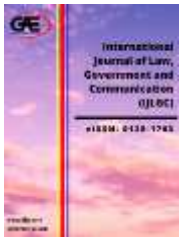
International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume: 11 Issue: 43 (March 2026) PP. 41-51



INTERNATIONAL JOURNAL OF LAW, GOVERNMENT AND COMMUNICATION (IJLGC)
www.gaexcellence.com/ijlgc

A LEGAL ANALYSIS OF MALAYSIA'S PRIVACY LAW: TOWARDS A MORE RESILIENT LEGAL FRAMEWORK IN THE DIGITAL ERA

Suharne Ismail[1]*, Zati Hanani Ismail[2], Siti Farhana Hasanudin[3], Siti Fadhilah Ghazali[4]

[1]Faculty of Business and Management Sciences, Universiti Islam Antarabangsa Tuanku Syed Sirajuddin, Perlis, Malaysia
suharne@unisiraj.edu.my https://orcid.org/0009-0008-2191-9506
[2]Faculty of Business and Management Sciences, Universiti Islam Antarabangsa Tuanku Syed Sirajuddin, Perlis, Malaysia
zatihanani@unisiraj.edu.my https://orcid.org/0009-0003-5395-7957
[3]Faculty of Business and Management Sciences, Universiti Islam Antarabangsa Tuanku Syed Sirajuddin, Perlis, Malaysia
farhana@unisiraj.edu.my https://orcid.org/0009-0004-1424-4329
[4]Faculty of Muamalat and Islamic Finance, Universiti Islam Antarabangsa Tuanku Syed Sirajuddin, Perlis, Malaysia
fadhilahghazali@unisiraj.edu.my https://orcid.org/0009-0004-0344-7569

Article Info:

Article history:
Received date: 22.12.2025
Revised date: 06.01.2026
Accepted date: 26.01.2026
Published date: 02.03.2026

To cite this document:

Ismail, S., Ismail, Z. H., Hasanudin, S. F., & Ghazali, S. F. (2026). A Legal Analysis of Malaysia's Privacy Law: Towards A More Resilient Legal Framework in The Digital Era. *International Journal of Law, Government and Communication, 11*(43), 41-51.

Abstract:

As digital technologies continue to transform industries and daily life, the protection of personal data has become a central issue in legal and policy discourse. In Malaysia, the Personal Data Protection Act 2010 (PDPA) represents a landmark statute governing data privacy in commercial contexts. However, the rapid development of technologies such as artificial intelligence, big data analytics, and cloud computing has raised concerns about the adequacy of the existing legal framework. This paper provides a legal analysis of Malaysia's privacy law, examining the effectiveness of the PDPA in addressing emerging data protection challenges in the digital era. It evaluates the PDPA's scope, enforcement mechanisms, and alignment with global standards while identifying significant gaps, particularly the exclusion of public sector data processing and limited data subject rights. Through critical examination, the study proposes key reforms aimed at strengthening Malaysia's legal framework to ensure a more comprehensive and resilient approach to privacy protection in an increasingly digitalized environment.

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume: 11 Issue: 43 (March 2026) PP. 41-51

DOI: 10.35631/IJLGC.1143004

Keyword:

Data Protection, Digital Transformation, Legal Reform, Privacy Law

Introduction

The rapid pace of digital transformation has fundamentally altered the way individuals, businesses, and governments collect, process, and share personal data. As societies become increasingly dependent on digital technologies such as cloud computing, artificial intelligence, and big data analytics, the protection of personal information has emerged as a critical legal and policy concern. This new digital ecosystem, while fostering innovation and economic growth, also heightens the risks of privacy violations, data breaches, and cybercrime. Consequently, countries around the world have sought to strengthen their privacy and data protection frameworks to address these challenges.

