Intelligence (AI) emerging as a key driver of innovation across multiple sectors. As organizations increasingly rely on Management Information Systems (MIS) to enhance productivity and service delivery, ethical concerns related to data use, surveillance, and AI have become more prominent. This paper examines the ethical and social implications of AI integration in MIS, focusing on issues of privacy, information systems management, and organizational responsibility. The study adopts a comparative analysis using ethical frameworks, including deontology, utilitarianism, the ACM Code of Ethics, and Laudon and Laudon's Five Moral Dimensions of Information Systems, to evaluate whether current technological practices align with moral and social standards. Empirical examples, such as the governance of MySejahtera, data breaches involving Maybank, ASTRO, and the Election Commission, and the use of facial recognition technologies in airports, are analyzed. The results reveal significant gaps in transparency, accountability, and system management within both public and private institutions. These shortcomings increase organizational and societal risks associated with digital information systems. This paper concludes by recommending stronger ethical governance, enhanced regulatory frameworks, improved monitoring mechanisms, and increased public awareness to promote the responsible and sustainable use of AI in MIS.

Keywords: *Management Information Systems, Artificial Intelligence, Data Privacy, Digital Ethics, Surveillance*

1. Introduction

In this era, digital technologies have become more advanced by the day. The evolution of digital technology from the personal computer (in the 1980s), towards the World Wide Web (in the 1990s), and fast forward to today, we are now dealing with cloud computing, Artificial Intelligence (AI), blockchain, and Internet of Things (IoT). In addition, the digital landscape now includes big data ecosystems, advanced machine learning algorithms, autonomous systems, smart sensors, robotic process automation (RPA), and next-generation communication tools such as 5G and quantum computing. Nowadays, we can do wonders with AI, especially in

* Corresponding author: maslin.kl@utm.my

prediction and data analysis. These advanced technologies continue to shape the world and pave the way for the future of our daily operations. With the advancement of technologies, data is a key thing that is being collected, processed, and utilized for faster and more accurate decision-making across all sectors.

These data must be managed properly to ensure accuracy, security, and accessibility. Improper handling of data may raise concerns ethically and socially. The public would be concerns on their data privacy, data security, and system management once their data is being collected. Various entities are constantly searching for data. Even simple information, such as a phone number and a name found on the internet, can be misused and exploited by the wrong people for harmful purposes.

Lack of knowledge on the Management of Information Systems (MIS) would lead to misuse of data, security breaches, data leakage, and weak data governance. Several cases of data breaches and leaks have been reported over the past few years. These incidents are caused by multiple factors, such as cyberattacks, human error, insider threats, and unauthorized system access. These real-world incidents have occurred repeatedly, indicating the need for accountability and responsible information management.

These showcase that there is a need for accountability, ethical evaluation, and better information system (IS) practice to protect the data and public rights. Therefore, it is important to refer to the ethical philosophical frameworks (such as deontology and utilitarianism), the ACM Code of Ethics, and Laudon and Laudon's five moral areas. This paper is going to analyze the work of [1] to propose recommendations for strengthening the ethical governance in Malaysia.

2. Literature Review

The addition of artificial intelligence (AI) and big data analytics into modern Management Information Systems (MIS) is a topic of debate among researchers and professionals. The worries are not only focusing on the technology itself, but also on how it may impact the people, organization, and society as a whole. In MIS, an information system is seen as more than just a tool, as it is the system that influences communication between employees, enables prompt decision making, and ensures the organization functions smoothly every day.

Technology is growing so fast that the existing ethical guidelines or regulations are unable to keep up with it [2]. This means the public is exposed to risks in data collection, storage, and use. The AI system developed may then collect a huge amount of personal data, but the people managing it may not fully understand

it, or the system may be biased or unstable. Since the technologies would affect privacy, security, and fairness, experts urge those stronger ethical rules are much needed to ensure public rights are protected and to avoid violations.

In the field of MIS, information systems do not act as just computers and software; instead, they have become socio-technical environments, meaning they can affect both social aspects (people, behaviour, and communication) and technical aspects (such as machines, data, and processes). A company can operate and function excellently using IS to communicate among the employees, for customer service, and for the leaders to make decisions. To correspond with [2], due to the rapid changes in digital technologies, organizations need to carefully design their MIS. They need to ensure the frameworks are correct, so that the data is not misused and safe practices. Ethical elements should be considered at the very beginning of developing the MIS system, such as how the data, algorithm, and user interface are being designed [3]. This is important because MIS can really affect how a company operates, and the decisions made by using MIS can affect society.

