Indexed in Clarivate Analytics WoS,
https://ebpj.e-iph.co.uk/index.php/EBProceedings/issue/archive

E-B
Environment - Behaviour
Proceedings Journal

ISSEC2025
https://sites.google.com/view/issec-2024/home

e-IPH
e-International
Publishing House Ltd.,
United Kingdom

International Social Sciences and Education Conference 2025
"Empowering Knowledge: Driving Change Through Social Science and Educational Research"
Virtual Conference
24-25 May 2025

Organised by: CLM PUBLISHING RESOURCES

Regulating Social Media Responses to Online Harms: A comparative study between the European Union (EU) and Malaysia

Muhammad Muslim Rusli[1]*, Zalina Abdul Halim[2], Amirah Sabirah Mujahid[3]
**Corresponding Author*

[1] PhD student, University of Malaya, Kuala Lumpur, Malaysia, [2] Senior Lecturer, University of Malaya, Kuala Lumpur, Malaysia, [3] Senior Lecturer, MARA Professional College, Pahang, Malaysia

S2002539@siswa.um.edu.my, zalina@um.edu.my, sabirah.mujahid@mara.gov.my
Tel: +60132198065

Abstract

The pervasive dominance of online harms has prompted global reconsideration of digital policy and regulation. Thus, this paper compares the regulatory approaches of the EU and Malaysia in terms of their theoretical frameworks and systemic governance of online harms. This study applies comparative legal analysis and finds that while both regions initially are in favour of cyberspace sovereignty, the status quo has led to advanced regulatory responses. The EU emphasizes user protection and transparency through rights-based laws through DSA, whereas Malaysia prioritises public security via the OSB law. The findings highlight evolving state intervention in digital governance.

Keywords: Social Media Law; Digital Service Act (DSA); online harms; Malaysia Online Safety Bill (OSB)

DOI: https://doi.org/10.21834/e-bpj.v10iSI33.7065

1.0 Introduction

Digital services are at the heart of economic, educational, social, and political affairs across the globe. Indeed, cyberspace autonomy plays a critical role in empowering individuals to catalyse national progress and innovations (Diop & Asongu, 2024). Consequently, social media and online services have become indispensable technologies, integral to human development and the evolution of future civilisations.

However, cyberspace freedom comes at a formidable price. Over time, the digital realm has also become a potent vector for online harms — a broad term that refers to the range of abusive, dangerous, or manipulative behaviors in digital spaces — that spread the rampant virus of disinformation, hate speech, and propaganda on a global scale. Landmark issues like Rohingya's Islamophobia, the Trump Election 2016, and the COVID-19 disinformation vividly illustrate how swiftly and profoundly these digital threats sway public

eISSN: 2398-4287 © 2025. The Authors. Published for AMER by e-International Publishing House, Ltd., UK. This is an open access article under the CC BY-NC-ND license (http://c5eativecommons.org/licenses/by-nc-nd/4.0/). Peer–review under the responsibility of AMER (Association of Malaysian Environment-Behaviour Researchers
DOI: https://doi.org/10.21834/e-bpj.v10iSI33.7065

opinions overnight (Jr., 2024). In many cases, the velocity of digital information outpaces cultural narratives and public discourses, putting society's value in pain (Qureshi & Patel, 2025). Growing concerns over these pernicious threats have compelled nations worldwide to confront the daunting challenge of safeguarding their cultural, social, and ethical values amid this turbulent digital landscape (Child et al., 2023).

The substantial damage wrought by online harms fuels a fierce debate between the appropriate balance to preserve online freedom and effective digital oversight. Whilst some advocate for minimal intervention to protect free speech, others emphasise the urgent need for comprehensive regulatory frameworks to protect human rights and social values (Guggenberger, 2023). This delicate dance is complicated by the rapid evolution of cyberspace platforms and the internet's borderless nature, calling for a responsive and dynamic oversight. In response, governments worldwide have increasingly prioritised the development of regulatory frameworks designed to enhance transparency, accountability, and user protection. Against this complex backdrop, this study endeavours to:

1) examine the recent advancements in regulatory approaches to social media governance worldwide
2) conduct a comparative analysis between European Union (EU) and Malaysia regulatory strategies; and
3) derive lessons from both experiences on future policy directions

2.0 Literature Review

The evolution of social media regulation globally reflects a dynamic tension between the liberty of free speech and the need to address online harms. This regulatory debate began in the United States of America (U.S), the birthplace of the globe's tech titans—Meta (Facebook, Instagram), Google (YouTube), and X (formerly Twitter)— as the state consistently embraced a 'laissez-faire' stance towards internet governance. Central to this approach is Section 230 of the Communications Decency Act of 1996 (CDA), which grants online platforms broad immunity from civil liability for user-generated content. Simultaneously, the act empowers online media companies to self-regulate the online community by moderating or removing harmful content in good faith to protect the digital realm (Cobbe, 2021). This legal architecture was originally designed to foster innovation and growth of dynamic internet services including the ability to protect the digital realm from online harms without government policy intervention. S230 of CDA has been instrumental to the internet's evolution of Web 1.0— from read-only content —to user-driven content and interactive services by virtue of Web the 2.0 era (Huddleston, 2022). The broad immunity granted under this Act empowers prosperity and innovation in the digital ecosystem. Yet, the same structure also weakens regulatory oversight as online harms become increasingly evident and proliferated under the purview of tech giants.

Thus, the structural freedoms of Web 2.0 expose significant regulatory gaps against the tide of online harms. Despite continuous judicial reinforcements that favour online platform's immunity —even when such rulings clash with foreign jurisdictions— high-profile cases such as the Snowden revelation and Cambridge Analytica scandal proved the disproportionate power wielded by tech giants but unregulated across cyberspace (Ibrahim et al., 2024). Furthermore, the online safeguards promoted by these companies have been exposed as superficial —only smoke and mirrors— raising doubts about their credibility and effectiveness (Hemphill & Banerjee, 2021). Accordingly, these issues trigger international concern over the failure of market-driven accountability. A wave of regulatory reforms began championed by Germany's Network Enforcement Act (NetzDG) 2018. The NetzDG law requires online platforms to swiftly remove unlawful content or face significant fines (Echikson & Knodt, 2018). This legislation marked a decisive move towards state-led digital governance, caused a wave of digital governance reforms across Europe, and influenced non-European states to assert sovereign control over their digital environments (Mchangama & Fiss, 2019).

This global recalibration on digital governance reflects public concern, especially among nation-states on the infestation of online harms in their territorial cyberspace boundary. Given the diversity of cultural values, beliefs, and social norms worldwide, many countries have sought to shield their national identity, social cohesion, and security through new regulatory frameworks (Suzor, 2019). Countries like India (Information Technology Rules 2021), Singapore (Online Safety (Miscellaneous Amendments) Act), Australia (Online Safety Act 2021), and the United Kingdom (Online Safety Bill) have introduced contemporary regulatory instruments that balance free speech with public security, reflecting unique cultural, political, and national interests. These jurisdictions openly resist the laissez-faire ethos under CDA which they view as enabling platform impunity and undermining transnational regulatory aspirations. In contrast, these nations advocate for stronger accountability measures and sovereign control over platform governance distinctive from the U.S.-centric digital liberalism (Johnson & Castro, 2021).

Building on this momentum, the European Union (EU) has introduced the Digital Services Act (DSA) 2022 as a comprehensive regulatory framework to address challenges related to online intermediaries and online harms. The Act represents a significant step to ensure online media providers are accountable and transparent in addressing users' expectations against the proliferation of online harms. Moreover, the DSA is a strategic milestone in the EU's pursuit of digital sovereignty; reducing dependency on foreign digital technologies and asserting greater control over digital infrastructure and data flows within her borders (Pohle, 2020). This legislative approach exemplifies the "Brussels Effect" where the EU's benchmark influences global digital governance norms and inspires other nations to adopt similar frameworks (Bueno & Canaan, 2024).