In Malaysia, the legal landscape governing privacy is primarily shaped by the Personal Data Protection Act 2010 (PDPA), which seeks to regulate the processing of personal data in commercial transactions. However, as the digital economy expands and new technologies disrupt traditional business models, questions have been raised about whether the existing framework remains adequate to safeguard individuals' rights. The rise of e-commerce, fintech, social media platforms, and smart technologies has intensified public concern over how personal information is collected, stored, and used, placing significant pressure on legislators and regulators to ensure that the law keeps pace with evolving threats. This article critically examines Malaysia's privacy framework in the context of digital transformation, assessing both its strengths and limitations. It explores the extent to which current legal provisions address contemporary challenges, highlights gaps and ambiguities in enforcement mechanisms, and considers lessons that may be drawn from global best practices. Ultimately, the discussion aims to contribute to the broader debate on how Malaysia can develop a more comprehensive and resilient legal regime that balances the imperatives of digital innovation with the protection of individual privacy rights.

Literature Review

The rapid digital transformation in Malaysia has generated a growing body of literature on data privacy and protection. Much of the scholarship emphasizes the inadequacy of traditional privacy laws to address contemporary challenges such as cross-border data flows, big data analytics, and the use of artificial intelligence (Rahman, 2021; Tan & Lee, 2022). The Personal Data Protection Act 2010 (PDPA), while considered a landmark statute, has been widely

critiqued for its limited scope, as it excludes federal and state government bodies and has yet to be harmonized with global standards such as the EU's General Data Protection Regulation (GDPR) (Yaacob, 2020). Comparative studies consistently note the lag in Malaysia's legislative framework when benchmarked against international best practices (Abu Bakar, 2023).

Recent literature also highlights the interplay between privacy protection and technological innovation. Studies by Norazah (2021) and Hamid et al. (2022) argue that the COVID-19 pandemic accelerated digitalization in sectors like healthcare, fintech, and education, leading to massive data collection and surveillance, which in turn raised questions on lawful processing, consent, and data minimization. These works emphasize that Malaysia's regulatory regime has struggled to keep pace with emerging technologies such as blockchain, Internet of Things (IoT), and AI-driven decision-making systems. Scholars have also discussed how industry self-regulation and corporate governance mechanisms have tried to fill these gaps, though inconsistently and with limited enforceability (Mustaffa, 2021).

From a doctrinal perspective, existing scholarship underscores a fragmented approach to privacy protection in Malaysia, shaped by statutory, common law, and sectoral regulations. For instance, case law analysis (e.g., Ghazali v Malayan Banking Berhad [2019]) suggests that the judiciary has only recently begun to explore privacy as a distinct right, and there remains an absence of constitutional recognition of privacy as a fundamental right. Furthermore, policy papers from the Malaysian Communications and Multimedia Commission (MCMC) and academic commentaries (Lim, 2022) advocate for a more robust, harmonized, and forward-looking privacy framework that integrates cyber security policies and digital economy strategies. These studies provide an important foundation for evaluating whether Malaysia's current privacy framework is adequate in addressing the demands of the digital era.

Privacy Law and Informational Privacy in The Digital Era

In Malaysia, the legal framework for privacy protection remains predominantly rooted in common law principles. Judicial approaches to privacy have historically been narrow, focusing largely on issues of morality and the chastity of women. At present, the Federal Constitution serves as the primary source of privacy-related rights (Leng, Vergara & Khan, 2021). Given the limited scope of such protections, scholars have argued for the creation of a clear statutory tort on invasion of privacy. A statutory regime would provide a comprehensive legal structure for addressing breaches of privacy and would offer individuals a more secure and enforceable means of safeguarding their personal rights (Adnan Trakic, Ridoan Karim & Hanifah Haydar Ali Tajuddin, 2023).

To address the growing misuse of personal data, Malaysia enacted the Personal Data Protection Act 2010 (Act 709) (hereinafter "the Act") as part of the Multimedia Super Corridor (MSC) initiative. Malaysia was the first ASEAN member state to introduce such a law. The Act, read together with the Communications and Multimedia Act 1998, aims to ensure the security, reliability and integrity of information networks. It regulates the collection and processing of personal data in commercial transactions and obliges organizations in thirteen sectors including communications, banking and financial services, insurance, healthcare, tourism, transportation, education, direct selling, real estate, utilities, services, pawnbroking and moneylending to register under its provisions. This legislation was introduced in response to increasing cases of personal data intrusion and requires organizations to notify individuals about the purpose and

scope of data collection and to obtain their consent before processing such data. However, the Act applies only to private-sector activities, as public-sector data management is governed internally within government ministries (Trakic, 2017).