The importance of ethical analysis while developing MIS can be guided using Laudon and Laudon's Five Moral Dimensions [4]. This framework introduced five focus areas, which are the rights for information, responsibility, property rights, quality of the system, and life quality, that act as guiding questions while developing the MIS system. This framework has been used by [5] to examine modern systems like ChatGPT. The study shows that new technologies such as ChatGPT will make the MIS system even more complicated. In AI technology, for example, the ownership of data that is being used to train the AI is often unclear. The way the data is being used in AI is also vague. Accountability is also an issue, as AI cannot be held responsible for any incorrect information or biased results produced.

Besides ethical and social concerns in data use and AI, digital technologies can intrude on our personal information. [6] stated that modern surveillance technologies can collect and 'predict' or 'guess' a lot of personal information without having to request consent first! This system works by collecting patches of people's information from several sites, and they can put them together to imitate their behaviour, preference and identity. This later on raise concern on privacy rights as it slowly invades people's private lives, as they lose control of their data each day. This risk proves why a stronger and better MIS system should be in place to ensure that digital technologies are not misused and are used responsibly.

Rapid development of technologies has made the ethical framework and regulations left behind, which have made a few companies operate in a 'grey area' [2]. These companies are eager to use the MIS system but lack proper guidance and regulations. This may lead to unethical or unfair/biased decisions. This finding connects with Laudon and Laudon's framework (Quality of Life) as IS can and may affect people's lives, such as their freedom and how they are being treated. The ethical issues that may arise from this are unclear information rights, uncertain data ownership, and unreliable systems, shows that Laudon and Laudon's framework is still relevant to this day. It has helped many people, especially businesses, policy makers, and researchers, to evaluate the risks and responsibilities when it comes to modern MIS technology.

3. Analysis and Discussion

3.1 Ethical and Social Issues in Malaysia

Malaysia has recorded several data breaches between 2021 and 2022, affecting millions of users across government agencies, financial institutions, telecommunications providers, airlines, and digital platforms. These incidents are reported to have leaked sensitive personal information, which are MyKad numbers, contact details, and home addresses. These cases have proven that the existing system in place is not enough and certainly show the gaps that need to be addressed, especially in data protection [7]. Data breaches were recorded in December 2022 that impacted 13 million customers of ASTRO, Maybank, and the Election Commission (EC). This has proven that there were indeed systemic weaknesses in data security [8]. In response, government authorities have initiated investigations through agencies such as CyberSecurity Malaysia and the National Cyber Security Agency (NACSA), as these affected companies were managing large-scale datasets. The companies (ASTRO, Maybank, and EC) have actually implemented safety measures such as carrying out internal reviews, implementing enhanced security, and notifying their customer if needed. However, the recurrence of these incidents has pointed to a much broader issue, which is the cybersecurity governance, especially in access control, third-party system management, and the enforcement of data-protection standards. This also highlights the need for a stronger, robust national policy to strengthen Malaysia's digital ecosystem.

In addition to that, there was an issue with the weakness of governance and security of the MySejahtera and Malaysia Vaccine Administration System (MyVAS) system. This was captured in the Auditor-General's 2021 Report, and this incident happened due to the unauthorized 'Super Admin' account, which granted administrative permission to third-party and general users. Consequently, 3

million Malaysians were affected by this incident, which highlights the monitoring failure, lack of control for the system access, and lack of data safety & security. Ministry of Health (MOH) later took remedial actions such as deactivating the accounts, enhancing the system detection by being able to detect any unusual or suspicious activity, and strengthening their firewall. Although the system manages to recover, however, this has accidentally revealed loopholes in handling sensitive public health data [9][10]. MOH learnt that stronger governance is needed, as well as clearer responsibility and better system security need to be in place before venturing into implementing any national initiative nationwide.

As for the governance challenges surrounding AI and digital technologies in Malaysia, the concerns are, of course, much wider. Currently, the AI governance in Malaysia remains relatively decentralized and siloed, which creates ambiguity and unclear of each and every institution's role [11]. Many of the AI systems in Malaysia are still lacking in privacy safeguards, which later raised concern among citizens about the potential for misuse when deployment [5]. Essentially, some people do not embrace digital technologies, especially the latest advancements such as AI, blockchain, the IoT, and surveillance systems. These people are 'afraid' of the technology due to the lack of awareness, and the system was not clearly explained to them [12]. Therefore, to build a surveillance system that people can trust, use, and utilize, we need to employ better rules and system management, privacy built into the system from the start, and clear responsibility for each of the entities.

