

Nidhal, Muhammad; Aaron, Rasya Athalla; Alfarisi, Aldrich

**Research Report**

## Shadows of censorship: Indonesia's content moderation policy development

Policy Brief, No. 31

**Provided in Cooperation with:**

Center for Indonesian Policy Studies (CIPS), Jakarta

*Suggested Citation:* Nidhal, Muhammad; Aaron, Rasya Athalla; Alfarisi, Aldrich (2025) : Shadows of censorship: Indonesia's content moderation policy development, Policy Brief, No. 31, Center for Indonesian Policy Studies (CIPS), Jakarta

This Version is available at:

<https://hdl.handle.net/10419/324483>

**Standard-Nutzungsbedingungen:**

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

**Terms of use:**

*Documents in EconStor may be saved and copied for your personal and scholarly purposes.*

*You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.*

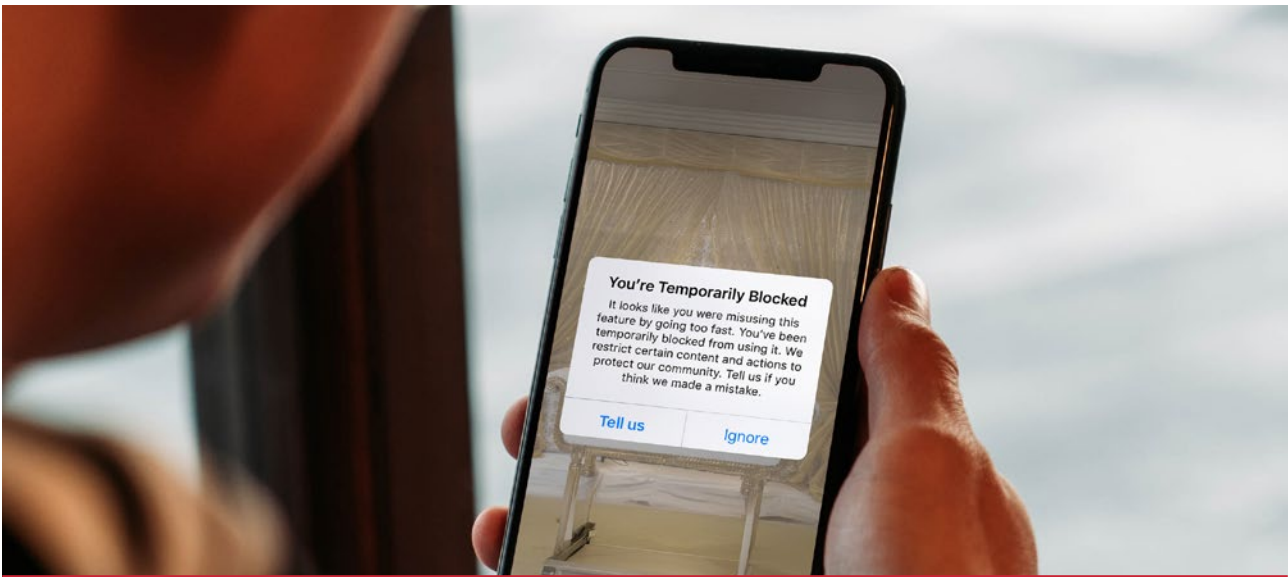
*If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.*



Policy Brief No. 31

## Shadows of Censorship: Indonesia's Content Moderation Policy Development

by Muhammad Nidhal, Rasya Athalla, and Aldrich Alfarisi



### Key Messages

- Indonesia's content moderation framework, governed by MOCI Regulation No. 5/2020, is often criticized for its lack of transparency, inconsistent enforcement, and broad legal definitions that risk overreach and censorship if applied indiscriminately.
- While efforts have been made to enhance the clarity of content moderation implementation, the framework outlined in MOCI Decree No. 522/2024 leaves considerable room for improvement, particularly regarding security, transparency, accountability, and the dual authority over content moderation.
- The rollout of the SAMAN system introduces additional content moderation measures at a time when Indonesia's startup ecosystem is facing a critical funding downturn, with investments dropping from USD 10.9 billion (IDR 174 trillion) in 2021 to just USD 800 million (IDR 13 trillion) in 2024.
- In Indonesia, deliberate state interference over the internet takes several forms, including total shutdown, internet throttling, and service blocking, with an estimated economic impact of a one-day total shutdown costing USD 53 million (IDR 848 billion) in GDP losses, while blocking online services for the same duration led to a USD 7 million (IDR 112 billion) loss.
- To balance the imperative of tackling harmful online content while safeguarding fundamental rights and accounting for local context, Indonesian policymakers should adopt a more balanced, transparent, and nuanced approach. This entails shifting from censorship-driven measures to a rights-focused approach; establishing unambiguous content definitions while following due process; improving the SAMAN system for consistent enforcement; fostering meaningful co-governance with relevant stakeholders; and committing to greater transparency and public oversight.



## Regulating Online Content: The Current Situation

Digital platforms have become a critical conduit of connectivity between businesses and millions of Indonesian consumers. Data from the Indonesian Internet Service Provider Association shows that Indonesia's internet penetration rate was at 79.5% in 2024, expected to increase 8% by 2030 (APJII, 2024; Twimbit, 2024). Over half of the 285 million people throughout Indonesia actively engage in social media, ranking third in Asia Pacific, after China and India, and first in Southeast Asia (Kemp, 2025). This extensive digital outreach has enabled the emergence of large volumes of user-generated content (UGC), among which illegal, harmful, and inappropriate materials pose challenges for maintaining the integrity of Indonesia's online space.

The Indonesian government, through the Ministry of Communication and Digital Affairs<sup>1</sup> (MCDA), has already taken notable measures to regulate online content, the implementation of which has drawn considerable criticism. The Electronic Information and Transactions (ITE) Law, first enacted in 2008 and amended in 2016 and 2024, remains the backbone of Indonesia's digital governance—designed to address issues such as electronic transactions, online content<sup>2</sup>, and cybercrime—specifically those associated with illegal and harmful content<sup>3</sup> (Mastur, 2016). It is under this law that MOCI Regulation No. 5/2020 on Private Electronic System Operators (ESOs<sup>4</sup>)—hereinafter MR5/2020—was introduced, which outlines Indonesia's content moderation framework and requires domestic and foreign ESOs, such as cloud computing providers, UGC platforms, and other applications serving Indonesians, operating in Indonesia to register with the government and comply with takedown requests for prohibited content.

In essence, the ministerial regulation grants MCDA more authority to access user data for law enforcement purposes, as well as hold platforms accountable to remove content deemed in violation of Indonesian law, such as public incitement or discrimination based on ethnicity or religion, with a strict turnaround time of four hours for urgent takedown requests and 24 hours for non-urgent ones. Failure to comply can result in heavy financial penalties and, ultimately, service shutdown. To streamline compliance and enforce fines for platform violations<sup>5</sup>, MCDA issued MOCI Decree No. 172/2024, later amended by MOCI Decree No. 522/2024 (Decree 522/2024), which introduced the Content Moderation Compliance System (*Sistem Kepatuhan Moderasi Konten*, abbreviated as SAMAN)—a centralized portal to manage content takedown requests and track violations. See Figure 1 for an illustration of the SAMAN workflow, detailing the step-by-step process of takedown requests, compliance pathways, and enforcement measures.

---

<sup>1</sup> Formerly known as the Ministry of Communication and Informatics (MOCI).

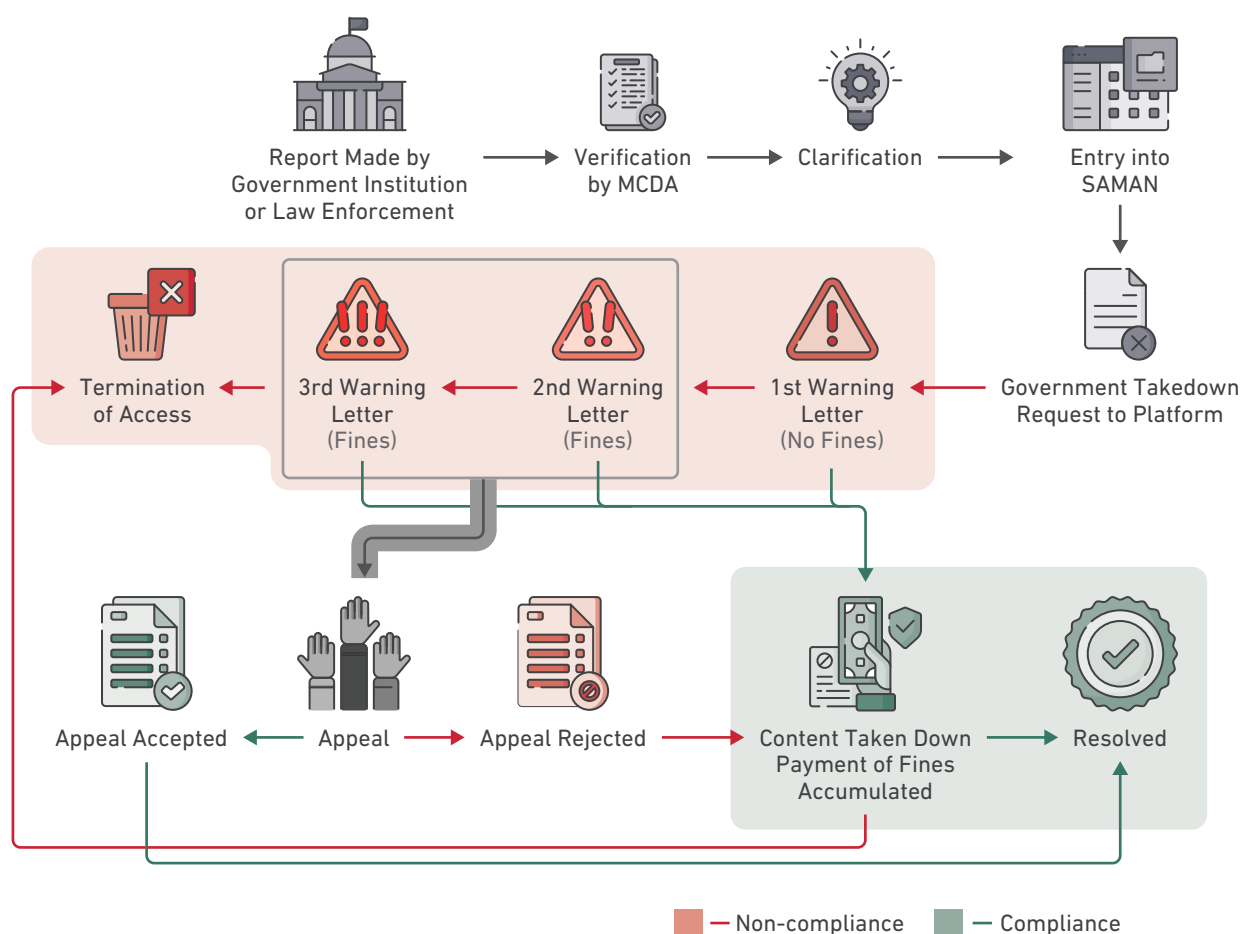
<sup>2</sup> Although the ITE Law did not explicitly define 'content,' it may be interpreted as any electronic information and electronic documents as further outlined in Article 1 of the law.

