Journal of Posthumanism
2025
Volume: 5, No: 6, pp. 1817–1826
ISSN: 2634-3576 (Print) | ISSN 2634-3584 (Online)
posthumanism.co.uk

DOI: https://doi.org/10.63332/joph.v5i6.2284

Platform Accountability and User Protection: A Comparative Analysis of Regulatory Approaches in Malaysia, United Kingdom and India

Suzarika Sahak[1], Ramalinggam Rajamanickam[2], Muhamad Sayuti Hassan@Yahya[3], Mafuzah Mohamad[4]

Abstract

In recent years, Malaysia's digital landscape has faced considerable challenges, particularly in promoting platform accountability and protecting users. These priorities, integral to fostering a well-regulated and secure digital environment, are shaped by the evolution of legal frameworks and regulatory policies. This article examines the Online Safety Act 2024, a newly passed law in Malaysia, by comparing its provisions with the United Kingdom and India regulatory approaches. The objective of this article is to examine Malaysia's Online Safety Act 2024 and its implications for platform accountability and user protection by comparing its provisions with the United Kingdom's Online Safety Act 2023 (OSA) and India's Information Technology Act 2000 (ITA), alongside the Intermediary Guidelines and Digital Media Ethics Code Rules 2021 (Intermediary Rules 2021). This article explores how these regulatory frameworks address key issues such as online harms, intermediary accountability, and user safety, highlighting significant gaps in the Malaysian Act. The analysis identifies potential shortcomings, such as the absence of explicit safe harbour protections, proactive risk mitigation strategies, and strong transparency obligations, which may impact the Act's ability to balance online safety with fundamental freedoms like freedom of expression and digital innovation, particularly as its implementation unfolds. Adopting a qualitative approach, this article evaluates these regulations and draws comparative insights from international frameworks. The findings underscore the need for a more adaptive regulatory framework to address the evolving challenges of the digital era while safeguarding both user protection and fundamental rights.

Keywords: *Malaysia Online Safety Act 2024, Online Safety, Platform Accountability, User Protections, Content Regulation.*

Introduction

The Malaysia Online Safety Act 2024 is a new legislative framework aimed at enhancing online safety by regulating harmful digital content and increasing the accountability of digital platforms. This Act addresses issues such as cyberbullying, online scams, and the protection of children, focusing particularly on platforms that host user-generated content such as social media. Its goal is to establish a legal framework for combating the growing threats posed by online harm while safeguarding freedom of expression and creating a conducive digital innovation (Bernama, 2024). The basis of the Act is a regulatory model that underlines the responsibilities of intermediaries to take action against harmful or illegal content. Platforms are required to implement safety measures, including content moderation systems, and to submit an Online Safety Plan detailing their strategies for identifying, managing, and removing harmful

[1] Legal Officer, Attorney General's Chambers of Malaysia, Email: erikasahak@gmail.com
[2] Associate Professor (PhD), Faculty of Law, Universiti Kebangsaan Malaysia (UKM), Email: rama@ukm.edu.my
[3] Faculty of Law, Universiti Kebangsaan Malaysia (UKM), Email: sayutihassan@ukm.edu.my
[4] Department of Business and Management, UNITEN Business School, Universiti Tenaga Nasional (UNITEN), Email: mafuzah@uniten.edu.my

content. The Malaysian Communications and Multimedia Commission (MCMC), an independent regulatory body established under the Malaysian Communications and Multimedia Commission Act 1998, is tasked with enforcing these regulations, ensuring compliance, and imposing penalties for non-compliance. However, the Act has sparked considerable criticism during the parliamentary debate about its potential implications for media freedom and the delicate balance between regulatory and platform, with over-regulation potentially stifling free expression and imposing disproportionate burdens on smaller platforms.