Studies also show that nowadays, there are AI system that uses facial recognition and surveillance tools in their service. However, these can be inaccurate for a certain group of people [13]. Digital technologies enable surveillance to be carried out using CCTV analytics. This initiative has been tried and tested at the Smart City in Iskandar Puteri, Johor, and Putrajaya. This surveillance system is supposed to detect suspicious crowd behaviour or loitering activity. However, this system is able to be biased because it can misinterpret social gatherings and normal social interactions as 'risky behaviour' [14][15]. This incident can occur when the AI models being used are not trained, have unbalanced data, not enough data, or have inconsistent camera coverage. Such bias can create unfair and unequal surveillance pressure [5], and it can concern the accountability in smart city governance.

One of the major cybersecurity incidents related to AI that has happened was the WannaCry cyber-attack on the 12th May 2017, which impacted more than 200,000 computers in over 150 countries. Among the companies affected were delivery service FedEx, carmakers Honda and Nissan, as well as the healthcare entity, the National Health Service (NHS) in the United Kingdom. This type of

malware infected the computers with a worm, encrypting users' files, and demanded a ransom payment in Bitcoin [16]. When this attack happened at the NHS, the hospital operations were disrupted, and all the patients were at risk. This is an example of digital technologies (in this case, AI technology) that, if used with malicious intention, can actually harm people, instead of making lives better.

3.2 Applying Ethical Frameworks

3.2.1 Deontological (Duty-Based) Analysis

Deontology is a theory that focuses on following the rules, responsibilities, and duties. So, in a deontological perspective, organizations have a responsibility to be transparent and trustworthy, especially when people are going to be providing data to their system (consciously or not). Informed consent by the customers has to be obtained, and data stewardship has to be in mind when handling data. Compared to incidents like MySejahtera, companies are obligated to be frank with their customers about how their data will be stored, used, and handled. Security and safety of the data should be thought at the early process of designing the system, and not after incidents happen [17][18].

3.2.2 Utilitarian (Consequentialist) Analysis

Utilitarian theory is a concept in which a decision is made after weighing the pros and cons or the impact of the decision. In this case, surveillance technology can bring benefits for using it, such as face recognition tools that enable us to make payments much safer, faster, and easier. Facial recognition is widely used, including for attendance records, unlocking phones, security clearance at airports, and more. However, this technology may have drawbacks, such as limiting people's freedom and unfairly targeting them and invading their privacy. Using the utilitarian concept, since the surveillance technology can bring betterment, but it has a trade-off, it is advisable to use the technology when it can truly benefit the people and when it can cause as little harm as possible. This means, using surveillance technology only, when necessary, in a limited, targeted, and appropriate way, not all the time, and not everywhere [13].

3.2.3 The ACM Code of Ethics

The Association for Computing Machinery **(**ACM) Code of Ethics is a set of rules for technology developers. It has clearly outlined the rules, such as avoiding harm to people, respecting people's privacy, and conducting a thorough evaluation before running the system. Cases recorded in Malaysia on data breaches show that the technology developers and AI developers in the country are still failing to

comply with the rules, due to the system not being properly tested, a lack of a comprehensive plan on data governance, and not being transparent with the customers on how their data is going to be used. The key risks of AI applications are transparency, reliability, and fairness [19][17], and these are the components that technology developers must adhere to to use the technology responsibly and safely.

3.2.4 Laudon and Laudon's Five Moral Dimensions

Laudon and Laudon's five ethical components are 5 key areas used to understand ethical problems in information systems (IS) (like digital platforms, AI systems, and data management). It can be used as a checklist to help technology developers anticipate risks and ethical considerations. Here are the five key areas in relation to ethical and social concerns in data use, surveillance, and AI.

i. Information rights – technology/ system developer needs to know what data is going to be collected, how it is managed, stored, and utilised, how it is being used, and who has access. Many Malaysians still lack clarity on how their data is being captured, like the case of MySejahtera.

ii. Property rights - customers of the system need to know who owns the rights to the information, like biometric data of facial recognition, whether the company or the consumer.

iii. Accountability and Control - who is responsible if things go wrong? For example, if an AI system discriminates against consumers, who should be blamed: the developer, the company, or the government [5][11].

iv. System Quality - making sure the system is running well and will not harm people due to poor design or weak security. This has to be in mind as data leaks are usually lacking security, safety, and proper system reliability. In the WannaCry case, it shows the need for more reliable and updated digital infrastructure [14][18].

v. Quality of life - how the system will affect the people's everyday lives. The system may impact in peoples' mental well-being, privacy, tasks, and freedom. An AI surveillance system may give some people a sense of security, but for people who are introverted, they may feel unease and feel it is invading their privacy [17].