<sup>3</sup> The law uses the term 'illegal content' (*konten ilegal*) to refer to electronic information and/or electronic documents containing: content that violates decency; gambling content; slander or defamation; extortion and/or threats; false and misleading news resulting in losses; hatred or hostility based on ethnicity, religion, race, and class; and threats of violence or intimidation that are directed at an individual.

<sup>4</sup> Broadly defined as any person, state officials, business entity, and community that provides, manages, and/or operates electronic systems individually or collectively for their users (Article 1 (5) of the MR5/2020). They serve their own needs or those of other parties.

<sup>5</sup> See Annex 1 for SAMAN's technical process.

**Figure 1.**  
**Content Takedown Request Mechanism Under SAMAN**



Source: Author's compilation based on MOCI Decree No. 522/2024

## Content Governance Gaps: MOCI Regulation No. 5/2020 and SAMAN

Despite commendable regulatory efforts, governance gaps remain in Indonesia's approach to content moderation. At the regulatory level, MR5/2020 and its implementing rule—Decree 522/2024—mandate stricter compliance for content takedown under the threat of administrative fines for non-compliance. The broad definition of “negative content,” coupled with government-centered takedowns and the lack of clear procedural guidelines for moderating ambiguous “gray-area” cases—such as political criticism or satire—raises concerns over potential overreach (SAFE-net, 2021). The state's concentration of power over online content governance increases the risk of abuse, censorship, and the erosion of online freedoms<sup>6</sup>.

In a February 2025 focused group discussion (FGD) convened by the Center for Indonesian Policy Studies (CIPS), representatives from the private sector and civil society coalitions expressed their concerns regarding the current content moderation governance (MR5/2020 and Decree 522/2024). Table 1 summarizes these concerns.

<sup>6</sup> Rights protected under Article 28 of the 1945 Constitution, Law No. 9/1998 on Freedom to Express Opinions in Public, and Law No. 39/1999 on Human Rights.

**Table 1.**  
**Stakeholders' Concerns in the Current Content Moderation Governance**

Thematic Issue	Stakeholder Concerns	Potential Implications
<b>Legal Risks</b> (ambiguity and overreach)	<ul style="list-style-type: none"> <li>• Opaque and broad definition of “public disorder” (Article 9(4)b) leaves room for over-censorship and arbitrary enforcement.</li> <li>• Absence of institutional safeguards to prevent abuse by either the government or platforms.</li> </ul>	<ul style="list-style-type: none"> <li>• Risk of excessive online censorship and reduced democratic discourse in the digital sphere.</li> <li>• Increased prevalence of politically-motivated takedown requests.</li> <li>• Erosion of freedom of expression and digital rights of users.</li> </ul>
<b>Governance Gaps</b> (transparency, due process, and SAMAN's security risks)	<ul style="list-style-type: none"> <li>• Lack of due process for content takedowns and appeals for both platforms and users (including content creators) to the government.</li> <li>• No independent review or appeal process is available to contest content takedown requests for platforms or decisions for the users.</li> <li>• The absence of data privacy and security safeguards for SAMAN, including third-party cybersecurity assessments and certifications.</li> </ul>	<ul style="list-style-type: none"> <li>• The absence of due process creates legal uncertainty for the tech industry and erodes public trust in regulatory systems.</li> <li>• Potential user privacy issues and data breaches.</li> </ul>
<b>Operational Feasibility</b> (strict compliance burdens)	<ul style="list-style-type: none"> <li>• Requires digital platforms to take down “prohibited content” within 24 hours (4 hours if urgent) or face penalties and internet blocking threats from MCDA.</li> </ul>	<ul style="list-style-type: none"> <li>• Impractical and excessively tight deadlines potentially force over-censorship by platforms and increased regulatory costs, especially for smaller firms.</li> <li>• Loss of trust in digital platforms and reduced user engagement.</li> </ul>
<b>Multi-stakeholder oversight</b> (government accountability to stakeholders)	<ul style="list-style-type: none"> <li>• Currently, there is no clear mechanism for holding the government accountable in content moderation.</li> <li>• Participants remain skeptical of a government-led independent oversight body as long as regulators prioritize censorship-driven content governance over a rights-based framework.</li> </ul>	<ul style="list-style-type: none"> <li>• Reduced credibility and the erosion of trust in governmental enforcement of content moderation.</li> <li>• The absence of an independent oversight body leads to concerns about fairness in content moderation.</li> <li>• Public perception of MCDA's ‘unfair’ content moderation is worsened, potentially hampering future attempts at streamlining content moderation.</li> </ul>
<b>Unintended Consequences</b> (economic loss and decline in investment)	<ul style="list-style-type: none"> <li>• Regulatory uncertainties and impractical implementation deter tech companies from investing or expanding in Indonesia.</li> <li>• Compliance costs divert resources from business growth.</li> </ul>	<ul style="list-style-type: none"> <li>• Stifled innovation in Indonesia's digital economy.</li> <li>• Job losses and reduced market competitiveness.</li> </ul>

Source: CIPS FGDs with the private sector and civil society (2025)

The stakeholders' concerns above highlight how Indonesia's content moderation governance, particularly under MR5/2020 and Decree 522/2024, is riddled with structural vulnerabilities. The strict, onerous timelines for content removal—only four hours for urgent and 24 hours for non-urgent cases—coupled with broad and vague definitions of prohibited content, may force users to self-censor, or platforms to preemptively take down perceived borderline content in order to avoid sanctions. This threatens the users' already fragile freedom of expression, particularly for journalism, satire, or political commentary that may be misinterpreted by regulators.

As for the SAMAN, established through MOCI Decree No. 172/2024 and amended by Decree No. 522/2024, the system was intended to bring procedural clarity and address long-standing criticisms of the MR5/2020 regime. SAMAN was designed to further streamline takedown procedures, increase transparency for content assessment, and provide a phased penalty structure to ensure proportional enforcement. It also introduced procedural pathways for appeals, which were previously absent under MR5/2020. Despite these efforts, questions remain about the system's overall effectiveness.

The SAMAN system's design is flawed due to its restrictive conditions and lack of independent oversight. The requirement that platforms first comply with the takedown order before lodging an appeal—either by removing the content and committing to payment or waiting until the third warning—eliminates the possibility of a meaningful review before enforcement. This process assumes guilt before due process, effectively forcing compliance regardless of whether the content was flagged incorrectly. Meanwhile, in principle, all law in Indonesia provides the right for all individuals to be presumed innocent until judicially proven guilty, as stipulated in Law No. 39/1999 on Human Rights.

The appeal process under SAMAN is carried out by the same government body that issued the takedown—the MCDA. With only 10 days allotted for review by MCDA, complex cases involving satire, news, or fair use, risk being rushed or mishandled. Furthermore, SAMAN's current one-year pilot phase covers limited content types such as child pornography, online gambling, terrorism, and illegal financial activity. However, once fully enforced, it will apply to all prohibited content under Indonesia's Criminal Code.