This global trend has also taken root in Southeast Asia where countries like Malaysia accelerate their own robust national online governance blueprint. Even as a relatively late entrant into the online regulatory arena, Malaysia has long enacted foundational legislation on internet governance through Communications and Multimedia (CMA) 1998 with the Malaysia Communication and Multimedia Commission (MCMC) as the central authority. The in-progress Online Safety Bill 2024 is supposed to complement CMA in addressing online harm, a significant pivot from a traditionally reactive approach to a more preventive/curative digital governance model (Article 19, 2024). Inspired by developments in the Western countries and other ASEAN countries, Malaysia's framework also aligns

with broader regional efforts such as the ASEAN Digital Masterplan 2025, emphasising the harmonization of digital regulations across Southeast Asia.

Correspondingly, the convergence towards stronger regulatory oversight is a global socio-political phenomenon. As global digital interdependence increases, states are reasserting digital sovereignty to safeguard national identity, public order, and democratic integrity. The EU and Malaysia exemplify this trend by integrating human rights considerations, platform responsibility, and adaptive regulatory strategies to manage the complexities of online ecosystems.

3.0 Methodology

This study employs a comparative method of legal study, which involves comparing legal rules and concepts between the EU and Malaysia. Comparative law is defined as a scientific process where legal elements are examined concerning countries (Samuel, 2014) to describe and analyze their similarities and differences. This paper aims to uncover the underlying intellectual concepts and philosophical values between both institutions beyond mere textual comparison (Edward J. Eberle, 2011). The multiple analytical techniques under this method ensure a comprehensive evaluation of a coherent and rigorous legal science (Husa, 2024). The comparative approach elucidates how the EU and Malaysia respond to common technological challenges such as fundamental liberties, prevention of online harms, institution designs for oversight, platform accountability and multi-stakeholder participation in digital governance while preserving their unique jurisprudential traditions as well as policy objectives.

The nations are chosen because the EU represents the most comprehensive regional effort framework for digital governance while Malaysia exemplifies distinctive regulatory models that reflect local sociocultural priorities. This North-South comparative axis offers valuable insights into the global dynamics of digital governance, revealing both the potential for regulatory convergence and the persistence of meaningful jurisdictional particularities. Moreover, the temporal proximity of these legislative initiatives (with both the DSA and OSB representing contemporary responses to online harms) ensures that the comparison remains analytically coherent while accounting for current technological and policy developments.

The comparative method applies data and evidence analysis through the examination of existing documents and records (Glenn, 2009). Thus, books, journals, newspapers, academic commentary, policy analyses, stakeholder responses and digital documents about DSA and OSB concerns will be referred to in this article. This source triangulation evidence captures both the formal legislative provisions and practical applications of each regulatory regime – academic, economic and social context.

4.0 Findings – Similarities between the Digital Service Act (DSA) and the Online Safety Bill (OSB)

The EU DSA and Malaysia OSB stand out as landmark regulatory frameworks for digital cyberspace. While both instruments originate from distinct legal and geopolitical contexts— the EU represents a supranational body belonging to the EU region while Malaysia is a country in Southeast Asia— both aim to enhance online safety, intermediary liability, and user protection.

This section aims to identify and analyze the key similarities between the DSA and the OSB by examining eleven (11) critical variables that underpin each legislative instrument; **application, harm mitigation, content risks definition, user empowerment, minor protections, transparency obligation, legal authority, intermediary liability, extra-territorial reach, media platform quasi-judiciary power and dispute resolution.**

The comparative data presented in the following table outlines the overlapping features and functional parallels of the DSA and OSB across these variables below:

Table 1. Similarities between DSA and OSB

Categories	Digital Services Act (DSA)	Online Safety Bill (OSB)
Application	Applies to all licensed application service/content/network providers in Malaysia (S2 (1)(a)(b)(c) of OSB, Regulation 2 (a) (b) Communications and Multimedia (Licensing) (Exemption) (Amendment) Order 2024) Excludes private messaging feature (S2(1)(d) of OSB) Focuses on providers with more than eight (8) million users (Regulation 5 (d)(e) Communications and Multimedia (Licensing) (Exemption) (Amendment) Order 2024)	Applies to all intermediary services conduit/caching/hosting services (S2(1) and S3(g) of DSA) Extra obligations apply to VLOPS with over 45 million users (A33(1) of DSA)
Harm Mitigation	Media providers must mitigate the risk of exposure to harmful and priority harmful content (S13 and 19 of OSB)	VLOPS must mitigate risks related to illegal content and systemic risks (Articles 34 and 35 of DSA) Small and micro enterprises are exempt from this duty (A19 of DSA)
Content risk definition	Defines Harmful content under S4 and the First Schedule of OSB.	Defines Illegal contents under A3(h) of DSA; per EU members state law