Despite its significance, literature on the Online Safety Act 2024 remains limited, reflecting its status as a newly enacted law. Currently, there are limited scholarly analyses addressing its principles, implications, and alignment with international standards. This lack of comprehensive discussion presents a gap in understanding the Act's potential impact on Malaysia's digital governance. This article begins by examining the existing legislative framework provided by the Online Safety Act 2024 in Malaysia. The discussion then shifts to a comparative analysis of the Online Safety Act 2023 of the United Kingdom and India's Information Technology Act 2000, along with the Intermediary Rules 2021, focusing on the liability of internet intermediaries for content regulation. These jurisdictions are chosen for comparison due to their comprehensive provisions and established standards for determining intermediary responsibilities, particularly in addressing harmful online content and ensuring accountability. For instance, the UK's framework emphasises risk-based obligations and proactive content moderation measures for platforms. The law outlines extensive duties of care for intermediaries, including mandatory transparency and reporting requirements, to mitigate online harms. Meanwhile, India's ITA, complemented by the Intermediary Rules 2021, introduces a tiered system of intermediary obligations, emphasising due diligence, grievance redressal mechanisms, and content takedown processes. The selection of these frameworks for comparison is based on their relevance to intermediary liability and their potential applicability in addressing similar regulatory challenges in Malaysia. The comparison will focus on critical areas, including safe harbour provisions, proactive risk mitigation, grievance redressal mechanisms, and transparency obligations, to assess how Malaysia's approach aligns with or diverges from global best practices observed in the UK and India. This article concludes by drawing insights from the UK and Indian legal frameworks to propose recommendations for enhancing Malaysia's approach to intermediary liability. These recommendations aim to strike a balance between safeguarding user rights, ensuring platform accountability, and fostering innovation in the digital space.

Methodology

The study employs a qualitative methodology of a critical analysis of legislative texts, policy and parliamentary documents. This approach involves systematically comparing legal systems, laws, or frameworks to identify similarities, differences, and best practices. Additionally, a comparative approach is used to analyse and contrast Malaysia's framework with those of the UK and India. By drawing insights from the UK's emphasis on self-regulation and risk-based assessments, as well as India's tiered intermediary obligations and structured grievance mechanisms, this article highlights the strengths and gaps in Malaysia's framework. Additionally, the analysis delves into areas such as the independence of the MCMC, the adequacy of user empowerment tools, and the robustness of grievance mechanisms under the Act. By critically examining these similarities and differences, this article contributes to the broader discourse on digital governance. It offers recommendations for enhancing Malaysia's regulatory framework, ensuring it strikes a balance between protecting users from online harms, safeguarding media freedom and embracing digital developments.

Background of Malaysia's Online Safety Act 2024

The Malaysia Online Safety Bill 2024 was tabled by the Minister in the Prime Minister's Department (Law and Institutional Reform) and passed by the Dewan Rakyat (House of Representatives) and the Dewan Negara (Senate) on 11 and 16 December 2024, respectively. It aims to strengthen the regulation of online content by imposing stricter responsibilities on digital service providers while protecting user interests in an increasingly challenging digital ecosystem. According to the Parliamentary Hansard, the drafting of this Bill complements the Communications and Multimedia Act 1998, introducing a more comprehensive regulatory approach (Parliament of Malaysia, 2024). Its primary focus is ensuring online user safety through the regulation of harmful content while introducing proactive obligations for service providers. The Act applies to several categories of digital service providers. This includes Application Service Providers (ASP), such as social media platforms and messaging applications, Content Application Service Providers (CASP), which cover video-sharing, streaming services, and digital news portals, and Network Service Providers (NSP), including telecommunications companies and internet providers under the Communications and Multimedia Act 1998 (CMA). However, private messaging features of the application or content services are excluded from its scope. The Act also extends its jurisdiction extraterritorially, with regulatory oversight vested in the Minister of Communications and enforcement by the MCMC. The UK's Online Safety Act 2023, on the other hand, focuses primarily on user-to-user services and search engines. It applies to social media platforms like video-sharing services and search engines. The Act also covers online gaming platforms that allow user interaction, and mandates age verification mechanisms for adult content websites (Department for Digital, Culture, Media and Sport, and the Home Office, 2020). Meanwhile, India's Information Technology Act 2000 (ITA) and the Intermediary Rules 2021 regulate a broader spectrum of digital platforms. This includes social media intermediaries as well as Over-the-Top (OTT) streaming platforms. India's framework also extends to digital news portals, which must comply with the Digital Media Ethics Code, and e-commerce, which are subject to specific intermediary obligations (Suryawanshi & Laturkar, 2019).