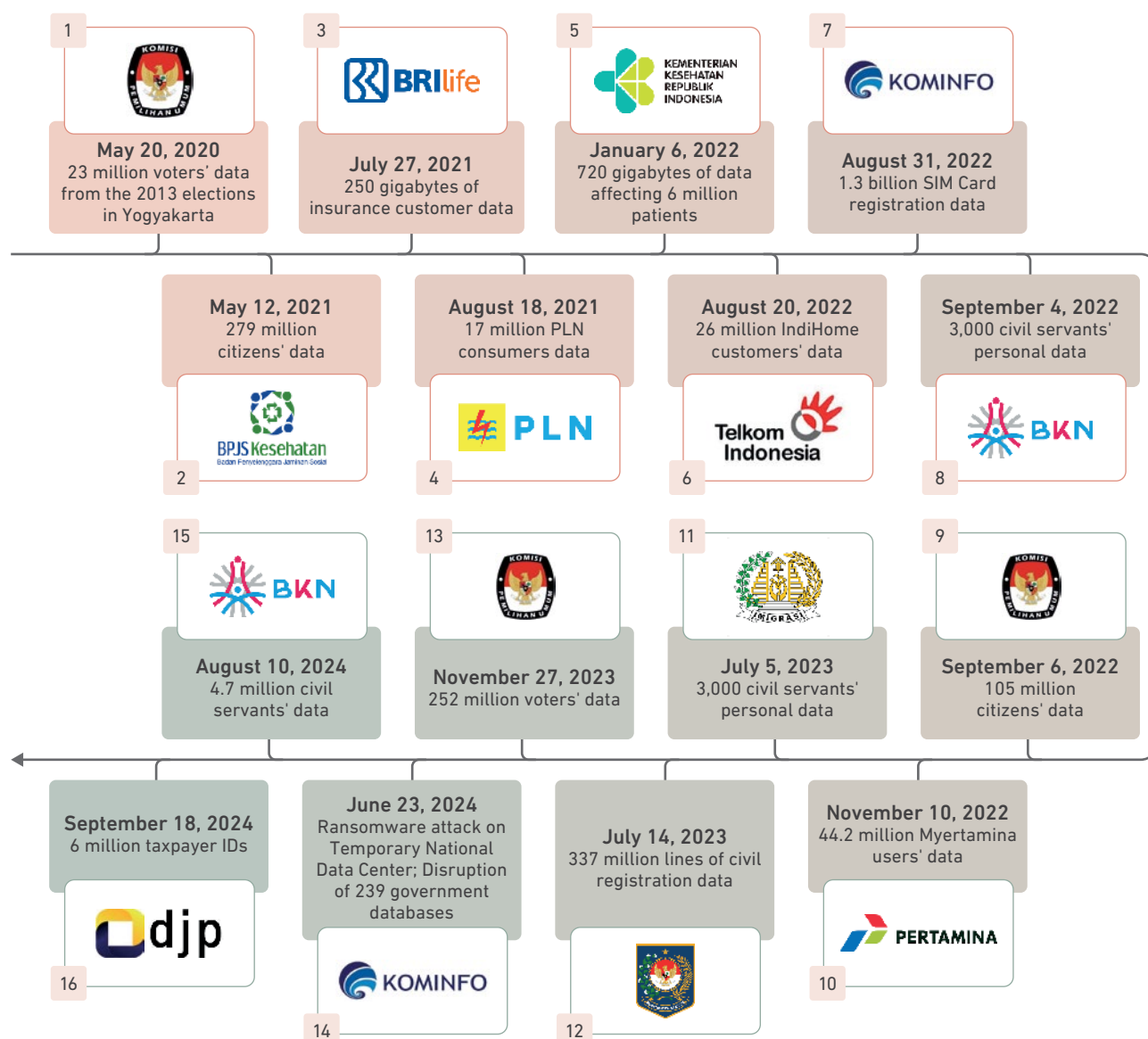
In this transitional phase, regulatory gaps allow institutions outside of MCDA, such as the National Police's Cyber Crime Directorate, to bypass SAMAN and issue takedown requests directly, adding to the fragmented enforcement landscape (Octavia & Setuningsih, 2025). Regional and local departments of the National Police have also exercised this in the past, especially nearing public holidays and elections (Ginta & Arief, 2023; Chariris, 2019; Maluku Regional Police, 2024).

Hence, instead of streamlining enforcement, the overlapping authorities in content moderation fuel ad-hoc, discretionary action across government bodies, going against the government's goal of digital bureaucratic reform. The result is a patchwork of standards vulnerable to personal biases, inconsistent enforcement, a reduced platform and less public trust in Indonesia's content moderation enforcement.

Beyond conflicts of authority, data security remains a pressing concern with the Indonesian government's poor track record in handling sensitive information. The MCDA and its predecessor have been implicated in multiple high-profile data breaches, repeatedly exposing millions of user-submitted records (Figure 2). Data from the National Cyber and Crypto Agency indicates that in 2023, approximately 70% of public data breaches in Indonesia involved government institutions (Ahdiat, 2024). At the time of writing, SAMAN has not been ISO-certified, thus lacks internationally recognized security standards and its capability against cyberattacks remains debatable. If the system were compromised, not only could sensitive enforcement records fall into unwanted hands, but the integrity of content moderation in Indonesia itself could also be jeopardized. This raises serious concerns about trust in the government's ability to fairly and securely implement SAMAN, when history suggests that user data has not been adequately protected.

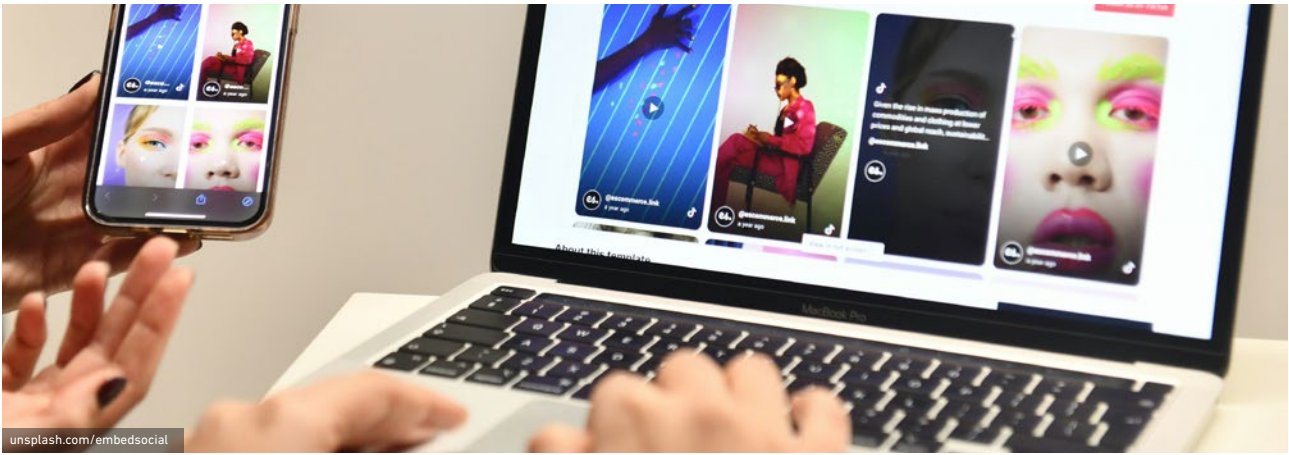


**Figure 2.**  
**Major Cases of Data Leaks in Indonesia between 2020-2024**



Source: compiled from CNBC (2020), Rosana (2021), Firmansyah (2023), ELSAM (2022), Idris (2022), Bestari (2022), and Tan (2024), modified by authors

Another major shortcoming of the SAMAN system is that developers of major platforms, many of whom have extensive experience in building scalable and secure content moderation systems, have stated that they were not consulted during the portal's development process (CIPS FGD, 2025). A co-regulatory approach, with a formalized co-design process between MCDA and digital platforms, as well as independent experts, should be considered to address these gaps and strengthen the legitimacy of SAMAN governance (Setiawan, 2021). Such a partnership will allow the moderation portal to accommodate platform-specific workflows while ensuring traceability, legal safeguards, and redress mechanisms. While SAMAN is still in its pilot phase, integrating experts' and platforms' feedback could help improve its technical efficiency, appeal mechanisms, and alignment with industry best practices, potentially making the system more sustainable over the long term.



## International Practices of Content Governance

Governments worldwide have developed diverse regulatory approaches to balance online freedom of expression, public safety, and platform accountability. Examining international regulatory models and frameworks that specifically address the moderation and/or restriction of online content can provide valuable insights into bridging Indonesia's regulatory gaps. Given the complexities, enforcement of these laws places a substantial burden on regulators to collaborate with digital platforms in developing clear guidelines and codes of practice through co-regulatory dialogues. This proactive approach ensures safer, more inclusive online environments. The subsequent paragraph outlines content governance across different jurisdictions as a reference for regulatory improvements in Indonesia, building on stakeholders' concerns identified in Table 1 above.

Australia provides a clear framework that categorizes harmful and illegal material, reducing legal ambiguity and government overreach under the Online Safety Act 2021. Parts 5 to 8 of the regulation specify key categories, including cyberbullying targeting children, non-consensual intimate images, cyber-abuse against adults, and violent content, with detailed definitions such as those in Section 15 for "intimate images" (Government of Australia, n.d.). Under Part 9, the Act classifies content into Class 1 and Class 2 based on Australian classifications, with Class 1 covering the most extreme material like child abuse and terrorism, and Class 2 involving less severe but still harmful content. Enforcement is centralized with the eSafety Commissioner, who has the authority to act independently, and an appeal process is available through the Administrative Appeals Tribunal. This structure minimizes conflicts across agencies and ensures consistent decisions, supported by interpretative provisions to guide enforcement and prevent vague or subjective interpretations.

The European Union (EU) and France, on the other hand, exemplify transparency and due process in digital services. The EU Digital Services Act (DSA), while subject to concerns about certain provisions<sup>7</sup>, builds upon good practices by requiring user appeals, explanations of content decisions, and standardized transparency reporting (Helberger & Samuelson, 2024). The DSA also establishes a harmonized, EU-wide legal framework for online services in relation to the content they transmit, host, and/or make available to the public. Similarly, France's Avia Law (Law No. 2020-766) mandates accessible reporting and user notifications regarding content removal, along with regular reports on moderation activities (Government of France, 2020). Although struck down by the French Constitutional Council on the grounds that it disproportionately restricted freedom of expression, the due process and transparency sections of the law were upheld.

<sup>7</sup> Peukert (2021) points out several issues, including Articles 12(2) and 15 for unfairly impacting smaller platforms; Articles 26(1)(c) and 27 for vague risk definitions that potentially threaten free speech; Articles 14(6), 15(2)(c), 17(5), and 23(1)(c) for potential over-blocking and implicit support for automated moderation; Articles 30, 35, 37 for indirectly incentivizing platforms to remove "disinformation" and harmful but legal content without clear legal basis; and Articles 31, 32, 38, 47–49 for creating bureaucratic monitoring institutions that could manipulate communication trends while lacking sufficient transparency or accountability.



In terms of operational feasibility and compliance, Japan's Provider Liability Limitation Act (PLLA) takes a notice-and-takedown approach that balances service provider liability with user rights, burdening neither. Rather than holding platforms automatically liable for UGC within their systems, Article 3 of the act provides a conditional safe harbor, as providers become liable only if they know (or should know within reason) of illegal content and fail to act (Ministry of Justice Japan, n.d.). The law outlines conditions under which providers can technically and lawfully remove infringing content, and it sets out a formal notice procedure for affected users. PLLA does not impose strict removal deadlines such as 24 or 48 hours, giving providers flexibility to assess each case appropriately. Additionally, the act does not require proactive monitoring, general filtering, or the appointment of compliance officers, helping providers manage legal risk without incurring excessive administrative or technical burdens.