User empowerment	Requires mechanisms for user reporting, user assistance, and self-management of online safety (S15-17 of OSB)	Requires user reporting mechanisms for illegal content and empowers users with clear information and redress. (A16-17, 20 and A27(1) of DSA)
Minor protection	Special duties to protect child users and their online safety. (S18, S22(3) (a), Second Schedule of OSB)	Special obligations for VLOPs to protect minors, including protection from illegal content and targeted advertising (A14(3), A28, A34(d), A359j), and A44(j) of DSA.)
Transparency obligation	Require issuance guidelines on online safety measures and content moderation (S14 of OSB)	Requires clear, transparent terms and conditions (A14(1)(2) of DSA), regular public transparency reports (A15(1), A24(1) of OSB) and advertising (A39 0f OSB)
Legal Authority	Enforcement and investigation power granted to the MCMC (S30-39, 52-68 of OSB), including financial penalties (S23(9), S25(4), S30(9), S32(6)(7)(8), S39, S61(3), S62, S75(2), S81(3) of OSB)	Enforcement by national authorities and European Commission (A13(2), A49 (1)(2), A51, S4 (A64-73) of USB), investigatory power (A59, A60 of USB) and fines for non-compliance (A74 of OSB).
Intermediary liability	Imposes limited fines on media companies Potential individual liabilities for directors and officers (S73 of OSB)	EU members and the EU Commission may impose 6% fines of annual turnover for non-compliance (A52 and A74 of DSA)
Extra-territorial reach	Applies to foreign providers serving Malaysian users. (S3 of OSB)	Applies to foreign providers serving EU users (A2 of DSA)
Media platform quasi-judiciary power	Recognises quasi-judiciary power of media platform companies (S21 and S22 of OSB)	Recognises quasi-judiciary power of media platforms (A20 of DSA)
Dispute resolution	Established Online Safety Tribunal (S40 of OSB) MCMC's decision can be appealed to the Online Safety Tribunal (S41 of OSB) The Tribunal decision is equal to a High Court Decision (S47 of OSB) Tribunal decision is non-appealable (S46 of OSB)	Prefers out-of-court settlement under (A21 of DSA) available to each EU member's court. National courts are limited in overruling EU Commission decisions (A82 (3) of DSA) EU members cannot question the EU Commission decision (A69(10) of DSA) EU Commission decision can be reviewed (S67 (3) of DSA) A final appeal to the Court of Justice (A81 of DSA and A261 of the Treaty on the Functioning of the European Union (TFEU))

Both DSA and OSB represent two contemporary legal instruments designed to regulate digital space. While these laws emerge from distinct legal jurisdictions—one from a supranational body and the other from a national legislature—they share regulatory focus areas such as intermediary responsibility, user safety, harm mitigation, and protection of minors. This section presents a parallel comparison of the DSA and OSB across key regulatory dimensions.

5.0 Discussions: Comparison Value

5.1 Regulatory Focus and Convergence

The legislative comparison between OSB and DSA represents a dynamic alignment in regulatory intent to address online harms. The DSA forms part of the "Europe Fit for the Digital Age" vision anchoring on a rights-based legal infrastructure and extensively researched by decades on online harms. Therefore, the Act was built on earlier voluntary frameworks—such as the GDPR, the Code of Practice on Disinformation, and the Code of Conduct on Hate Speech—while acknowledging their limitations. As such, the EU has legislated binding legislative instruments via the DSA, the Digital Markets Act (DMA), and the Chips Act to achieve digital sovereignty objectives; critical infrastructure acquisition, and local technological innovation over-dependence on foreign technology (Roberts et al., 2021).