Within this regulatory framework, compliance with data protection obligations is particularly significant in the context of higher education institutions, which manage large volumes of personal information about students and staff. Universities, by virtue of their custodial role, are required to establish comprehensive information security policies (Angraini, Alias & Okfalisa, 2020). Data privacy compliance involves identifying legal and governance requirements for data security, storage and access, and implementing policies and procedures that ensure protection from misuse or unauthorized access. Non-compliance exposes institutions to financial liability, reputational damage and potential regulatory scrutiny (Kyobe, 2010).

The challenge of safeguarding privacy has increased with the advent of digital transformation, which has fundamentally reshaped the scope of informational privacy. The integration of digital technologies into everyday activities has led to the large-scale collection, processing and dissemination of personal data across multiple platforms. As personal information becomes a valuable asset in the digital economy, concerns about misuse, unauthorized access and intrusion into private life have intensified (Solove, 2021; Tene & Polonetsky, 2023). Consequently, informational privacy has emerged as a central theme in discussions on data governance and individual rights in the digital era.

Technological advancements such as big data analytics, artificial intelligence (AI), the Internet of Things (IoT) and cloud computing have been key drivers of this transformation. These innovations enable organizations to gather, analyze and leverage massive datasets to predict consumer behaviour and deliver highly personalized services (Mittelstadt et al., 2016; Zuboff, 2019). However, they also generate new challenges for privacy protection. For example, big data techniques combine data from various sources to reveal patterns and personal insights, AI can make automated decisions that affect individuals, IoT devices constantly collect sensitive data from personal spaces, and cloud-based systems introduce risks related to cross-border storage and cyberattacks (Mhlambi, 2020).

These emerging technologies have significantly increased privacy-related risks, including profiling, pervasive surveillance and identity theft. Profiling can be used to create detailed digital identities that may be exploited for commercial, political or governmental purposes, while advanced surveillance systems blur the boundaries between public and private life (Zarsky, 2017). Moreover, the interconnected nature of these technologies makes personal information more vulnerable to misuse, fraud and cybercrime. These issues underline the need for strong legal, institutional and ethical frameworks to ensure that the benefits of digital transformation do not come at the expense of fundamental privacy rights (Bygrave, 2021).

Legal and Institutional Framework for Data Privacy in Malaysia

The central statute governing personal data protection in Malaysia is the Personal Data Protection Act 2010 (PDPA), which came into force in 2013. Although it marked a significant milestone by introducing a statutory framework for regulating the processing of personal data, its scope is narrowly confined to commercial transactions. Data processing by public sector entities is explicitly excluded, leaving a substantial gap in protection given that large volumes of sensitive personal information are held by government departments and agencies. This

limitation reflects one of the most persistent criticisms of the Act: its inability to provide a comprehensive, cross-sectoral privacy regime.

At the substantive level, the PDPA adopts a principle-based approach aligned with international standards. The Act sets out seven data protection principles, including notice and choice, purpose limitation, disclosure limitation, data security, data retention, data integrity, and access and correction. These principles impose obligations on data users to ensure lawful and transparent processing, while granting data subjects rights to access, correct, and withdraw consent. In practice, however, these rights are relatively weak. There are no explicit provisions for portability or erasure, and the absence of a right to object to automated decision-making means that individuals have limited control over how their data is profiled or used by organizations in an increasingly digital economy.

The Act's enforcement and oversight mechanisms also warrant scrutiny. The Personal Data Protection Commissioner has statutory powers to issue codes of practice, investigate complaints and impose sanctions. Nonetheless, the enforcement regime is largely reactive rather than proactive, relying on complaints rather than systemic supervision. The absence of a dedicated, independent authority with robust investigative powers and resources—akin to the data protection authorities in the EU—limits the deterrent effect of the PDPA. Moreover, penalties are relatively modest when compared with international best practices, reducing the incentive for compliance.