Section 13 of the Act requires providers to implement measures to reduce user exposure to harmful content, ensuring proportionality in enforcement. The Act regulates two primary categories of content; "harmful content" and "priority harmful content." Harmful content includes materials such as child sexual abuse material, financial fraud, obscene or indecent content, content inciting violence or terrorism, and content promoting ill-will or public hostility. Priority harmful content, a subset of harmful content, specifically includes child sexual abuse material and financial fraud, both subject to more stringent controls. Section 14 requires clear user guidelines, while Section 15 compels service providers to equip users with tools for managing online safety, including features to restrict interactions and visibility. Further, Sections 16 to 18 establish mechanisms for reporting harmful content and protecting vulnerable groups, including children, while Section 20 mandates the development of Online Safety Plans detailing compliance efforts. The Act outlines procedures under Sections 21 to 23 for reporting harmful content and imposes obligations for swift assessments and remedial actions. Enforcement mechanisms under Sections 15 and 39 empower the Malaysian MCMC to impose penalties of up to RM1 million for non-compliance, reflecting a corporate compliance-oriented approach.

During the parliamentary debates, the Bill garnered a number of objections. Concerns have been made regarding the legislation's potential to turn Malaysia into a digital dictatorship by excessive control over internet material, drawing comparisons with models in North Korea and China.

There were suggestions that the Bill be forwarded to a Parliamentary Select Committee for a full assessment, with civil society organisations and industry experts included to guarantee more balanced participation. Debates also highlighted criticisms regarding the vague definition of harmful content, which was seen as creating a risk of unfairly curtailing freedom of speech. The MCMC's broad enforcement powers emerged as a crucial problem, with requests for the establishment of an independent body to offer checks and balances and guarantee fair and transparent enforcement. Furthermore, the high penalties imposed on service providers were questioned as possibly harming small and medium-sized businesses.

Article 19 and the Centre for Independent Journalism (CIJ), an international non-governmental organisation, have also expressed serious concerns about the Online Safety Bill 2024, stressing its potential to undermine freedom of speech in Malaysia (Naidu, 2024). While acknowledging the need for platform responsibility in addressing negative consequences on human rights, they emphasise the Bill's inability to strike an acceptable balance between regulatory supervision and safeguards for free expression. Despite some beneficial provisions, such as the prohibition on private messaging under Section 2(2) and the limitation of unjustified restrictions on expression under Section 13(3), concerns remain concerning the Minister's and the MCMC's broad powers. They argue that these capabilities, combined with insufficient mechanisms for openness and accountability, have the potential to undermine human rights protections and democratic ideals online (Article 19, 2024). The Online Safety Bill has also been heavily criticised by the Online Safety Advocacy Group (OSAG) and numerous civil society organizations for its possible influence on freedom of speech. Despite appeals from the opposition coalition to submit the Bill to the Parliament Special Select Committee (PSSC) for additional consideration, it was passed on a division vote, with 77 voting in and 55 against. While OSAG and civil society organisations recognise the necessity of holding internet service providers and social media platforms responsible, they claim that the Bill does not offer adequate transparency and accountability procedures. Instead, its provisions give the MCMC broad authority, prompting worries about overreach and repression of free expression (Amnesty International, 2024).

Comparative Framework: Key Aspects of Malaysia's Online Safety Act 2024, United Kingdom's Online Safety Act 2023 and India's Information Technology Act 2000

a. Immunity and Protection to Internet Intermediary

Safe harbour provisions are a cornerstone of intermediary liability frameworks, offering conditional immunity to platforms for user-generated content, provided they comply with legal obligations. These provisions were pioneered in the United States under the Digital Millennium Copyright Act 1998 (DMCA) and have influenced global legislation, including the UK and India (Yeh & Jeweler, 2004). The UK's Online Safety Act emphasises a duty of care, requiring platforms to mitigate risks and remove harmful content (Price, 2021). Similarly, India's ITA 2000 and the Intermediary Rules 2021 extend safe harbour protections to intermediaries demonstrating due diligence, such as timely removal of unlawful content upon notification (Gupta & Srinivasan, 2023). In contrast, Malaysia's Online Safety Act 2024, as outlined in Sections 13 to 23, imposes significant obligations on service providers, including measures to mitigate harmful content, provide user safety tools, and establish reporting mechanisms. However, it does not explicitly include safe harbour protections. Section 13 focuses on reducing risks of harmful content, Section 14 mandates user guidelines, and Sections 21-23 detail reporting mechanisms for harmful content. Despite these proactive measures, the absence of safe harbour provisions could expose platforms, particularly smaller ones, to heightened liability

risks. This approach places disproportionate burdens on intermediaries, potentially hindering innovation and deterring smaller platforms from operating in Malaysia. The frameworks in the UK and India strike a balance between platform responsibilities and protections, fostering a more conducive environment for innovation and accountability. Introducing explicit safe harbour provisions within the Malaysian framework could address these gaps, ensuring a balanced approach to intermediary liability while promoting digital growth.