In contrast, the OSB adopts a context-pragmatic approach suited to Malaysia's environment. This Act complements the foundational internet regulatory model under CMA.

Although neither DSA nor OSB explicitly incorporates the GNI Principles or the Manila Principles on Intermediary Liability and UNESCO Guidelines for regulating digital platforms: a multistakeholder approach to safeguarding freedom of expression and access to information, their regulatory concerns reflect the values in these frameworks; a tacit recognition on global principles of online harms governance.

This convergence gives way to divergence in institutional implementation as explored below.

5.2 Institutional Design and Interest

A notable difference lies in the institutional depth of the regulatory structure. The DSA imposes a tiered obligation against VLOPs with a supranational oversight structure with Digital Services Coordinators (DSCs) appointed across EU Member States (Sagar & Hoffmann,

2021). Meanwhile, the OSB introduces the Online Safety Tribunal as a user-friendly dispute resolution mechanism within a national administrative framework. This tribunal-based model allows Malaysia to take an incremental yet direct approach to cyberspace regulation sustaining her social media development aligned with national interests.

This contrast illustrates a broader difference in regulatory traditions; the DSA operates as a transnational governance framework, while the OSB embeds digital governance within a domestic structure.

5.3 Stakeholder Integration

Another distinct feature designated by both legislation is the stakeholder's involvement. The DSA assigns operational roles to 'trusted flaggers' under 22(2) of the DSA, thereby involving civic participation directly in content moderation processes. By contrast, the OSB contemplates civil participation in a consultative role through the Online Safety Committee, whose composition is subject to ministerial discretion under Section 5(3) of OSB. While both frameworks acknowledge the importance of non-governmental expertise, the EU model leverages more public enforcement participation to civil actors.

Thus, while both frameworks acknowledge the role of non-state actors, the DSA institutionalises participatory enforcement whereas the OSB centralises control within the executive — distinct models of regulatory legitimacy between them.

5.4 Enforcement and Transparency

A further point of comparison lies in the enforcement and transparency provisions of each framework. The DSA's supranational structure fosters a proactive compliance culture (Leerssen, 2023). Current proceedings against Meta, X and TikTok reflect significant regulatory pressure. For instance, the EU Commission secured a concession from TikTok through the suspension of TikTok Lite's rewards feature (TikTok Lite Rewards Programme, 2024). Additionally, the EU's transparency extends beyond procedural requirements to public scrutiny as enforcement updates and compliance evaluations are available online.

Conversely, the OSB's enforcement remains nascent with limited success preceded by MCMC. While transparency is required under S14 and S30-39 of OSB, the Act lacks procedural visibility and public accountability present in the EU's model.

This divergence suggests a more mature compliance culture within the EU while Malaysia's enforcement framework is still consolidating procedural visibility and public accountability.

5.5 Media-User Agreement

Both legislative instruments emphasise media-user agreements. A14 of DSA mandates that terms of service be intelligible, accessible, and transparent — particularly concerning algorithmic recommendations and content takedowns (Decarolis & Li, 2023).

Meanwhile, S14-20 of OSB states the required media providers to prepare guidelines and Online Safety Plans; with a greater emphasis on user protection and security rather than user autonomy. This structure complements Part VIII: Consumer Protection S188-190 of the CMA 1998 and Part 3: Advertisement (Marketing Communications) of Content Code 2022 which already implicit fair and transparent terms and conditions.

This contrast illustrates differing regulatory priorities: the DSA champions user agency and informed consent whilst the OSB leans toward a state-driven duty integrated into protective governance.

5.6 Corporate Engagement

Corporate engagements illuminate further the functional effectiveness between the two (2) regimes. The EU's extensive engagement with tech titans through more than 270 consultations on the DSA reinforces a balanced policy dialogue. Industry concerns—such as Microsoft's caution over the rush to regulate—depict an equilibrium between legislative ambition and corporate counsel. Moreover, voluntary instruments like the EU Code of Practice on Disinformation (with 44 signatories) and the Hate Speech Code (12 signatories) laid the groundwork for regulatory expectations ahead of the DSA (Bank et al., 2021). Importantly, multi-stakeholder involvement— tech platforms, academics, and NGOs—was a pivotal element of the EU's regulatory process (Rudohradská & Treščáková, 2021).