Beyond the PDPA, the wider Malaysian legal framework for privacy remains fragmented and underdeveloped. While provisions in the Communications and Multimedia Act 1998 and cybercrime offences in the Penal Code supplement data protection efforts, these statutes do not specifically address informational privacy. Reliance on common law remedies such as breach of confidence is also limited, as the judiciary has been slow to recognize privacy as a standalone cause of action, focusing historically on issues such as morality and reputation. This patchwork of laws leaves many aspects of data protection unregulated, particularly in light of emerging risks posed by artificial intelligence, big data analytics and cross-border data flows.

Although the PDPA represents a significant legislative advancement in the protection of personal data in Malaysia, its structural limitations remain evident. Chief among these is the exclusion of the public sector from its ambit, the predominantly reactive enforcement model, the relatively narrow scope of data subject rights, and the absence of a comprehensive statutory privacy tort. These deficiencies collectively render the existing Malaysian data protection framework insufficient to address the increasingly complex and sophisticated privacy challenges posed by digital transformation. Moving forward, comprehensive legislative reform that harmonises privacy obligations across both public and private sectors, strengthens the substantive rights of data subjects, and equips regulatory institutions with robust supervisory and enforcement mechanisms is required if Malaysia is to align its privacy regime with contemporary global standards of data governance.

Judicial Approaches to Privacy in Malaysia

In the absence of a comprehensive statutory right to privacy, Malaysian courts have developed privacy protections incrementally through common law causes of action such as breach of confidence and unauthorized disclosure of private information. A significant early example is *Ultra Dimension Sdn Bhd v Kook Wei Yee* [2004] 2 MLJ 624, where the court recognized that

International Journal of Law, Government and Communication
EISSN : 0128-1763
Volume: 11 Issue: 43 (March 2026) PP. 41-51

breach of confidence could provide a remedy for unauthorized disclosure of confidential information. This laid the groundwork for extending limited judicial protection to private data. In *M Mohandas Gandhi v Ambank Berhad [2014] 1 LNS 1025,* the plaintiffs sued credit reporting agency, CITOS, for producing a report that included information relating to the plaintiffs' ongoing court case with a bank for alleged default on their loans. The plaintiffs argued that the information was private and that by publishing a public report, CITOS allegedly invaded their privacy. Lau Bee Lan J cited that the information was not private as it was already available in the public domain.

A more explicit recognition of privacy interests occurred in *Maslinda Ishak v Mohd Tahir Osman & Ors* [2009] 6 MLJ 826, where the court awarded damages to a plaintiff who had been secretly filmed by a police officer, describing the act as an invasion of privacy. Similarly, in *Lee Ewe Poh v Dr Lim Teik Man & Anor* [2011] 1 LNS 1042, damages were awarded against a doctor and hospital for taking and publishing private photographs without consent, demonstrating that unauthorized publication of sensitive personal data can attract judicial intervention.

Despite these developments, privacy claims remain dependent on existing legal doctrines and have not resulted in the recognition of a general tort of privacy. Constitutional arguments have also had limited success. In *Dato' Seri Anwar bin Ibrahim v Public Prosecutor* [2010] 3 CLJ 845, the Federal Court noted that while personal liberty is protected by Article 5 of the Federal Constitution, there is no express guarantee of a right to privacy. More recently, *Pua Kiam Wee v Ketua Pengarah Imigresen Malaysia & Ors* [2018] MLJU 1774 highlighted the gap created by the exclusion of public sector data handling from PDPA oversight. These cases illustrate that the judicial protection of privacy in Malaysia has been piecemeal and reactive, filling gaps left by statutory law but without establishing a coherent doctrine. As a result, individuals remain uncertain about the availability and scope of judicial remedies, especially in addressing privacy violations arising from emerging digital technologies and state surveillance.

More recently, *Genting Malaysia Bhd v PPDP* [2022] 11 MLJ 898 marked a significant judicial endorsement of the primacy of PDPA protections, even against a public authority invoking powers under the Income Tax Act. Though the Court of Appeal later reversed it on procedural grounds, the case reinforces the tension between data subjects' rights and statutory authority. Similarly, *Public Bank Berhad v Tan Teck Seng Jason* [2021] MLJU 92 underscores obligations over biometric data as sensitive personal data. Meanwhile, decisions such as *Kopitiam Asia Pacific v Modern Outlook* [2019] 10 MLJ 243 illustrate the careful balancing act courts undertake between privacy and legal discovery under Section 39 PDPA.