Laudon and Laudon's Five Moral Dimension aligns with the paper by [1] on the protection, preventing harm, and preserving people's autonomy.

4. Conclusion and Recommendations

This study finds that when combines the idea from philosophy, information system ethics, and Laudon and Laudon's moral framework, we are able to grasp the situation of the complicated ethical problem of today's data practices, surveillance system and AI technology. As [1] mentioned, AI technology produces new challenges as it is relatively new and people are still trying to understand how the technology works. In Malaysia, real-world cases discussed have shown that issues such as data breaches and poor system management exist across institutions.

To prevent these incidents, we need to take drastic measures, such as strengthening enforcement of the Personal Data Protection Act (PDPA). This should be able to ensure people's rights and penalties for organizations that misuse data. Besides that, a transparency audit for the AI system can also be implemented. This would help consumers understand the system and automatically increase public trust.

On behalf of the governments of Malaysia, realizing that AI technologies have rapidly become a phenomenon, Malaysia already stepped up and came up with the National Guidelines on AI Governance and Ethics [20], which was developed by the Ministry of Science, Technology, and Innovation (Figure 1). This guideline provides ethical principles for AI that one must abide by in the governance area.

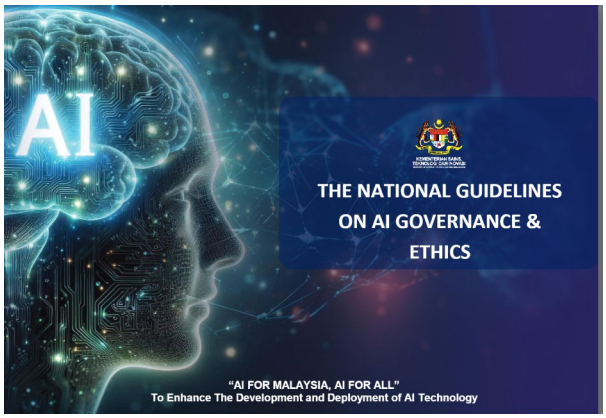

Figure 1. National Guidelines on AI Governance and Ethics [20]

Later on, the Ministry of Digital established the Malaysia National AI Office (NAIO) in December 2024, an agency responsible for accelerating AI adoption as well as ensuring responsible, transparent AI use. Ministry of Digital [21] has also recently initiated the development of the National Artificial Intelligence (AI) Action

Plan 2030, which aims to be the long-term strategy of utilizing AI for ethical and societal benefits across all sectors (Figure 2).

Figure 2. Consultation session for the National Artificial Intelligence (AI) Action Plan 2030 [21]

Malaysia needs to build a robust and stronger ecosystem for a more secure cybersecurity system and digital technologies. This would mean better monitoring tools, improve the data protection, and training more experts in cybersecurity. Besides that, it is time to enhance communication and awareness programmes to educate people about the risks and how to use digital technology ethically and responsibly. In short, managing information systems ethically is important for protecting the public's trust and ensuring that Malaysia's digital technology benefits society and improves the quality of people's lives.

Acknowledgments

The authors would like to express their appreciation to the Faculty of Artificial Intelligence, Universiti Teknologi Malaysia, for the continuous support throughout this study.

Conflicts of Interest

The authors declare that there is no conflict of interest regarding the publication of this paper.

References

[1] M. Mirbabaie, A. B. Brendel, and L. Hofeditz, "Ethics and AI in information systems research," *Communications of the Association for Information Systems*, vol. 50, pp. 726–753, 2022.
[2] C. Aprilia, "The role of ethics in business information: Narrative literature review," *Data Science: Journal of Computing and Applied Informatics*, vol. 8, no. 2, pp. 96–105, 2024. https://doi.org/10.32734/jocai.v8.i2-15855