Unfortunately, the OSB does not yet reflect this depth of corporate pre-engagement and may benefit from a state-corporate dialogue approach as implementation matures.

This comparative gap underscores the importance of multistakeholder engagement not only for norm-setting but also for fostering regulatory compliance and trust.

In sum, both DSA and OSB reflect distinct regulatory traditions — the former is supranational and participatory while the latter is national and state-driven — yet share a converging ambition to regulate cyberspace. Despite differences in demographical practice, this convergence shows a consensus on the need to domesticate and humanise the digital environment—whether through the Brussels effect or the state-driven frameworks.

6.0 Conclusion& Recommendations

Both the EU Digital Services Act and Malaysia's Online Safety Bill embody ambitious responses to digital ecosystem regulation. Their architecture demonstrates a clear recognition that online harms demand robust regulatory intervention. Yet, as these laws strive to make the internet safer, they also raise a dichotomy about the balance between security and fundamental rights.

A central concern is the potential for these regimes to impede freedom of speech and privacy. The DSA attempts to safeguard rights while imposing obligations on tech giants. Meanwhile, the OSB focuses on user protection but faces scrutiny over the broad content

definitions and huge discretionary powers held by MCMC. Nevertheless, both mechanisms must grapple with the risk of overreach into tools for censorship or surveillance.

Notwithstanding these comparative insights, several limitations of this study warrant acknowledgment. The asymmetrical maturity of these regulatory frameworks presents analytical challenges — the DSA builds upon decades of EU digital policy development while the OSB represents a more abrupt shift in Malaysia's regulatory approach. Moreover, as both instruments are nascent, their long-term efficacy is provisional rather than conclusive. This temporal constraint means the comparative legal method could not fully encapsulate ground-level enforcement dynamics or platform adaptation strategies.

Therefore, potential research direction should assess longitudinal regulatory impacts — especially on society's protection against online harms and corporate compliance practices — to evaluate the legislative effectiveness in both regions.

Paper Contribution to Related Field of Study

The study significantly advances the legislative comparative concepts between European Union Digital Service Act (DSA) and Malaysia Online Safety Bill (OSB) regulations, offering valuable insights for scholars, policymakers, and practitioners in online safety regulation, online harms concepts, and public policy.

References

Article 19. (2024). *Malaysia : Concerns with the Online Safety Bill*. Article 19.

Bank, M., Duffy, F., Leyendecker, V., & Silva, M. (2021). The Lobby Network: Big Tech's Web of Influence in the EU. In *Corporate Europe Observatory and LobbyControl e.V.*

Bueno, T. M., & Canaan, R. G. (2024). The Brussels Effect in Brazil: Analysing the impact of the EU digital services act on the discussion surrounding the fake news bill. *Telecommunications Policy*, *48*(5), 102757. https://doi.org/10.1016/j.telpol.2024.102757

Child, D., Hanna, J.-O., Hildreth, A., & Grant, J. I. (2023). *Toolkit for Digital Safety Design Interventions and Innovations: Typology of Online Harms* (Issue August). https://www3.weforum.org/docs/WEF_Typology_of_Online_Harms_2023.pdf

Cobbe, J. (2021). Algorithmic Censorship by Social Platforms: Power and Resistance. *Philosophy and Technology*, *34*, 739–766. https://doi.org/10.1007/s13347-020-00429-0

Decarolis, F., & Li, M. (2023). Regulating online search in the EU: From the Android case to the digital markets act and digital services act. *International Journal of Industrial Organization*, *90*,102983. https://doi.org/10.1016/j.ijindorg.2023.102983

Diop, S., & Asongu, S. A. (2024). Information and Communication Technologies as Catalyst for the Achievement of Sustainable Development Goals at the Local Level in Africa. *Forum for Social Economics*, 1–19. https://doi.org/10.1080/07360932.2024.2387099

Echikson, W., & Knodt, O. (2018). Germany's NetzDG: A key test for combatting online hate. *CEPS Research Report No. 2018/09*.