b. Risk Assessments, Mitigation, and Transparency

Proactive measures and transparency are central to Malaysia's Online Safety Act 2024, which emphasises platform accountability and preventive strategies to ensure a safer digital environment. The Act requires platforms to address harmful online content by implementing an Online Safety Plan, detailing strategies for identifying, managing, and mitigating harmful content. This approach ensures that preventive measures are in place before harmful content reaches users. The MCMC oversees the enforcement of these measures, imposing penalties for non-compliance to ensure adherence. This proactive stance aligns with global best practices. For instance, the UK's Online Safety Act 2023 mandates platforms to conduct comprehensive risk assessments and implement preventive measures to minimise the spread of harmful content, with Ofcom serving as the independent regulatory authority. Similarly, India's Intermediary Rules 2021 require significant social media intermediaries to deploy automated tools to identify and remove illegal content, such as child sexual abuse material, enabling swift action against online harms. Malaysia's framework, while distinct, shares the proactive ethos of these models by requiring platforms to actively assess and address potential risks through their Online Safety Plans. This reduces reliance on reactive measures, such as post-reporting content takedowns. However, the Malaysian framework could benefit from integrating additional elements, such as mandatory risk assessments and advanced automated content moderation tools seen in the UK and India. These measures would strengthen the framework's capability to prevent online harms effectively while maintaining a balance that fosters innovation and minimises undue burdens on platforms.

Transparency is another critical element for building trust in digital governance. The UK's Online Safety Act mandates platforms to publish detailed transparency reports, disclosing risk assessments, content moderation activities, and compliance efforts. These reports are audited and made publicly available, ensuring accountability and fostering public trust. Similarly, India's regulations require platforms to submit monthly compliance reports, outlining grievances addressed and actions taken, thereby promoting a culture of transparency. In contrast, Malaysia's Act focuses on submitting Online Safety Plans to the MCMC but does not mandate the publication of transparency reports. This lack of public accountability may undermine the effectiveness of the regulatory framework and erode stakeholder trust. Introducing mandatory transparency obligations, akin to those in the UK and India, would ensure that platforms are held accountable for their practices, fostering greater trust among users, stakeholders, and the broader public.

c. User Empowerment and Grievance Mechanisms

Ensuring user empowerment and effective grievance redressal is crucial for holding online platforms accountable and fostering a safer digital environment. The UK's Online Safety Act 2023 sets a strong precedent by mandating filtering tools that allow users, especially adults, to control their exposure to harmful yet legal content. Platforms must provide customisable safety settings, giving users greater control over their online experiences. Additionally, the Act requires

platforms to establish clear and accessible complaint mechanisms under Section 21, enabling users to report harmful content and appeal moderation decisions. Ofcom, the independent regulator, plays a central role in ensuring compliance, enforcing transparency requirements, and imposing penalties for non-compliance when necessary. Child safety is also a priority, with platforms required to implement age-appropriate content controls and conduct risk assessments to prevent harm. Regular transparency reports must be submitted, ensuring accountability and public oversight. The UK's approach effectively balances platform responsibility with user rights, fostering a trustworthy regulatory framework for online safety.

Similarly, India's regulatory framework emphasises timely grievance redressal to build public trust in digital governance. Platforms are required to appoint Grievance Officers, who must acknowledge complaints within 24 hours and resolve them within 15 days. The Ministry of Information and Broadcasting (MIB) oversees a three-tier grievance redressal system, ensuring that complaints unresolved at the platform level can be escalated to independent bodies and, if necessary, to the ministry itself. Platforms must follow standards to ensure that unlawful content, such as hate speech, threats, or defamation, is handled appropriately while maintaining a balance between user safety and freedom of expression. By implementing transparent and standardised procedures, India promotes a responsible digital environment where user concerns are addressed efficiently.