Lastly, the New Zealand Code of Practice for Online Safety and Harms presents a strong model of a participatory multi-stakeholder system through collaboration to protect the integrity of the digital information ecosystem from abuse. The New Zealand Code established an Oversight Committee that consists of a range of stakeholders, including representatives from the platforms, Maori cultural partners, civil society and other relevant and agreed-upon stakeholders such as government and academics. The Oversight Committee meets at least once a year to review how platforms are meeting their commitments under the Code, including assessing platforms' annual compliance reports, complaints submitted through the Complaints Mechanism, and progress of the Code's implementation (Netsafe and NZTech, 2022).

## The Economic Consequences of Digital Censorship in Indonesia

The increasingly stringent content moderation measures risk stifling Indonesia's digital economy growth, which is predicted to reach USD 360 billion (around IDR 5.8 quadrillion<sup>8</sup>) by 2030 (Google, Temasek & Bain, 2024). Unclear guidelines on permissible content could also lead to arbitrary takedowns and disproportionately affecting independent creators and small businesses, which contribute over 60% of the country's GDP but lack the resources to navigate complex regulatory landscapes (CMEA, 2022). Additionally, the disruption of online services and internet shutdowns can impose severe economic losses. A regulatory climate as such may deter both domestic and foreign investment in the growing tech sector, which are vital for Indonesia's economic growth. The following subsections will explore the potential trade barriers and the costs associated with online disruptions that can undermine Indonesia's growth trajectory.

### Potential trade barriers and a decrease in innovation and investment

Investors seek stability, transparency, and access to reliable information before committing capital to a country. Heavily controlled speech can lead to manipulation of the economic data and obscure market conditions, resulting in an unpredictable business environment that deters investment. A study by the CCIA Research Center and Copia Institute found that strong intermediary liability protections have led to higher investment in innovative companies, while removing these protections depressed investment in targeted startup categories by between 15.2% and 73.4% across the seven jurisdictions studied, including Germany, the US, Australia, China, India, Pakistan, and Indonesia (Masnick, 2023). For example, Germany's 2017 NetzDG law saw venture (late-stage) investment into German social media companies fall from over USD 85 million (IDR 1.36 trillion) in the three years before the law was implemented to just USD 30 million (IDR 480 billion) afterward, while investment in neighboring France and the UK continued to rise during the same period. Research into the issue suggests that NetzDG may have limited the ability of innovative companies and services to grow and succeed (Masnick, 2023).

---

<sup>8</sup> All USD figures in this paper are converted at the exchange rate of USD 1 = IDR 16,000, unless otherwise stated..

### **Box 1.** **The Case of Germany's NetzDG**

Germany passed the Network Enforcement Act (NetzDG) in 2017, a moderation law which includes imposing high fines for social media networks with two million or more registered users. The NetzDG has often been described as both a blueprint and a justification for expanded government control over digital spaces in semi-authoritarian countries, with at least 13 nations having adopted or proposed similar frameworks since 2019 (Mchangama, 2019).

Despite its intentions to combat hate speech and promote online safety, emerging evidence suggests that most content removal requests mandated by NetzDG are ineffective and impose substantial resource burdens for platforms. In 2022, four major social media platforms (YouTube, Facebook, Instagram, and X) received over 2.7 million complaints pursuant to NetzDG, of which 99.8% were either non-violative of NetzDG or duplicative, 84.4% were false positives, and 98.8% of the remaining reports had already been handled under existing platform community guidelines. That same year, users spent (accumulated) an estimated 27 million minutes (about 51.6 years) filing reports<sup>9</sup> that resulted in less than 0.000000215% of content being removed due to NetzDG (Wagener & Cade, 2023). Moreover, compliance with the law required 441 full-time staff across the four major platforms and cost between USD 1,741 and USD 5,116 (IDR 28 million and IDR 82 million) per incremental takedown. The broader economic impact was estimated at USD 22.25 million (IDR 356 billion) annually, or roughly USD 4,336 (IDR 70 million) per takedown (Wagener & Cade, 2023).

The high compliance costs caused by strict takedown enforcement mechanisms disproportionately affect smaller platforms and startups, potentially creating barriers to entry and reinforcing the dominance of incumbent tech companies. This anti-competitive effect is especially concerning to countries that modelled their regulation from NetzDG and are experiencing declining tech investment and startup funding environments. Despite the regulatory pressure, the overall volume of harmful content removed under the NetzDG regime was minimal, with fewer than 2,000 posts taken down per platform every six months, even though these platforms process billions of posts. This suggests that while enforcement burdens are high, the actual impact on content moderation outcomes remains limited.

Inspired by Germany, Indonesia implemented laws similar to those of NetzDG, with stringent intermediary liability frameworks under MR5/2020 and its derivatives. For instance, Articles 15 and 16 of MR5/2020 establish a strict 24-hour deadline for content removal, mirroring Section 3 of NetzDG. Hefty fines and access blocking (Articles 45–46) also echo the sanctions outlined in Section 4 of NetzDG. Both also concentrate enforcement authority under one ministry (Articles 13, 16, and 21 of MR5/2020 versus Section 3 of NetzDG).

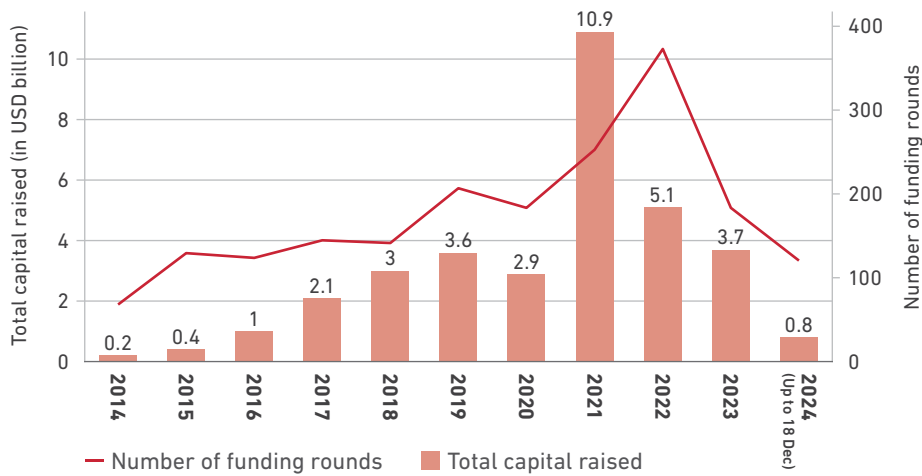
Over time, government-directed content removal increasingly suppresses dissent and politically sensitive speech (Wagener & Cade, 2023; SAFEnet, 2025). MCDA reportedly requested the removal of thousands of contents monthly, as shown in tech companies' transparency reports. Between June and December 2021, MCDA requested Google to delist over 500,000 URLs, but only 0.03% were removed (Google, 2022). X (formerly Twitter) reported nearly 30,000 legal demands for content removal from July to December 2021 (Masnick, 2023). Meanwhile, Meta recorded 149 million content restrictions in Indonesia in the first half of 2024, the highest globally (Meta, 2025). Under the existing content moderation regulations, mass government takedowns could result in millions of USD in fines. If platforms fail to comply, fines may double, triple, or lead to blocking.

---

<sup>9</sup> Conservatively assuming it takes an average of ten minutes to complete each detailed submission form.

The rollout of the SAMAN system adds another layer of content moderation enforcement at a time when Indonesia's startup ecosystem is grappling with a downturn in funding (often known as “tech winter”). The funding figures (Figure 3) indicate a sharp drop in startup funding from USD 10.9 billion (IDR 174 trillion) in 2021 to only USD 800 million (IDR 13 trillion) in 2024 (Yordan, 2024). According to a report by DealStreetAsia, Indonesia recorded only 13 equity funding deals raising a modest USD 60 million (IDR 960 billion) in the final quarter of 2024, the lowest quarterly volume in over six years. This is far below the USD 4.5 billion (IDR 72 trillion) raised across 59 deals in Q4 2021 (DealStreetAsia, 2025). Late-stage funding saw an even steeper decline, plummeting from USD 7.51 billion (IDR 120 trillion) in 2021 to a mere USD 70 million (IDR 1.1 trillion) in 2024, a drop of approximately 99.1% (DealStreetAsia, 2025). Moreover, Indonesia's share of regional startup funding fell to 9.6% in 2024, down from 16.3% in 2023 and 40.3% in 2021 (Meilina, 2025; Abudheen, 2025). Funding levels could decrease further in 2025, especially in light of financial scandals involving high-profile startups, i.e., fintech lending pioneer Investree and aquatech unicorn eFishery.

**Figure 3.**  
**Funding Trend in Indonesia Over the Past Decade**



Source: Yordan (2024), modified by authors

While post-pandemic investor caution, tech winter, macroeconomic headwinds from a shrinking middle class and rising inflation, and the challenge of building sustainable business models have all played a part, Indonesia's regulatory complexity compounds investors' reluctance. Indonesia's attractiveness as a digital investment hub in the region may further decline if regulatory unpredictability persists (US International Trade Administration, 2024). For instance, tech startups may hesitate to launch innovative products or services if they fear regulatory backlash or service shutdown<sup>10</sup>, especially smaller companies with limited resources to comply fully. As a result, even as the global investment climate stabilizes, regulatory barriers could ward off both prospective and existing investors, hindering Indonesia's competitiveness in both tech and innovation.