Critical Evaluation of Malaysia's PDPA in the Digital Transformation Era

While the PDPA has been a central pillar of Malaysia's approach to data protection, its ability to safeguard personal data in the face of rapid digital transformation remains questionable. The first area of concern is the scope and coverage of the Act. By limiting its application to commercial transactions and expressly excluding the public sector, the PDPA leaves a significant gap in the protection of personal data managed by government agencies. In a context where ministries and state bodies maintain extensive digital databases, this gap exposes large volumes of sensitive personal information to risks without any statutory safeguards. Compounding this weakness is the absence of robust regulation for cross-border data flows,

with the current mechanism relying on ministerial discretion rather than clear adequacy standards.

A second critical issue lies in the weakness of the enforcement model. Oversight is entrusted to the Personal Data Protection Commissioner, but the powers of this office are narrow, reactive, and under-resourced. Enforcement is largely triggered by complaints rather than proactive monitoring, which means that breaches often come to light only after harm has occurred. Penalties are modest by international comparison, creating limited deterrent effect, particularly for organizations processing data on a large scale. Unlike regulators in other jurisdictions, such as the European Data Protection Board under the GDPR, the Malaysian Commissioner lacks institutional independence and significant sanctioning powers. Furthermore, the PDPA's principles-based approach has not been updated to address modern technological realities. While its provisions were designed to be technology-neutral, they are silent on new risks associated with artificial intelligence, automated profiling, algorithmic decision-making and the Internet of Things (IoT). These technologies permit data processing on an unprecedented scale and complexity, creating risks such as algorithmic bias and invasive behavioural profiling that the 2010 Act was not designed to mitigate.

Another limitation stems from the Act's over-reliance on consent as a primary mechanism for data protection. In an era of widespread data collection, individuals are constantly asked to agree to terms that are lengthy and complex. This phenomenon often described as consent fatigue reduces the effectiveness of consent as a safeguard, as users routinely accept terms without meaningful understanding. Moreover, the Act does not grant modern data subject rights such as data portability, erasure, or the right to object to automated decision-making, leaving individuals with limited recourse once their data has been collected. Taken together, these limitations indicate that the PDPA, while valuable as a first-generation data protection statute, is increasingly inadequate in the context of pervasive digitalization. The Malaysian legal framework now requires comprehensive reform: expanding the scope of the PDPA to include the public sector, strengthening enforcement powers and resources, providing clearer rules on cross-border data transfers, and introducing new rights and safeguards capable of addressing the realities of AI-driven data processing. Without such reforms, Malaysia's data protection regime will remain ill-equipped to meet the challenges of the digital era.

Key Challenges, Future Directions and Proposals for Reform

Despite the statutory framework provided by the PDPA and the incremental protection afforded by the courts, the Malaysian privacy and data protection regime remains inadequate to meet the demands of the digital era. The exclusion of public sector data processing, the fragmented and reactive nature of enforcement, and the limited scope of data subject rights continue to create systemic weaknesses. In addition, emerging technologies such as big data analytics, artificial intelligence and the Internet of Things have exposed gaps that a principles-based, first-generation statute is unable to address. Moving forward, comprehensive reform is necessary. This reform should expand the scope of the PDPA to include the public sector, introduce robust rules for cross-border data transfers, strengthen the independence and powers of the Personal Data Protection Commissioner, and modernise rights to include erasure, portability and safeguards against automated processing. The recognition of a clear statutory right to privacy, supported by an updated legal framework, would enable Malaysia to align with international standards and respond effectively to the sophisticated privacy challenges of digital transformation.

In light of these challenges, several specific proposals for reform can be advanced. Foremost is the need to extend the PDPA to cover public sector data processing, ensuring a consistent standard of transparency, accountability and security across both public and private institutions. Equally important is the creation of a clear legal framework for cross-border data flows, replacing reliance on ministerial discretion with statutory adequacy criteria or binding safeguards.

Institutional reforms are also vital. The Personal Data Protection Commissioner must be strengthened through greater independence, adequate resources, and expanded supervisory powers. These should include the authority to conduct proactive audits, issue binding guidance and impose effective administrative fines. Such reforms would make the regulatory framework more agile and responsive, capable of keeping pace with rapid technological change.