Contrary, Malaysia's Online Safety Act 2024 lacks clear provisions for user empowerment tools and grievance redressal mechanisms, limiting users' ability to manage their online experiences and seek recourse for harmful content. While the Act requires licensed application service providers (ASPs) and content application service providers (CASPs) to implement measures that reduce users' exposure to harmful content, these obligations remain vague. Section 13(1) requires service providers to apply the safety measures indicated in the code of conduct, while Section 16 requires them to provide tools to help customers manage their online safety. However, the Act does not specifically require content filtering technologies, which are critical for allowing users to personalise their online interactions and protect themselves from harmful content. Furthermore, the Act establishes an Online Safety Appeals Tribunal to review MCMC's decisions, but it lacks a well-defined grievance redressal mechanism for users to report harmful content or challenge platform decisions effectively. Without a structured complaints and appeals process, users have limited options to seek redress, making it difficult to hold platforms accountable. This gap highlights the need for stronger user protection measures to ensure a transparent and fair regulatory framework.

d. Malaysian Communications and Multimedia Commission's Lack of Independence and Overreach of the Communication Online Safety Appeal Tribunal

The Online Safety Act 2024 also raises critical concerns regarding freedom of expression and effective governance due to its reliance on MCMC, which lacks independence and operates under broad discretionary powers (Amnesty International, 2024). Critics argue the Act could be misused for censorship, as it allows MCMC to block content, even outside predefined harmful categories, and overrule service providers. The lack of safeguards for freedom of expression and its potential to suppress dissent are main concerns (MalaysiaNow, 2024). Key provisions, such as Sections 30(1), 54-57, and 60-61, grant MCMC authority to monitor, investigate, and regulate online platforms without adequate judicial oversight, including access to user data and search and seizure powers. The Minister's expanded authority under Sections 35, 74, 80, and 81 further centralises control, undermining accountability mechanisms and judicial checks. While the

Online Safety Committee includes diverse stakeholders, its advisory role lacks substantive regulatory influence, with primary powers remaining with MCMC. The Online Safety Act 2024 in Malaysia diverges significantly from the approaches of the United Kingdom and India in terms of governance and oversight of online platforms.

The UK's Online Safety Act 2023 delegates regulatory powers to Ofcom, an independent body with clear safeguards to ensure accountability and the protection of freedom of expression. Ofcom's mandate includes implementing a duty of care, requiring platforms to mitigate risks of harmful content while safeguarding users' rights, supported by transparent mechanisms and public oversight. In India, the regulation of internet intermediaries is governed by the ITA and the Intermediary Rules 2021, overseen by the Ministry of Electronics and Information Technology (MeitY) and the Ministry of Information and Broadcasting (MIB). The division of responsibilities between MeitY and MIB under the Intermediary Rules 2021 is not explicitly stated in the Rules but is reflected in official practice and policy implementation. MeitY oversees Part II, which deals with intermediary obligations and grievance redressal, while MIB manages Part III, covering the code of ethics and digital media regulations. According to Press Information Bureau, Government of India's Press release, this division aligns with their traditional roles, where MeitY handles technology and intermediaries, and MIB focuses on media content regulation. The ITA provides safe harbour protections to intermediaries that follow due diligence, such as promptly removing unlawful content when notified. It includes judicial review to balance intermediary responsibilities with fundamental rights. A tiered grievance system and content guidelines further ensure accountability, especially for OTT platforms and digital news portals.

The Online Safety Act 2024 introduces the Online Safety Appeal Tribunal under Section 40 to provide due process and ensure the right to be heard. The Online Safety Appeal Tribunal's decisions are determined by a majority vote of its members and are considered final and binding, with no further appeals permitted. Additionally, its decisions can be enforced in the same manner as judgments or orders issued by the High Court. However, concerns arise from Section 48(2), which grants the Tribunal the authority to determine and punish contempt, a power traditionally reserved for courts. This provision risks undermining the separation of powers by allowing a quasi-judicial body to exercise judicial functions. Such overreach could disrupt the balance of authority between the judiciary and other branches of governance. In comparison, neither the UK's Online Safety Act 2023 nor India's ITA 2000 grants contempt powers to regulatory bodies or tribunals overseeing online safety. In the UK, issues such as contempt remain under the jurisdiction of the courts, with Ofcom, the independent regulator, focusing solely on administrative enforcement. Similarly, India's framework assigns regulatory responsibilities to government bodies without empowering them to adjudicate contempt, thereby maintaining judicial oversight.