Edward J. Eberle. (2011). The Methodology of Comparative Law. *Roger Williams University Law Review*, *16*(1), 51–72. https://doi.org/10.1080/18758444.1994.11788003

Glenn, A. B. (2009). Document Analysis as a Qualitative Research Method. *Qualitative Research Journal, 9*(2), 27–40. doi:10.3316/qrj0902027

Guggenberger, N. (2023). Moderating Monopolies. *Berkeley Technology Law Journal*, *38*, 119–171.

Hemphill, T. A., & Banerjee, S. (2021). Facebook and self-regulation: Efficacious proposals – Or 'smoke-and-mirrors'? *Technology in Society*, *67*,101797. https://doi.org/10.1016/j.techsoc.2021.101797

Huddleston, J. (2022). Competition and Content Moderation: How Section 230 Enables Increased Tech Marketplace Entry. *Cato Policy Analysis*,922; 1-14.

Husa, J. (2024). Traditional Methods. In M. Siems & P. J. Yap (Eds.), *Cambridge Handbook of Comparative Law* (pp. 15–31). Cambridge University Press.

Ibrahim, H., Debicki, M., Rahwan, T., & Zaki, Y. (2024). Big Tech Dominance Despite Global Mistrust. *IEEE Transactions on Computational Social Systems*, *11*(3), 3741–3752. https://doi.org/10.1109/TCSS.2023.3339183

Johnson, A., & Castro, D. (2021). How Other Countries Have Dealt With Intermediary Liability. *Information Technology & Innovation Foundation*, *February*, 1–14. https://itif.org/publications/2021/02/22/how-other-countries-have-dealt-intermediary-liability

Krotoszynski, R. J Jr. (2024). Disinformation, Misinformation, and Democracy: Defining the Problem, Identifying Potentially Effective Solutions, and the Merits of Using a Comparative Legal Approach. In R. J. Krotoszynski, A. Koltay, & C. Garden (Eds.), *Disinformation, Misinformation and Democracy* (pp. 1–34). Cambridge University Press.

Leerssen, P. (2023). An end to shadow banning? Transparency rights in the Digital Services Act between content moderation and curation. *Computer Law and Security Review*, *48*,105790. https://doi.org/10.1016/j.clsr.2023.105790

Mchangama, J., & Fiss, J. (2019). The Digital Berlin Wall: How Germany (Accidentally) created a prototype for global online censorship. *Justitia.*

Pohle, J. & T. T. (2020). Digital Sovereignty. *Internet Policy Review*, *9*(4), 1–19. https://doi.org/10.15211/SOVEUROPE220214049

Qureshi, A., & Patel, M. (2025). *When Lies Outpace Truth : How Disinformation undermines AI during conflict events & national crises*. Byesforall.Pk. https://www.bytesforall.pk/post/when-lies-outpace-truth-how-disinformation-undermines-ai-during-conflict-events-national-crises

Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: An analysis of statements and policies. *Internet Policy Review*, *10*(3), 1–28. https://doi.org/10.14763/2021.3.1575

Rudohradská, S., & Treščáková, D. (2021). Proposals for the Digital Markets Act and Digital Services Act: Broader Considerations in Context of Online Platforms. *EU and Comparative Law Issues and Challenging Series (ECLIC)*, *5*, 487–500. https://doi.org/10.25234/eclic/18317

Sagar, S., & Hoffmann, T. (2021). Intermediary Liability in the EU Digital Common Market – from the E-Commerce Directive to the Digital Services Act. *Revista de Internet, Derecho y Politica*, *34*, 1–12. https://doi.org/10.7238/IDP.V0I34.387691

Samuel, G. (2014). *An Introduction to Comparative Law Theory and Method* (Vol. 16, Issue 1). Hart Publishing.

Suzor, N. P. (2019). *Lawless: The Secret Rules That Govern our Digital Lives*. Cambridge University Press. https://doi.org/10.1017/9781108666428

TikTok Lite Rewards Programme. (2024).