In addition to these core reforms, Malaysia must adopt forward-looking principles that address the challenges of digital transformation. Specifically, the incorporation of data ethics as a guiding framework would ensure that technological innovation respects the rights and expectations of individuals. Algorithmic transparency requirements would oblige organizations using AI and automated decision-making to disclose the logic and consequences of such processing, mitigating risks of discrimination and opaque profiling. Furthermore, mandating data protection impact assessments for high-risk processing already standard practice in jurisdictions like the EU and Singapore would encourage proactive risk assessment rather than reactive enforcement (Wright & Raab, 2022).

Finally, data protection cannot be viewed in isolation from broader digital governance. Integration of privacy law with cybersecurity frameworks, AI ethics guidelines, digital economy strategies, and fintech regulation is essential to create a cohesive and resilient policy ecosystem. A coordinated approach would not only strengthen trust in Malaysia's digital economy but also facilitate responsible participation in cross-border data flows and international trade. These proposals seek to transition Malaysia's data protection regime from a narrow, reactive model to a comprehensive, future-proof framework. By expanding statutory coverage, strengthening institutional capacities, and embedding modern principles such as data ethics, transparency and impact assessment, Malaysia will be better positioned to meet the privacy challenges of an era defined by big data, artificial intelligence and globalised digital services.

Conclusion

The development of privacy and data protection law in Malaysia shows that while the Personal Data Protection Act 2010 marked a significant step forward, the existing framework remains uneven and insufficient. Its narrow application to commercial transactions, the exclusion of the public sector, weak enforcement mechanisms and limited recognition of individual rights leave substantial gaps in protection. Judicial interventions, though important, have not established a comprehensive privacy right, and the overall framework continues to rely on outdated common law principles that are ill-suited to the scale and complexity of modern data processing.

The acceleration of digital transformation driven by big data, artificial intelligence, the Internet of Things and cross-border data flows has made these weaknesses increasingly urgent. As demonstrated throughout this analysis, Malaysia must modernize its privacy and data protection laws by expanding the scope of the PDPA, strengthening institutional capacities, and

embedding forward-looking principles such as data ethics, algorithmic transparency and impact assessment. Only through such comprehensive reform can the legal framework evolve into a coherent and future-proof regime that protects individuals, fosters trust, and positions Malaysia to meet the demands and risks of the digital age.

Acknowledgements:	We want to express our sincere gratitude to Universiti Islam Antarabangsa Tuanku Syed Sirajuddin (UniSIRAJ) and the Research Management & Innovation Centre (RMIC) for the research grant.
Funding Statement:	This research received financial support from Universiti Islam Antarabangsa Tuanku Syed Sirajuddin (UniSIRAJ) under short term Grant [STG-090/2023].
Conflict of Interest Statement:	We would like to declare that there is no conflict of interest regarding the publication of this paper. All authors have contributed to this work and approved the final version of the manuscript for submission to the International Journal of Law, Government and Communication (IJLGC).
Ethics Statement:	This study did not involve human, or animal subjects or sensitive data requiring ethical approval and was conducted in compliance with recognised academic integrity and ethical publishing standards.
Author Contribution Statement:	All authors contributed significantly to the development of this manuscript. [Author 1] was responsible for the conceptualization, methodology, and overall supervision of the study. [Author 2] handled data collection, analysis, and interpretation of results. [Author 3 and 4] contributed to the literature review, drafting, and critical revision of the manuscript. All authors read and approved the final version of the manuscript prior to submission.

References

Abu Bakar, A. (2023). Comparative analysis of Malaysia's data protection framework with global standards. Journal of Law and Digital Governance, 5(2), 115–133.

Adnan Trakic, R., Karim, R., & Tajuddin, H. H. A. (2023). Data protection in Malaysia: Challenges in the digital era. Asian Journal of Law and Society, 10(1), 55–74.

Angraini, Alias, R. A., & Okfalisa. (2020). Information security compliance in Malaysian higher education institutions. Journal of Theoretical and Applied Information Technology, 98(14), 2871–2882.

Bygrave, L. A. (2021). Data protection law: Approaching its rationale, logic and limits (2nd ed.). Oxford University Press.