e. Approaches in Regulating Harmful Content

Malaysia's Online Safety Act 2024, the United Kingdom's OSA**,** and India's Section 79 of the Information Technology Act 2000 (ITA) present distinct approaches to regulating harmful content and holding intermediaries accountable. A key difference lies in how harmful content is defined and addressed within these frameworks. In Malaysia, the Online Safety Act 2024 introduces a broad and vague definition of harmful content under Section 4**,** encompassing both illegal content and "legal but harmful" material, such as obscene or indecent content and content promoting ill-will or hostility. While certain categories, such as child sexual abuse material, are

well-defined, others remain ambiguous, raising concerns about enforcement and the risk of over-censorship. This ambiguity increases the likelihood of lawful content being disproportionately removed, potentially suppressing legitimate speech and dissent (Amnesty International, 2024). By contrast, the UK Online Safety Act employs a more structured approach by clearly distinguishing between illegal and "priority harmful" content, with detailed guidelines for platforms to address such material in a proportional and transparent manner. India's framework under Section 79 of ITA**,** supplemented by the Intermediary Rules 2021, defines harmful content more narrowly, focusing on specific obligations like removing unlawful material upon notification, which reduces ambiguity and ensures greater clarity (Marsoof & Gupta, 2019).

The requirements imposed on service providers further distinguish these systems. In Malaysia, the Online Safety Act places additional obligations on Application Service Providers, Content Application Service Providers, and Network Service Providers. Providers must proactively monitor and filter harmful content, submit Online Safety Plans, and meet the reporting obligations outlined in Sections 13 to 23. In contrast, the UK Online Safety Act stresses a risk-based approach, requiring platforms to undertake risk assessments and apply preventative measures while adhering to a duty of care. Platforms that meet these criteria are protected from responsibility. In India, Section 79 provides safe harbour protections to intermediaries that act diligently, including the prompt removal of unlawful content upon complaint. This due diligence approach balanced intermediary obligations with legal protection, creating a less burdensome regulatory environment compared to Malaysia's liability-centric approach (Kamil & Azmi, 2020).

f. Safeguarding Freedom of Speech

The shift from intermediary liability to responsibility reflects changing regulations on platform accountability. Traditionally, intermediaries were protected from liability unless they actively engaged with content. Now, they face increasing obligations to monitor, detect, and remove unlawful material, raising concerns about due process, over-censorship, and privatised regulation. As platforms take on a greater role in policing content, there is a need for balanced policies that uphold both free expression and accountability (Frosio, 2017). Safeguards for freedom of speech also vary significantly between the three frameworks. The UK Online Safety Act has strong protections, such as requiring transparency reporting and guaranteeing that enforcement is handled by an independent regulator, Ofcom, which works outside of direct government authority. India's Section 79 provides for procedural safeguards such as judicial review to prohibit arbitrary censorship. Although intermediaries are required to respond to notifications, their activities are subject to judicial scrutiny, ensuring that freedom of speech is not jeopardised. In Malaysia, the Online Safety Act's ambiguous definitions of harmful information and content raise concerns about over-removal of lawful expression, creating the risk of government interference in content moderation to suppress dissenting or critical views. While content monitoring can assist in identifying problematic materials, excessive takedown measures may encroach on user privacy and freedom of expression. Without safe harbour laws and with a large dependence on content moderation tools, there is a greater danger of excessive limitations on valid content, thereby harming the privacy and freedom of speech provided by Article 10(1)(a) of the Federal Constitution. Furthermore, the lack of precise definitions for harmful content fails to meet the principle of legality under Article 19(3) of the International Covenant on Civil and Political Rights (ICCPR), which mandates that restrictions on speech must be clear, legitimate, and necessary within a democratic society (Article 19, 2024).

The Online Safety Act 2024 raises concerns over freedom of speech due to its broad discretionary powers granted to MCMC, potential political intervention, lack of judicial oversight, and potential for censorship. Unlike the UK and India, where independent regulators like Ofcom and judicial review mechanisms help balance online safety with fundamental rights, Malaysia's framework centralises authority within MCMC and the Minister, increasing the risk of political interference in content regulation. The Tribunal's power to punish contempt, a function typically reserved for courts, further undermines the separation of powers and expands regulatory overreach. Without proper safeguards, independent and clear legal protections, the Act risks restricting legitimate speech and digital rights. This underscores the urgent need for stronger legal clarity and accountability to ensure online regulations do not compromise fundamental freedoms.