[3] F. M. Santoro and R. M. E. M. Costa, "Towards ethics in information systems," *Journal on Interactive Systems*, vol. 12, no. 1, 2021. https://doi.org/10.5753/jis.2021.961
[4] K. C. Laudon and J. P. Laudon, *Management Information Systems: Managing the Digital Firm*. Pearson, 2020.
[5] A. Ghandour, B. J. Woodford, and H. Abusaimeh, "Ethical considerations in the use of ChatGPT: An exploration through the lens of five moral dimensions," *IEEE Access*, vol. 12, pp. 60682–60694, 2024. https://doi.org/10.1109/ACCESS.2024.3394243
[6] A. Jallauddin, "Privacy concerns and data protection in an era of AI surveillance," *International Journal of Law and Criminology*, vol. 3, no. 8, pp. 71–76, 2023.
[7] R. Loheswar, "Major data breaches in Malaysia in the past 24 months," *Malay Mail*, Dec. 31, 2022. https://www.malaymail.com/news/malaysia/2022/12/31/major-data-breaches-in-malaysia-in-the-past-24-months/47722
[8] Bernama, "Data leak claim involving Maybank, Astro and EC being probed, says Fahmi," *Daily Express Malaysia*, Dec. 30, 2022. https://www.dailyexpress.com.my/news/205202/data-leak-claim-involving-maybank-astro-and-ec-being-probed-says-fahmi/
[9] CodeBlue, "Audit: MySejahtera data breach affected three million users," Feb. 16, 2023. https://codeblue.galencentre.org/2023/02/16/audit-mysejahtera-data-breach-affected-three-million-users/
[10] E. Lee, "Court case, PAC report raise questions on need for MySejahtera app in endemic phase and other issues," *The Edge Malaysia*, Apr. 11, 2022. https://theedgemalaysia.com/article/court-case-pac-report-raise-questions-need-mysejahtera-app-endemic-phase-and-other-issues
[11] F. Said and F. Nabilah, *Future of Malaysia's AI Governance*. Institute of Strategic and International Studies (ISIS) Malaysia, 2024.
[12] A. Ergashev, "Privacy concerns and data protection in an era of AI surveillance technologies," *International Journal of Law and Criminology*, vol. 3, no. 8, pp. 71–76, 2023. https://doi.org/10.37547/ijlc/Volume03Issue08-14
[13] M. J. Mosa, A. M. Barhoom, M. I. Alhabbash, F. E. Harara, B. S. Abu-Nasser, and S. S. Abu-Naser, "AI and ethics in surveillance: Balancing security and privacy in a digital world," *International Journal of Academic Engineering Research*, vol. 8, no. 10, pp. 8–15, 2024.
[14] M. Ryan and A. Gregory, "Ethics of using smart city AI and big data: The case of four large European cities," *ORBIT Journal*, vol. 2, no. 2, 2019. https://doi.org/10.29297/orbit.v2i2.110
[15] N. A. Samsudin, M. S. F. Rosley, L. Y. Lai, S. R. Omar, M. F. Rashid, N. S. N. M. Hanifi, and I. S. Bakhtiar, "A comparative study of smart city initiatives in Malaysia: Putrajaya and Iskandar Puteri," *Planning Malaysia*, vol. 20, no. 5, pp. 14–28, 2022.
[16] D.-Y. Kao and S.-C. Hsiao, "The dynamic analysis of WannaCry ransomware," in *Proceedings of the 20th International Conference on Advanced Communication Technology (ICACT)*, IEEE, 2018, pp. 159–166. https://doi.org/10.23919/ICACT.2018.8323682
[17] U. Khalid, M. Ahmad, T. J. Chan, M. Pradana, and S. Singh, "Mediating role of digital ethics on the impact of artificial intelligence usage and public relations practices: Evidence from Malaysia," *Frontiers in Artificial Intelligence*, vol. 8, 2025. https://doi.org/10.3389/frai.2025.1662219
[18] A. Borda, A. Molnar, C. Neesham, and P. Kostkova, "Ethical issues in AI-enabled disease surveillance: Perspectives from global health," *Applied Sciences*, vol. 12, no. 8, 2022. https://doi.org/10.3390/app12083890
[19] A. McNamara, J. F. R. de Amorim, K. W. Miller, J. N. Fiesler, and R. B. Friedman, "The ACM Code of Ethics," in *Proceedings of the ESEC/FSE Conference*, 2018.
[20] Ministry of Science, Technology and Innovation, *The National Guidelines on AI Governance & Ethics*. Malaysian Science, Technology Information Centre (MASTIC), 2024. https://mastic.mosti.gov.my/publication/the-national-guidelines-on-ai-governance-ethics/
[21] Ministry of Digital, *National Artificial Intelligence Action Plan 2030 Consultation Materials*, 2025. https://ai.gov.my