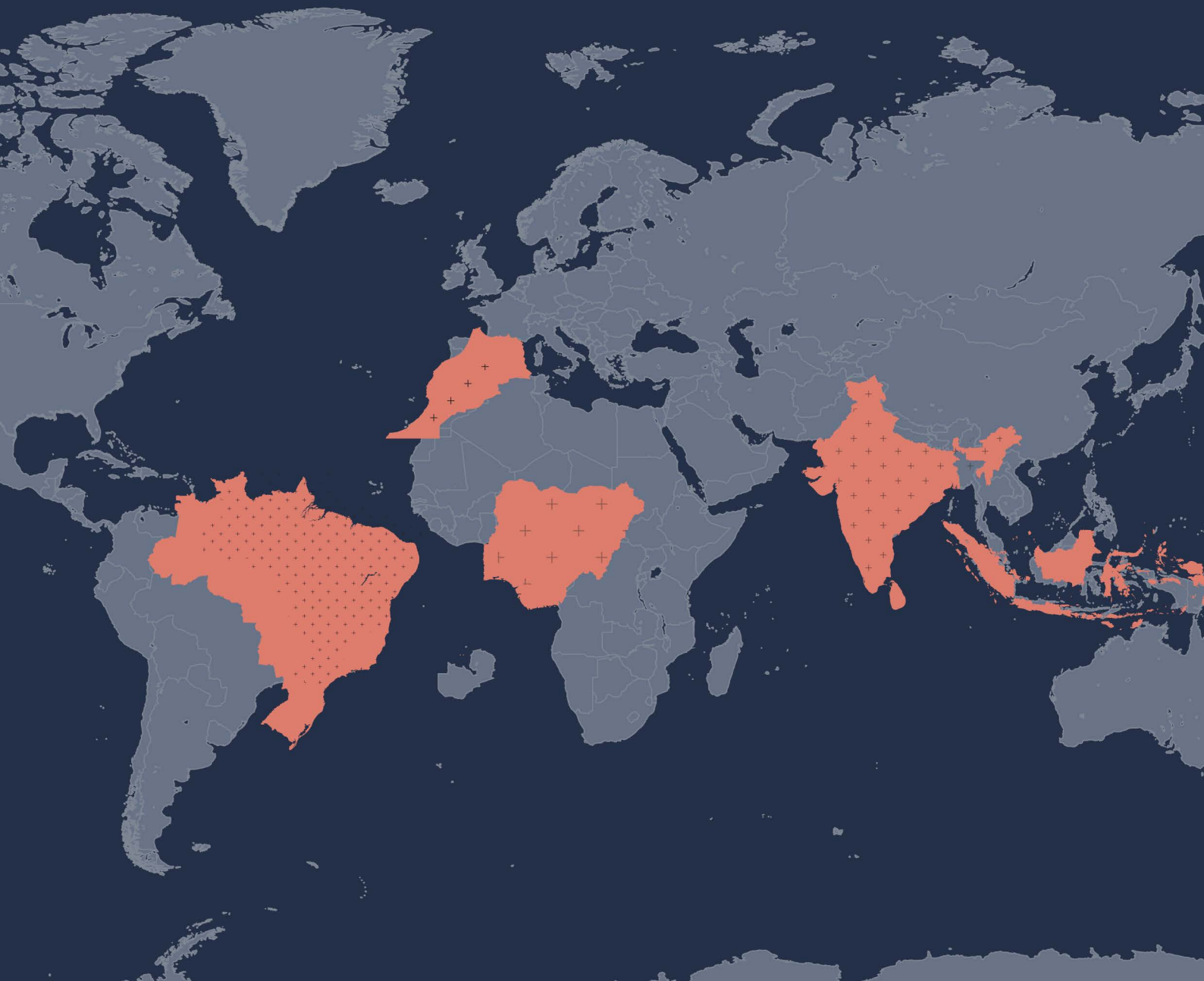
GLOBAL PARTNERS DIGITAL

Globalising Platform Regulation

The Impact of Online Platform Regulations from the European Union, the United Kingdom and Australia on Platform Regulation in Global Majority countries



Overview

This report examines how recent Online Platform Regulations introduced in the European Union, the United Kingdom, and Australia are shaping regulatory approaches to online platforms in the Global Majority. Focusing on six diverse case studies – Brazil, India, Indonesia, Morocco, Nigeria, and Sri Lanka – we explore how the Global North platform regulation frameworks are influencing emerging regulatory models across varied geopolitical, cultural, and legal contexts.

For each regulatory framework, we explore the approach to the scope of regulated entities, platform liability, additional duties of online platforms, regulatory mechanisms and considerations of human rights. Our analysis is grounded in international human rights law and draws on a wide range of evidence to assess both direct and indirect impacts of Global North regulation. We identify patterns of both convergence and divergence, seeking to highlight the means and strategies through which Global Majority countries adapt and localise external regulatory trends.

The report concludes with targeted recommendations for policymakers in the Global Majority, emphasising how international frameworks and global best practices can be critically adapted to local realities. In doing so, we aim to support the development of platform governance models that are context-sensitive, effective and rights-respecting.