Dato' Seri Anwar bin Ibrahim v Public Prosecutor, [2010] 3 CLJ 845 (Federal Court, Malaysia).

Genting Malaysia Bhd v Pesuruhjaya Perlindungan Data Peribadi & Ors, [2022] 11 MLJ 898 (High Court, Malaysia).

Hamid, N., Mahmud, M., & Rahman, S. (2022). Privacy and surveillance in Malaysia's post-pandemic digital landscape. Malaysian Journal of Policy Studies, 9(1), 21–40.

Kyobe, M. (2010). A knowledge management approach to e-Government: Challenges and lessons from Malaysia. Government Information Quarterly, 27(2), 164–173.

Kopitiam Asia Pacific Sdn Bhd v Modern Outlook Sdn Bhd & Ors, [2019] 10 MLJ 243 (High Court, Malaysia).

Leng, O. T. S., Vergara, R. G., & Khan, S. (2021). Personal data protection and privacy law in Malaysia. Sweet & Maxwell.

Lim, J. (2022). Digital economy and privacy law: A Malaysian perspective. Asian Business Law Journal, 8(3), 65–78

Lee Ewe Poh v Dr Lim Teik Man & Anor, [2011] 1 LNS 1042 (High Court, Malaysia).

Malaysia. (2010). Personal Data Protection Act 2010 (Act 709). Malaysia: The Commissioner of Law Revision.

Malaysia. (1997). Multimedia Super Corridor (MSC) Bill of Guarantees. Government of Malaysia.

Malaysia. (1936, revised 1997). Penal Code (Act 574).

Malaysia. (1957, as amended). Federal Constitution. Malaysia: The Commissioner of Law Revision.

Malaysia. (1998). Communications and Multimedia Act 1998 (Act 588). Malaysia: The Commissioner of Law Revision.

Maslinda Ishak v Mohd Tahir Osman & Ors, [2009] 6 MLJ 826 (High Court, Malaysia).

M Mohandas Gandhi v Ambank Berhad [2014] 1 LNS 1025 (High Court, Malaysia).

Mhlambi, S. (2020). From rationality to relationality: Ubuntu as an ethical framework for AI governance. Carr Center Discussion Paper Series, Harvard Kennedy School.

Mittelstadt, B. D., Allo, P., Taddeo, M., Wachter, S., & Floridi, L. (2016). The ethics of algorithms: Mapping the debate. Big Data & Society, 3(2), 1–21.

Mustaffa, N. (2021). Corporate governance and self-regulation in Malaysia's data privacy landscape. Journal of Corporate Law Studies, 21(3), 457–475.

Norazah, M. S. (2021). Digital transformation and privacy in Malaysia: Lessons from the COVID-19 pandemic. International Journal of Law and Information Technology, 29(4), 357–375

Public Bank Berhad v Tan Teck Seng Jason & Anor, [2021] MLJU 92 (High Court, Malaysia).

Pua Kiam Wee v Ketua Pengarah Imigresen Malaysia & Ors, [2018] MLJU 1774 (High Court, Malaysia).

Rahman, F. (2021). Emerging challenges in personal data protection law in Malaysia. Asian Journal of Comparative Law, 16(2), 243–264.
Solove, D. J. (2021). Understanding privacy (Updated ed.). Harvard University Press.
Tan, P., & Lee, M. (2022). The adequacy of Malaysian data protection law in the context of cross-border data flows. International Data Privacy Law, 12(3), 189–204.
Tene, O., & Polonetsky, J. (2023). Privacy in the age of big data: The new frontiers. Stanford Law Review, 75(1), 55–112.
Trakic, A. (2017). Personal data protection in Malaysia: Balancing innovation and privacy. Malayan Law Journal, 6, lxxix–xci.
Ultra Dimension Sdn Bhd v Kook Wei Yee, [2004] 2 MLJ 624 (Court of Appeal, Malaysia).
Wright, D., & Raab, C. (2022). Privacy impact assessment. Springer.
Zarsky, T. Z. (2017). Incompatible: The GDPR in the age of big data. Seton Hall Law Review, 47, 995–1020
Zuboff, S. (2019). The age of surveillance capitalism. Public Affairs.