Conclusion

The Online Safety Act 2024 is a significant step in shaping Malaysia's digital landscape, introducing regulations aimed at strengthening platform accountability and user protection. However, as a newly enacted law, there is still limited scholarly analysis on its practical impact, enforcement challenges, and effectiveness. Future studies and legal discourse will be critical in determining how effectively this Act conforms with worldwide best practices and if it accomplishes its intended goals while protecting basic freedoms. This article has successfully addressed the regulatory gap in the Online Safety Act 2024 by critically examining its enforcement methods, supervisory structure, and impact on free expression.. Through a comparative analysis of the United Kingdom and India, it emphasises both strengths and weaknesses, providing insights into best practices and areas for legislative refinement.

The legislative process leading to the Act's enactment has also sparked extensive debate, reflecting both support and concerns over broad regulatory powers, content moderation policies, and the extent of government oversight. While the Act seeks to prevent online harm, the absence of defined safe harbour protections, independent oversight, and clear definitions of harmful content raises questions about the balance of regulation and free expression. Despite these concerns, the passing of this Act is a welcome start toward tackling the issues of digital governance. To be effective and comprehensive, the law must be adaptive, transparent, and sensitive to technological advances. To ensure the security and respect for human rights in Malaysia's digital environment, judicial supervision must be strengthened, legislative definitions revised, and an independent regulatory framework established.

References

Amnesty International. (2024). Passage of the Online Safety Bill a grave blow to freedom of expression. Amnesty International. https://www.amnesty.my/2024/12/12/online-safety-bill/

Article 19. (2024). Malaysia: Concerns with the Online Safety Bill 202. Article 19. https://www.article19.org/resources/malaysia-online-safety-bill/?utm_source

Bernama. (2024). Online Safety Act enhances online safety of Malaysian community - Fahmi. The Sun. https://thesun.my/malaysia-news/online-safety-act-enhances-online-safety-of-malaysian-community-fahmi-AH13414037#:~:text=KUALA NERUS%3A The Online Safety,of speech%2C including among students.

Department for Digital, Culture, Media and Sport, and the Home Office. (2020). Online Harms White Paper: Full Government Response to the Consultation.

Frosio, G. F. (2017). Reforming intermediary liability in the platform economy: a European digital single market strategy. Nw. UL Rev. Online, 112, 18.

Giancarlo F. (2017). "Why keep a dog and bark yourself? From intermediary liability to responsibility." Int. J. Law Inf. Technol., 26, 1-33. https://doi.org/10.1093/ijlit/eax021.

Gupta, I., & Srinivasan, L. (2023). Evolving scope of intermediary liability in India. International Review of Law, Computers and Technology, 37(3), 294–324. https://doi.org/10.1080/13600869.2022.2164838

India Information Technology Act 2001

India Intermediary Guidelines and Digital Media Ethics Code Rules 2021

Kamil, I.S., & Azmi, I.M. (2020). Gatekeepers Liability for Internet Intermediaries in Malaysia: Way Forward. International Journal of Business, Economics and Law, 21 (4).

Malaysia Online Safety Act 2024

MalaysiaNow. (2024). Proposed "online safety" law another censorship tool for Putrajaya, critics warn. MalaysiaNow. https://www.malaysianow.com/news/2024/10/21/proposed-online-safety-law-another-censorship-tool-for-putrajaya-critics-warn

Marsoof, A., & Gupta, I. (2019). Shielding internet intermediaries from copyright liability—A comparative discourse on safe harbours in Singapore and India. The Journal of World Intellectual Property. https://doi.org/10.1111/JWIP.12126.

Naidu, W. (2024). Malaysia: Halt the repressive amendments to the Communications and Multimedia Act. Article 19. https://www.article19.org/resources/repressive-amendments-comunications-multimedia-act/

Parliament of Malaysia. (2024). Dewan Rakyat Parlimen Kelima Belas Penggal Ketiga Mesyuarat Ketiga. Parliament of Malaysia.

Price, L. (2021). Platform responsibility for online harms: towards a duty of care for online hazards. Journal of Media Law, 13(2), 238–261. https://doi.org/10.1080/17577632.2021.2022331

Suryawanshi, P., & Laturkar, V. (2019). Government Initiatives Towards Transformation Through Digital India. International Journal of Management and Social Sciences, 8, 81-86.

United Kingdom Online Safety Act 2023

Yeh, B. T., & Jeweler, R. (2004). Safe Harbor for Service Providers Under the Digital Millennium Copyright Act.