In mid-2022, the MOCI's temporary blocking of major US-based online services—including PayPal, Steam, Epic Games, and Yahoo—for failing to meet MR5/2020 registration deadlines, sparked public outrage and economic disruption, particularly for freelancers, gamers, and digital small and medium-sized enterprise (SMEs) dependent on these global services (Mulyanto & Galuh, 2022; Antara News, 2022). Such incidents exemplified the regulatory unpredictability that global platforms face in Indonesia. In response, the US government has considered imposing

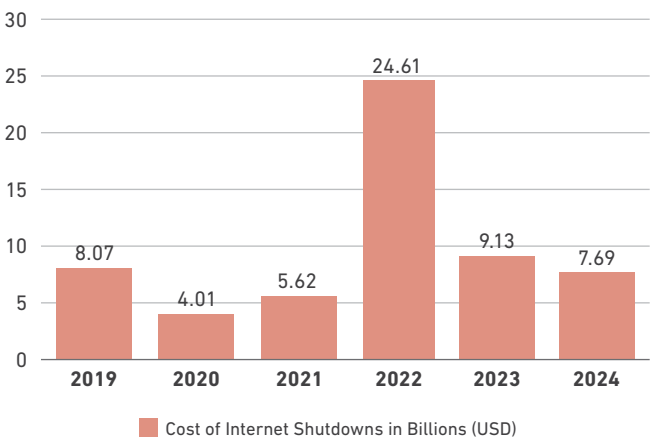
<sup>10</sup> Palagashvili (2021) found that more-regulated industries may have fewer technology startups and potentially “less innovation” in their space because startups are pivoting into other industries or subindustries to avoid complying with industry-specific regulations. In Indonesia, UGC platforms may modify or limit their services to Indonesian users to avoid having to comply with MR5/2020 or other regulations. A case in point is Tumblr, which has been heavily self-censoring for the Indonesian market following its ban due to widespread pornographic content.

tariffs to pressure Indonesia to implement clearer regulatory guidelines that protect foreign businesses, particularly those from the United States. The 2025 National Trade Estimate Report on Foreign Trade Barriers issued by the Office of the US Trade Representative cites Indonesia's content moderation governance as one of the factors influencing the imposition of reciprocal tariffs on Indonesia, possibly reaching effective rates as high as 47% (Kristianus, 2025; USTR, 2025).

### The cost of online disruptions

There has been a rising trend of internet disruptions carried out by governments over the past decade, employing various methods such as complete internet shutdowns<sup>11</sup>, throttling bandwidth<sup>12</sup>, or blocking specific online services<sup>13</sup>. Between 2015 and 2024, 196 local internet disruptions and 60 nationwide internet shutdowns were recorded around the world, mainly triggered by political protests (Statista Research Department, 2024). A study by Howard et al. (2011) revealed that between 1995 and early 2011, there were 606 instances in which 99 different governments deliberately interfered with the normal functioning of the internet. Meanwhile, according to the Shutdown Tracker by Access Now, there were at least 296 documented internet shutdowns globally in 2024, an increase of 76.19% compared to the 168 shutdowns recorded in 2020 (Access Now, 2024). These shutdowns cost the global economy USD 7.69 billion (IDR 123 trillion) in 2024 alone, with governments causing 88,788 hours of disruptions—a 12% increase from 2023 and the highest recorded to date (Figure 4) (Migliano, 2025). This included 49,101 hours of blackouts and 39,687 hours of social media blocks, affecting 648.4 million people (approximately 8.05% of the 2024 global population). Platform X was the most targeted platform with 20,322 hours of disruption, followed by TikTok at 8,115 hours and Signal at 2,880 hours (Table 3) (Migliano, 2025).

**Figure 4.**  
**Annual Cost of Internet Shutdowns Since 2019**



Source: Migliano (2025)

<sup>11</sup> Internet access is completely cut off by the government. This extreme measure cannot be directly circumvented.

<sup>12</sup> Internet speeds have been reduced to 2G, which permits the use of SMS and voice calls only. This is an internet blackout in all but name.

<sup>13</sup> Access to popular digital platforms and social media, such as Facebook, WhatsApp, TikTok or X is blocked. This can typically be circumvented by using a Virtual Private Network (VPN).

**Table 3.**  
**Most Blocked Social Media Platforms Worldwide in 2024**

Social Media Platform	Stakeholder Concerns	Potential Implications
X	20,322	11
TikTok	8,115	8
Signal	2,880	1
Facebook	2,091	8
Instagram	2,010	8
WhatsApp	1,977	5
Telegram	1,824	3
YouTube	1,755	7
Clubhouse	1,092	1

Source: Migliano (2025)

Generally, quantifying the economic impact of internet disruptions is complex due to the difficulty in tracking shutdowns and collecting relevant economic data. However, existing models suggest substantial losses. Using the NetLoss Calculator<sup>14</sup> developed by the Internet Society Pulse, a one-day internet shutdown in Indonesia in 2025 would result in an estimated USD 53 million (IDR 848 billion) GDP loss, while blocking online services for the same period could cost USD 7 million (IDR 112 billion)—including an increase in unemployment of between seven and 52 individuals per day (Internet Society, 2025). Another model of calculation, the Cost of Shutdown Tool<sup>15</sup> (COST), developed by internet monitoring NGO Netblocks, estimates that every hour of an internet blackout costs Indonesia USD 6 million (IDR 96 billion), while blocking major platforms<sup>16</sup> leads to USD 706,000 (IDR 11 billion) in hourly losses per platform (Netblocks, 2025).

Online services sustain a huge chunk of Indonesia's digital economy, contributing over USD 90 billion (IDR 1.4 quadrillion) to the country's GDP—the largest in the region (Google et al., 2024). Disrupting these services would mean severe economic consequences, halting e-commerce, delaying time-sensitive transactions, increasing unemployment, disrupting business-customer interactions, and exposing companies to financial and reputational risks. Between 2016 and 2024, at least 15 internet cutoffs were observed in Indonesia, with 2019 witnessing the highest incidents and the largest economic losses, estimated at around USD 187.7 million (IDR 3 trillion) (Woodhams & Migliano, 2020; Access Now, 2024). The most severe internet blackouts have been confined to the Papua region, which has long been a conflict area.

Throughout 2019, coinciding with the election year, the Indonesian government employed a combination of total shutdown, internet throttling, and service blocking in the country. The official justification was to curb fake news, hate speech, and content promoting violence, followed by "precautionary measures" for public safety and national security (Antony, 2019; Kumparan, 2020). Such extreme measures affected numerous cities, severely limited access to information, and disrupted business activities, including that of fintech companies and SMEs, which relied heavily on internet connectivity (Juniarto, 2020; Burhan, 2020).

<sup>14</sup> See the full methodology here: [https://pulse.internetsociety.org/wp-content/uploads/2023/06/Methodology\\_Internet-Society-Pulse-NetLoss-Calculator\\_June-2023.pdf](https://pulse.internetsociety.org/wp-content/uploads/2023/06/Methodology_Internet-Society-Pulse-NetLoss-Calculator_June-2023.pdf)

<sup>15</sup> Access COST tool here: <https://netblocks.org/projects/cost>

<sup>16</sup> WhatsApp, X, Facebook, YouTube, and Instagram.



The 2019 Papua internet shutdown, which lasted from August 21 to September 4, was ruled unlawful by the Jakarta State Administrative Court, citing that the government failed to provide sufficient justification for such extreme measures (Global Freedom of Expression, 2020). The shutdown affected social media providers, over-the-top communications services, and internet search providers. Google alone lost an estimated USD 13,000 (IDR 208 million) per day in advertising revenue, while 1.46 million Papuan users were cut off from online access (ITC, 2022). Internet services were again shut down in West Papua's capital, Jayapura, in May 2021 amid a military operation. Frequent restrictions on connectivity in Papua have hindered small businesses and individuals' ability to engage in economic activities.

As previously discussed, MOCI's decision in mid-2022 to block access to major global platforms that failed to comply with the MR5/2020 regulation has sparked public backlash. In November 2022, the Jakarta Legal Aid Institute (LBH Jakarta) and Digital Freedom Advocacy sued MCDA in the Jakarta State Administrative Court over enforcement of the law, claiming that it harmed users and relied on an "overly broad" legal interpretation. LBH Jakarta compiled 213 complaints from workers who were affected during the blockade, and 47 of them suffered losses of IDR 1.5 billion (approximately USD 97,000<sup>17</sup>) because they could not access PayPal's financial applications (AJI, 2022).

The government's stronger grip raised concerns over digital rights, regulatory overreach, and the negative economic impacts on Indonesia's digital ecosystem. Economists in Indonesia warn that frequent internet disruptions foster an unstable environment that discourages investment, particularly among those looking to develop digital technologies (Burhan, 2020). Restrictions are usually carried out solely at the government's behest, in which security agencies work with national communications regulators, citing national political security reasons and public order considerations (CIPESA, 2017). However, the United Nations (UN) has declared these actions constitute a violation of political civil rights. The UN has called upon nations to refrain from shutting down internet networks, including during political unrest (OHCHR, 2022). According to a 2024 report from Freedom House, Indonesia is categorized as "partly free," with a declining internet freedom score<sup>18</sup> to 49, from 56 out of 100 in 2016 (Freedom House, 2024). The People Power Under Attack report published in December 2024 further notes that Indonesia's civic space remains rated as "obstructed" with a score of 44 out of 100. Among the main concerns are the use of restrictive laws, including defamation provisions against human rights defenders and journalists (CIVICUS Monitor, 2024).

---

<sup>17</sup> Based on the November 2022 exchange rate.

<sup>18</sup> Scores are based on a scale of 0 (least free) to 100 (most free). They assign three ratings on internet freedom: (1) Scores 100-70 = Free, (2) scores 69-40 = Partly Free, (3) Scores 39-0 = Not Free.

# Conclusion and Policy Recommendations

Indonesia's content moderation framework remains a work in progress, often criticized for its lack of transparency, inconsistent enforcement, and broad legal definitions that risk overreach and censorship if applied indiscriminately. As digital adoption accelerates across the archipelago, online platforms have become indispensable for businesses and millions of Indonesians. The estimates presented in this brief, along with publicly available evidence, suggest that disruptions to online ecosystems—internet shutdowns and service blockages—can have severe economic consequences with far-reaching costs for the nation's economy and people's fundamental rights. If disruptions become more frequent and prolonged, the impacts will likely be magnified, jeopardizing Indonesia's digital growth and economic resilience.

In light of these concerns, this brief examines the potential unintended consequences of platform regulations that have been rarely explored before. The findings firmly highlight that when governments restrict online speech and limit access to information, they risk initiating a self-perpetuating cycle of economic decline. This cycle includes diminished innovation, reduced investment, shrinking job opportunities, and ultimately lower living standards. The government thus should exercise greater caution and transparency in regulating political speech, understanding that attempting to control citizens' political views is both impractical and a breach of their rights. To address these challenges, Indonesian policymakers should adopt a more balanced, transparent, and nuanced approach. Key recommendations to consider include:

- **Shift from restrictive, censorship-driven content governance to a user-centric, rights-based approach.** The current framework under the MR5/2020 and Decree 522/2024 prioritizes reactive and restrictive measures that risk overreach and censorship while failing to adequately protect users, particularly children<sup>19</sup>. A user-centric, human rights approach would prioritize user protection, including guaranteeing their right to appeal any removal or blocking decisions through courts or impartial tribunal proceedings. It would also ensure that regulatory interventions safeguard digital rights, data privacy, and consumer interests. Equally important, MCDA should grant legal immunity to ESOs that have complied with MR5/2020. Specifically, the clause "may be exempted from legal liabilities" in Article 11 should be revised to "will be exempted from legal liabilities" for ESOs, including digital platforms, who have fulfilled their obligations.
- **Provide clear content definitions, be unambiguous, transparent, and follow due process.** To avoid over-criminalization, MCDA should either revoke Article 9(b) of MR5/2020 or, at minimum, establish narrowly defined categories of illegal content, focusing on truly unlawful material (e.g., child sexual abuse material (CSAM), explicit incitement to violence, and other prioritized takedowns). Harmonizing national laws and regulations related to illegal and harmful content will minimize the possibility of multiple interpretations and regulatory overlaps. Internationally recognized standards should<sup>20</sup> serve as benchmarks. Enforcement mechanisms must also be standardized, ensuring proportionality, due process, and transparency in content takedown procedures. In addition, the establishment of a dedicated personal data protection (PDP) authority is also critical in exercising better due process. A regulatory framework with well-defined criteria, clear moderation guidelines, and an independent PDP authority operating with a strong mandate will foster a more accountable, rights-respecting digital governance system in Indonesia.

<sup>19</sup> The Indonesian government has recently enacted GR 17/2025 or the PP TUNAS, establishing online child safety measures that mandates private ESOs to conduct stricter protections for minors in the digital space. The regulation also mandates age verification measures and outlines sanctions for ESOs that fail to comply. While it is a welcome move by regulators—particularly in enforcing risk assessments and banning exploitative practices—its effectiveness remains to be seen.

<sup>20</sup> Such as the three-part test of legality-necessity-proportionality outlined in the ICCPR Article 19, the six-part threshold test based on the Rabat Plan of Action, or the Manila Principles on Intermediary Liability (Office of the United Nations High Commissioner for Human Rights, 1966; UNHRC, 2012; Electronic Frontier Foundation and Partners, 2015).

- Fine-tune data security, improve procedural fairness, and streamline institutional clarity of the SAMAN.** In terms of data security, SAMAN needs to adopt internationally recognized security standards (i.e. ISO 27001 certification), clarify data sharing protocols, and ensure the integrity of enforcement records to better prevent data breaches and system failures. The framework should also allow platforms to contest takedown orders before compliance is mandated, supported by an independent review panel to ensure fairness and due process. Equally important, MCDA must serve as the sole regulator of content moderation to eliminate conflicting and overlapping enforcement by police and other agencies. These measures will elevate SAMAN into a more accountable, efficient, and legally sound framework for content moderation.
- Implement a meaningful co-governance approach.** As online content continues to evolve, a co-governance model that engages policymakers, digital platforms, industry associations, civil society, academia, and independent experts throughout the policy development process should be adopted. As exemplified by New Zealand's Oversight Committee on Online Safety and Harms, the Indonesian government—led by MCDA—should establish a formalized multi-stakeholder policy advisory forum to provide ongoing input on policy formulation, enforcement, and evaluation. Such a co-governance model can help develop voluntary content standards<sup>21</sup> and localize terms of service and community guidelines, reflecting Indonesia's unique socio-political and cultural context. It can also contribute to the development and improvement of the SAMAN system and reinforce institutional safeguards. Ultimately, it will aim to ensure that open internet principles, as well as international human rights principles, best practices, and standards, are taken into account when regulating online space. This participatory framework will improve legitimacy, transparency, and enforceability, as well as provide an extra check against any potential abuse of power.
- Enforce transparency report and public oversight.** To foster public-private trust and accountability in content moderation, both MCDA and platforms should publish regular transparency reports detailing content takedowns and moderation decisions as well as the rationale behind them. This should include data on government-issued content removal orders, the number of appeals, and final resolutions, enabling scrutiny by civil society and the public. Under the current MR5/2020 regime, transparency reporting is not required by either the MCDA or ESOs (digital platforms). By institutionalizing clear and periodic reporting, MCDA can enhance public awareness and reinforce trust between the government, platforms, and users, which ultimately strengthens Indonesia's digital governance ecosystem.

<sup>21</sup> Such as guidelines to curb election misinformation, empower users to make informed choices, and set online safety standards for children.

# References

---

- Abudheen, S. (2025, January). *The Great Decline: How Indonesia's Tech Funding Hit a 3-year low*. e27. <https://e27.co/the-great-decline-how-indonesias-tech-funding-hit-a-3-year-low-20250123/>
- Access Now. (2024). *Shutdown Tracker Optimization Project (STOP) Dashboard v.1*. Access Now. <https://www.accessnow.org/keepiton-data-dashboard/>
- Ahdiat, A. (2024, June). *Kebocoran Data RI Terbanyak dari Sektor Pemerintahan*. Databoks Katadata Media Network. <https://databoks.katadata.co.id/teknologi-telekomunikasi/statistik/f2b65112cfdccc4/kebocoran-data-ri-terbanyak-dari-sektor-pemerintahan>
- Aliansi Jurnalis Independen [AJI]. (2022, December 20). *Indonesia's Ministry of Communications sued after blocking 8 digital platforms*. Aliansi Jurnalis Independen. <https://aji.or.id/informasi/indonesias-ministry-communications-sued-after-blocking-8-digital-platforms>
- Antara News. (2022, June). *Kominfo minta platform digital segera mendaftar*. Antara News. <https://www.antaranews.com/berita/2953833/kominfo-minta-platform-digital-segera-mendaftar>
- Antony, N. D. (2019, August). *Pemblokiran Internet di Papua Diprotes, Jokowi: Untuk Kebaikan Bersama*. Detik News. <https://news.detik.com/berita/d-4676953/pemblokiran-internet-di-papua-diprote-jokowi-untuk-kebaikan-bersama>
- Asosiasi Penyelenggara Jasa Internet Indonesia [APJII]. (2024, February). *APJII Jumlah Pengguna Internet Indonesia Tembus 221 Juta Orang*. APJII. <https://apjii.or.id/berita/d/apjii-jumlah-pengguna-internet-indonesia-tembus-221-juta-orang>
- Bestari, N. P. (2022, August). *Setelah PLN, 26 Juta Data Indihome Bocor & Disebar Hacker*. CNBC Indonesia. <https://www.cnbcindonesia.com/tech/20220822062837-37-365431/setelah-pln-26-juta-data-indihome-bocor-disebar-hacker>
- Burhan, F. A. (2020, June). *Kerugian Blokir Internet Capai Triliunan Rupiah*. Katadata. <https://katadata.co.id/digital/teknologi/5edf9beb3c0a8/kerugian-blokir-internet-capai-triliunan-rupiah>
- Center for Indonesian Policy Studies [CIPS]. (2025, February). *Moderasi Konten dan Kebebasan Berekspresi di Ruang Digital, Laporan FGD Bersama Koalisi Masyarakat Sipil*. CIPS.
- \_\_\_\_\_. (2025, February). *Moderasi Konten dan Kebebasan Berekspresi di Ruang Digital, Laporan FGD Bersama Platform dan Industri*. CIPS.
- Chariris, M. (2019, January). *Kejahatan Online Marak, Polisi Take Down Akun Bodong*. Jawa Pos Radar Mojokerto. <https://radarmojokerto.jawapos.com/hukum-kriminal/82995244/kejahatan-online-marak-polisi-take-down-akun-bodong>
- CIVICUS Monitor. (2024). *People Power Under Attack 2024*. CIVICUS Monitor. [https://cipesa.org/wp-content/files/reports/Full-Report\\_Calculating-the-Economic-Impact-of-Internet-Disruptions-in-Sub-Saharan-Africa\\_September-29.pdf](https://cipesa.org/wp-content/files/reports/Full-Report_Calculating-the-Economic-Impact-of-Internet-Disruptions-in-Sub-Saharan-Africa_September-29.pdf)
- CNBC. (2020, May). *Ini Kronologi Tersebar nya Jutaan Data KPU yang Bocor*. CNBC Indonesia. <https://www.cnbcindonesia.com/tech/20200522141735-37-160286/ini-kronologi-tersebar-nya-jutaan-data-kpu-yang-bocor>
- Collaboration on International ICT Policy for East and Southern Africa [CIPESA]. (2017). *A Framework for Calculating the Economic Impact of Internet Disruptions in Sub-Saharan Africa*. CIPESA. [https://cipesa.org/wp-content/files/reports/Full-Report\\_Calculating-the-Economic-Impact-of-Internet-Disruptions-in-Sub-Saharan-Africa\\_September-29.pdf](https://cipesa.org/wp-content/files/reports/Full-Report_Calculating-the-Economic-Impact-of-Internet-Disruptions-in-Sub-Saharan-Africa_September-29.pdf)
- Coordinating Ministry for Economic Affairs Republic of Indonesia [CMEA]. (2022, March). *Press Release HM.4.6/178/SET.M.EKON.3/3/2022 - Coordinating Minister Airlangga: Government Continues to Encourage Strengthening Economic Foundations by Establishing Digital Transformation of MSMEs as One of the Priorities*. Kementerian Koordinator Bidang Perekonomian Republik Indonesia. <https://ekon.go.id/publikasi/detail/4065/coordinating-minister-airlangga-government-continues-to-encourage-strengthening-economic-foundations-by-establishing-digital-transformation-of-msmes-as-one-of-the-priorities>
- DealStreetAsia. (2025, January). *Mapping SEA and Indonesia's 2024 Journey*. DealStreetAsia. <https://www.dealstreetasia.com/reports/se-asia-deal-review-fy-2024>
- Electronic Frontier Foundation [EFF] and Partners. (2015, May). *The Manila Principles on Intermediary Liability*. Manila Principles. [https://www.eff.org/files/2015/07/08/manila\\_principles\\_background\\_paper.pdf](https://www.eff.org/files/2015/07/08/manila_principles_background_paper.pdf)
- Firmansyah, M. J. (2023, July). *Dirjen Imigrasi Silmy Karim Bilang Kebocoran Data Paspor Terjadi pada Januari 2022*. Tempo. <https://www.tempo.co/hukum/dirjen-imigrasi-silmy-karim-bilang-kebocoran-data-paspor-terjadi-pada-januari-2022-165764>
- Freedom House. (2024). *Freedom on the Net 2024 | Indonesia*. Freedom House. <https://freedomhouse.org/country/indonesia/freedom-net/2024>
- Ginta, Y. V. S., & Arief, T. M. V. (2023, December). *Polisi Bakal "Take Down" Konten Negatif Saat Natal dan Tahun Baru di Bali*. Kompas. <https://regional.kompas.com/read/2023/12/23/194310278/polisi-bakal-take-down-konten-negatif-saat-natal-dan-tahun-baru-di-bali>
- Global Freedom of Expression. (2020, June). *Expands Expression Case Analysis*. Global Freedom of Expression. <https://globalfreedomofexpression.columbia.edu/cases/alliance-of-independent-journalists-v-minister-of-communication/>

- Google. (2022). Google Transparency Report: Government Request to remove Content. Google Transparency Report. [https://transparencyreport.google.com/government-removals/government-requests/ID?hl=en&country\\_request\\_explore=period:2021H2;authority:ID&lu=country\\_request\\_explore&country\\_request\\_amount=group\\_by:requestors;period;;authority:ID](https://transparencyreport.google.com/government-removals/government-requests/ID?hl=en&country_request_explore=period:2021H2;authority:ID&lu=country_request_explore&country_request_amount=group_by:requestors;period;;authority:ID)
- Google, Temasek, & Bain & Company. (2024). e-Conomy SEA 2024: Report Highlights. Google e-Conomy SEA. <https://economysea.withgoogle.com/report/>
- Government of Australia. (n.d.). Current legislation | Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts. Department of Infrastructure, Transport, Regional Development and Communications. <https://www.infrastructure.gov.au/media-technology-communications/internet/online-safety/current-legislation>
- Government of France. (2020, June). LAW No. 2020-766 of June 24, 2020 aimed at combating hateful content on the internet (1). Légifrance. <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031970>
- Helberger, N. & Samuelson, P. (2024, March). The Digital Services Act as a Global Transparency Regime. Verfassungsblog. <https://verfassungsblog.de/the-digital-services-act-as-a-global-transparency-regime/>
- Howard, P. N., Agarwal, S. D., & Hussain, M. M. (2011). The Dictators' Digital Dilemma: When Do States Disconnect Their Digital Networks? *Issues in Technology Innovation*, (13), 1-11. [https://www.brookings.edu/wp-content/uploads/2016/06/10\\_dictators\\_digital\\_network.pdf](https://www.brookings.edu/wp-content/uploads/2016/06/10_dictators_digital_network.pdf)
- Idris, M. (2022, August). *PLN Klarifikasi Dugaan 17 Juta Data Pribadi Pelanggan Bocor dan Dijual*. Kompas.com. <https://money.kompas.com/read/2022/08/20/101218826/pln-klarifikasi-dugaan-17-juta-data-pribadi-pelanggan-bocor-dan-dijual>
- Internet Society. (2025). *Netloss Calculator*. Internet Society Pulse. [https://pulse.internetsociety.org/en/netloss/?country\\_code=ID&start\\_date=2025-01-01&end\\_date=2025-01-02&shutdown\\_type=shutdown](https://pulse.internetsociety.org/en/netloss/?country_code=ID&start_date=2025-01-01&end_date=2025-01-02&shutdown_type=shutdown)
- Juniarto, D. (2020). *Internet Shutdown in Indonesia: The New Normal Policy to Censor Information Online? SAFENet*. <https://safenet.or.id/2020/10/internet-shutdown-in-indonesia-the-new-normal-policy-to-censor-information-online/>
- Kemp, S. (2025, February). *Digital 2025: Global Overview Report — DataReportal — Global Digital Insights*. DataReportal. <https://datareportal.com/reports/digital-2025-global-overview-report>
- Kristianus, A. (2025, April). *Indonesia Prepares Economic Stimulus to Counter US Tariffs, Protect Local Jobs*. Jakarta Globe. <https://jakartaglobe.id/business/indonesia-prepares-economic-stimulus-to-counter-us-tariffs-protect-local-jobs>
- Kumparan. (2020, January). *Indonesia Blokir Internet 338 Jam dan Medsos 78 Jam Selama 2019*. Kumparan Tech. <https://kumparan.com/kumparantech/indonesia-blokir-internet-338-jam-dan-medsos-78-jam-selama-2019-1scXn1qXfNf>
- Lembaga Studi & Advokasi Masyarakat [ELSAM]. (2022, January). *New Year, New Data Breach: Kebocoran Data Kesehatan Terjadi Kembali, Bukti RUU PDP Penting Segera Disahkan*. ELSAM Lembaga Studi & Advokasi Masyarakat. <https://www.elsam.or.id/siaran-pers/new-year-new-data-breach-kebocoran-data-kesehatan-terjadi-kembali-bukti-ruu-pdp-penting-segera-disahkan>
- Maluku Regional Police. (2024, September). *Amankan Pilkada, Polda Maluku Patroli Cyber, Takedown Konten Ujaran Kebencian di medsos*. Tribrata News Polda Maluku. <https://tribratanews.maluku.polri.go.id/informasi/berita/baca/amankan-pilkada-polda-maluku-patroli-cyber-takedown-konten-ujaran-kebencian-di-medsos>
- Masnick, M. (2023, April). *The Unintended Consequences of Internet Regulation*. Computer & Communications Industry Association. <https://ccianet.org/research/reports/unintended-consequences-of-internet-regulation/>
- Mastur. (2016). Implementasi Undang-undang Nomor 11 Tahun 2008 tentang Informasi dan Transaksi Elektronik Sebagai Tindak Pidana Non Konvensional. *Kosmik Hukum*, 16(2). <https://doi.org/10.30595/kosmikhukum.v16i2.1995>
- Mchangama, J. (2019, November). *The Digital Berlin Wall: How Germany (Accidentally) Created a Prototype for Global Online Censorship*. Justitia. <https://justitia-int.org/en/the-digital-berlin-wall-how-germany-created-a-prototype-for-global-online-censorship/#:~:text=According%20to%20Freedom%20House%27s%20Freedom,co%2Dauthor%20of%20the%20report>
- Ministry of Justice Japan. (n.d.). *Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Sender*. Japanese Law Translation. <https://www.japaneselawtranslation.go.jp/en/laws/view/3610/en>
- Meilina, K. (2025, Maret). *Investasi ke Startup Indonesia Anjlok Terdalam Se-ASEAN, Tak ada Unicorn 2024*. Katadata. <https://katadata.co.id/digital/startup/67dd1b7354af6/investasi-ke-startup-indonesia-anjlok-terdalam-se-asean-tak-ada-unicorn-2024>
- Meta. (2025). *Content Restrictions Based on Local Law*. Meta Transparency Center. <https://transparency.meta.com/reports/content-restrictions/>
- Migliano, S. (2025, January). *Government Internet Shutdowns Cost \$7.69 Billion in 2024*. Top 10 VPN. <https://www.top10vpn.com/research/cost-of-internet-shutdowns/>
- Mulyanto, R., & Galuh, L. (2022, August). *Indonesia's PayPal, Yahoo bans cast cloud over tech hub dream*. Aljazeera. <https://www.aljazeera.com/economy/2022/8/4/indonesias-paypal-ban-casts-cloud-over-tech-hub-dreams>
- Netblocks. (2025). *The NetBlocks Cost of Shutdown Tool*. Netblocks. <https://netblocks.org/cost/>



Netsafe and NZTech. (2022, July). *Aotearoa New Zealand Code of Practice for Online Safety and Harms*. The Code. <https://thecode.org.nz/wp-content/uploads/sites/38/2023/06/THE-CODE-DOCUMENT-FINAL.pdf>

Octavia, S., & Setuningsih, N. (2025, February). *Polri akan Surati E-commerce untuk "Takedown" Penjualan Barang Elektronik Illegal*. Kompas. <https://nasional.kompas.com/read/2025/02/04/17202491/polri-akan-surati-e-commerce-untuk-takedown-penjualan-barang-elektronik>

Office of the United Nations High Commissioner for Human Rights [OHCHR]. (2022, June). *Internet shutdowns: UN report details 'dramatic' impact on people's lives and human rights*. OHCHR. <https://www.ohchr.org/en/press-releases/2022/06/internet-shutdowns-un-report-details-dramatic-impact-peoples-lives-and-human>

Palagashvili, L. (2021). Exploring How Regulations Shape Technology Startups. *Mercatus Research Series*. <http://dx.doi.org/10.2139/ssrn.3868272>

Peukert, A. (2021, August). *Five Reasons to be Skeptical About the DSA*. Verfassungsblog. <https://verfassungsblog.de/power-dsa-dma-04/>

Rosana, F. C. (2021, July). *Kebocoran Data Nasabah BRI Life Bukti Lemahnya Proteksi dan Regulasi*. Tempo. <https://www.tempo.co/arsip/kebocoran-data-nasabah-bri-life-bukti-lemahnya-proteksi-dan-regulasi-489587>

SAFEnet. (2021, February). *Permenkominfo 5/2020: Peraturan Moderasi Daring yang Diterapkan di Indonesia Mungkin Yang Paling Represif di Dunia*. SAFEnet. <https://safenet.or.id/id/2021/02/pm-kominfo-5-2020-peraturan-moderasi-daring-yang-diterapkan-di-indonesia-mungkin-yang-paling-represif-di-dunia/>

\_\_\_\_\_. (2025, February). *Indonesia's Digital Rights Situation Report 2024 Shows the Legacy of Repression on the Internet*. SAFEnet. <https://safenet.or.id/2025/03/indonesias-digital-rights-situation-report-2024-shows-the-legacy-of-repression-on-the-internet/>

Setiawan, I. (2021). *Who is Responsible for User-Generated Content on Digital Platforms in Indonesia*. CIPS Policy Brief No. 8. [https://c95e5d29-0df6-4d6f-8801-1d6926c32107.usrfiles.com/ugd/c95e5d\\_abe0d7a0df384fca93611645c71bd109.pdf](https://c95e5d29-0df6-4d6f-8801-1d6926c32107.usrfiles.com/ugd/c95e5d_abe0d7a0df384fca93611645c71bd109.pdf)

Statista Research Department. (2024, October). *Number of internet connection disruption cases worldwide from 2015 to 2024, by type and reason*. Statista. <https://www.statista.com/statistics/1412147/number-of-internet-shutdowns-worldwide-by-type-and-reason/>

Tan, A. (2024, June). *Pusat Data Nasional Jebol: Menkominfo Mundur atau Dimaklumi?* Kompas. <https://nasional.kompas.com/read/2024/06/28/08212831/pusat-data-nasional-jebol-menkominfo-mundur-atau-dimaklumi?page=all>

Twimbit. (2024). *Navigating 2030: AI and the Attention Economy in Indonesia*. Twimbit. <https://cdn.twimbit.com/uploads/2024/03/06073340/Navigating-2030-AI-and-Attention-Economy-Indonesia.pdf>

United Nations Human Rights Council [UNHRC]. (2012, October). *The Rabat Plan of Action | OHCHR*. ohchr. <https://www.ohchr.org/en/documents/outcome-documents/rabat-plan-action>

UNHRC General Assembly Resolution 2200A (XXI). (1966, December). *International Covenant on Civil and Political Rights*. ohchr. <https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights>

United States International Trade Administration [ITA]. (2024, September). *Indonesia Digital Economy*. ITA. <https://www.trade.gov/country-commercial-guides/indonesia-digital-economy>

United States International Trade Commission [ITC]. (2022). *Foreign Censorship, Part 2: Trade and Economic Effects on U.S. Businesses*. United States International Trade Commission. <https://www.usitc.gov/publications/332/pub5334.pdf>

United States Trade Representative [USTR]. (2025). *2025 National Trade Estimate Report on Foreign Trade Barriers*. USTR. <https://ustr.gov/sites/default/files/files/Press/Reports/2025NTE.pdf>

Wagener, T., & Cade, K. (2023, April). *Greater Internet Regulations – like NetzDG – Hurt Investment, Innovation, and Free Speech*. DisCo | Disruptive Competition Project. <https://project-disco.org/competition/greater-internet-regs-hurt-investment-innovation-free-speech/>

Woodhams, S. & Migliano, S. (2020, January). *Government Internet Shutdowns Cost \$8 Billion in 2019*. Top 10 VPN. <https://www.top10vpn.com/research/cost-of-internet-shutdowns/2019/>

Yordan, J. (2024, December). *Should Indonesian Startups Brace for a Stormy 2025?* Tech in Asia. <https://www.techinasia.com/should-indonesian-startups-brace-for-a-stormy-2025>

# Annexes

---

## Annex I. SAMAN Technical Process

After a government institution flags content deemed harmful, a report is submitted to MCDA through SAMAN to be reviewed. Depending on the validity of the report, the report could be sent back for further clarification or processed. SAMAN then automatically notifies the offending platform with the reported content, and the platform complies by taking the content down within a given time frame. The MCDA will send warning letters (i) every 4 hours for urgent access termination requests concerning child pornography, terrorism, and public order disturbances; and (ii) every 24 hours for non-urgent access termination requests of any kind. The maximum number of warning letters given is three times.

Platforms are incentivized to comply through a series of administrative and financial penalties. Failure to comply or pay these fines will lead to a full suspension of platform access until the issue is resolved. Decree No. 522/2024 utilizes a progressive sanction in which the violation points are multiplied by the administrative fine rate of IDR 100,000 (approximately USD 6) per point. Violation points follow a formula with multiple weighted indexes multiplied by the maximum amount of 5000 points. The formula is as follows:

$$\text{Administrative fine} = (\text{Content Category} \times \text{UGC} \times \text{Business Scale} \times \text{Warning} \times \text{Compliance} \times \text{Virality} \times 5000) \times \text{IDR } 100,000$$

- Content Category Index based on severity of flagged content, weighted between 0.25 to 1 accordingly.
- User Generated Content Index based on average number of daily users, weighted between 0.2 to 1 accordingly.
- Business Scale Index based on annual net profit, weighted between 0.25 to 1 accordingly.
- Warning Index based on the 3 warnings given multiplied by time frame according to urgency of the takedown, weighted between 0 to 1 accordingly.
- Compliance Index based on the platform's compliance success rate in the previous year, weighted between 0.25 to 1 accordingly.
- Virality Index based on views and downloads of the flagged content.

Platforms are also given the opportunity to lodge an appeal against the takedown order following the second warning letter, given that they have taken down the flagged content and submitted a binding payment commitment letter, or following the third and final warning letter without the aforementioned requirements. The appeal is directed towards the Minister in the case of content flagged for pornography or gambling, or with a copy to the government institution that flagged the content in other cases. The Minister then has 10 days to respond by either accepting or rejecting the appeal. If accepted, the content could then remain on the platform, or restored if already taken down. Otherwise, the platform must comply with the takedown request on top of the administrative fines, or risk having their access terminated by the MCDA.

## ABOUT THE AUTHORS

**Muhammad Nidhal** is a Research and Policy Analyst at CIPS. He holds a Bachelor's degree in International Relations from Jayabaya University in Jakarta with a minor in Postcolonial Studies. Prior to joining CIPS, he worked at the Embassy of Uzbekistan in Jakarta as an assistant to the Political and Economic Section. He first joined the CIPS Emerging Policy Leaders Program in 2022.

**Rasya Athalla Aaron** is a Research and Policy Associate at CIPS. He graduated with a Bachelor of International Relations from Parahyangan Catholic University (UNPAR) in 2023. Before joining CIPS as a Research and Policy Associate, he interned at CIPS on the research team and for the Badan Riset dan Inovasi Nasional's Deputy for Research and Innovation Infrastructure, worked freelance in the entertainment industry, volunteered for the Indonesian Deaf Basketball community, and actively served in his university's student executive body.

**Muchammad Aldrich Alfarisi** graduated with a Bachelor's degree in International Relations (IR) from the University of Indonesia (UI) in 2024. Before graduating, he participated as a visiting international student at Victoria University of Wellington in New Zealand through the IISMA Program, administered by Indonesia's Ministry of Education and Culture. Prior to interning at CIPS' research team from January to March 2025, he volunteered as a teaching assistant for the Modern Diplomacy and International Institution courses at IR UI.

Our work relies on your support.

To support CIPS, visit [www.cips-indonesia.org/donate](http://www.cips-indonesia.org/donate).



# Explore other policy briefs published by the Center for Indonesian Policy Studies



Impact of Trade Policies on the MSMEs' Competitiveness in Indonesia: The Case of E-commerce Import Restrictions



Indonesia's Strategies for Joining the ASEAN Digital Economy Framework Agreement



Establishing Foreign Higher Education Institutions in Indonesia



Digital Taxation in Indonesia



Cybersecurity Protection in Indonesia



Who is Responsible for User-Generated Content on Digital Platforms in Indonesia?



Data Privacy in the Indonesian Personal Data Protection Legislation



RCEP: The Opportunity for Indonesia and Steps of Its Implementation, An Insider's Perspective



Attracting FDI Post Covid-19 by Simplifying Indonesia's Regulatory Framework

Go to our website to access more titles:

[www.cips-indonesia.org/publications](http://www.cips-indonesia.org/publications)



**CIPS**

Center for Indonesian  
Policy Studies

#### **ABOUT THE CENTER FOR INDONESIAN POLICY STUDIES**

**Center for Indonesian Policy Studies (CIPS)** is a strictly non-partisan and non-profit think tank providing policy analysis and practical policy recommendations to decision-makers within Indonesia's legislative and executive branches of government.

CIPS promotes social and economic reforms that are based on the belief that only civil, political, and economic freedom allows Indonesia to prosper. We are financially supported by donors and philanthropists who appreciate the independence of our analysis.

#### **KEY FOCUS AREAS:**

**Sustainable Food Systems and Agriculture:** CIPS engages in research on the sustainable growth and modernization of Indonesia's agriculture. CIPS also researches and advocates for policy alternatives that open up trade in strategic food items in order to stabilize food prices and achieve greater food security for Indonesians. We expose links between agriculture, trade and investment, food prices, and a nutritious diet of Indonesian consumers with the aim of ensuring that low-income families can access affordable quality food.

**Quality Education:** CIPS conducts research and advocacy on education policy in Indonesia to improve education accessibility and quality. We focus on how private initiatives, greater school autonomy, and appropriate skills among students and teachers alike can build a resilient education system in Indonesia, facilitate the improvement of education quality and increase education choices for low-income Indonesians.

**Open and Competitive Business Environment:** CIPS believes that greater economic freedom and open markets generate economic opportunities for Indonesians to access and earn decent livelihoods. Whether through trade and investment, digital technologies, entrepreneurship, property rights, or employment opportunities, CIPS advocates for policy reforms that enable Indonesians of all backgrounds to seek greater prosperity for themselves and their communities.

[www.cips-indonesia.org](http://www.cips-indonesia.org)

 [facebook.com/cips.indonesia](https://facebook.com/cips.indonesia)

 [@cips\\_id](https://twitter.com/cips_id)

 [@cips\\_id](https://www.instagram.com/cips_id)

 [Center for Indonesian Policy Studies](https://www.linkedin.com/company/cips-indonesia)

 [CIPS Learning Hub](https://www.youtube.com/cips_id)

Jalan Terogong Raya No. 6B  
Cilandak, Jakarta Selatan 12430  
Indonesia