Acknowledgements

This report was authored by Jacqueline Rowe on behalf of Global Partners Digital, with input from Maria Paz Canales (Head of Policy and Advocacy, Global Partners Digital). We also thank Ian Barber (former Legal and Advocacy Lead, Global Partners Digital) and Rose Payne (Policy and Advocacy Lead, Global Partners Digital) for their contributions on the framing of the research.

GLOBAL PARTNERS DIGITAL

Summary

Influence of the Global North

The regulatory choices in the EU's Digital Services Act (DSA), the UK's Online Safety Act (UK-OSA), and Australia's Online Safety Act (A-OSA) are influencing how Brazil, India, Indonesia, Nigeria, Sri Lanka, and Morocco are considering regulating online platforms.

Much like the GDPR's "Brussels Effect," the DSA in particular is setting a global precedent for transparency, accountability, and risk-based regulation.

Areas of Convergence

Systemic risk-based approaches: Several Global Majority countries are adopting duties of care, risk assessments, and transparency obligations inspired by the DSA, UK-OSA, or A-OSA frameworks.

Child safety: The jurisdictions analysed in Asia and Africa show strong alignment with the UK and Australian focus on age assurance and child protection.

Transparency & accountability: Requirements for clear terms of service, reporting, and researcher data access tend to mirror DSA provisions, expanding the ability of researchers and civil society actors to pursue evidence-based accountability from platforms.

Areas of Divergence

Regulatory independence: Unlike in the Global North, many Global Majority regulations face limitations in institutional settings. In many cases, regulators in charge of overseeing the frameworks can be closely tied to governments, creating risks of censorship and political misuse.

Human rights safeguards: Stronger protections for freedom of expression and privacy found in Global North laws are often absent or diluted in Global Majority frameworks. This creates opportunities to leverage the UN Guiding Principles on Business and Human Rights (UNGPs), oriented by the work of the OHCHR B-Tech Project, and best practices for shaping platform governance in the UNESCO's Guidelines for the Governance of Digital Platforms.

The role of encryption: While the EU exempts encrypted services under the DSA, the UK model threatens end-to-end encryption, and some Global Majority frameworks are leaning toward the UK's approach.

Risks of Transplantation

- Directly copying Global North frameworks into weaker rule-of-law environments may enable repression.
- Age assurance measures may harm privacy and disproportionately exclude vulnerable groups.
- Overly broad takedown obligations can incentivise platforms to censor legitimate speech.

Recommendations

1

Anchor platform regulation in human rights

2

Align with global norms and frameworks

3

Contextualise **regulatory approaches**

4

Establish an enabling regulatory ecosystem

5

Create independent and well-resourced regulators

6

Require transparency from online platforms

7

Adopt inclusive, multi-stakeholder processes

8

Carefully calibrate duty of care frameworks

9

Enhance the resilience of the information ecosystem

10

Foster transnational dialogue and Global Majority leadership

Contents

1. Introduction

Governments around the world are grappling with how and when to regulate online platforms, which have become an increasingly integral part of everyday life. While online platforms create unprecedented opportunities for communication, economic inclusion, access to information and movement-building, they also pose significant risks to people's wellbeing, human rights and democratic institutions – sometimes with devastating consequences. In response, governments worldwide are accelerating efforts to establish regulatory frameworks that hold online platforms accountable for the harmful effects of their services.

For many years, online platforms benefited from broad exemptions from liability for user-generated content. Early regulatory efforts largely focused on requiring faster removals of specific types of prohibited content – such as hate speech, terrorist content or child sexual abuse material (CSAM). In recent years, however, governments have begun adopting more comprehensive approaches. These newer frameworks impose wide-ranging duties on platforms to protect users from illegal and harmful content, safeguard users' rights and ensure fair competition.

A handful of Global North governments have already enacted holistic platform regulations of this kind. The **European Union's Digital Services Act** (**EU-DSA**), **Australia's Online Safety Act** (**A-OSA**) and the **United Kingdom's Online Safety Act (UK-OSA)** exemplify this trend. While they differ in scope and design, each framework imposes heightened obligations on online intermediaries – particularly large platforms – to monitor and mitigate illegal content, to assess and manage systemic risks, and to be more transparent and accountable to users and government. Both the UK-OSA and the A-OSA also require platforms to address "legal but harmful" content and to safeguard children from harms, including through age assurance measures.

As some of the earliest major blueprints for platform accountability, these regulations are reshaping the regulatory landscape not only at home but also abroad. Much like the EU's General Data Protection Regulation (GDPR) triggered a global wave of data protection reforms, the **EU-DSA** and its counterparts are influencing how governments around the world look to regulate platforms in their own contexts. The ability of the European Union, in particular, to set global standards through its regulatory approaches even beyond its borders is often described as "the Brussels Effect".[1] Some elements of the three frameworks mentioned above provide useful models for rights-respecting platform regulation.

Yet they also reflect the specific legal traditions, cultural values, and institutional capacities of Europe, the UK, and Australia, and require substantial financial and institutional resources to establish and sustain the relevant oversight mechanisms, which may prove more challenging in a range of Global Majority contexts. Furthermore, human rights organisations have raised concerns about the potential negative impacts of these regulations on freedom of expression and privacy, and the long-term consequences of these frameworks for human rights remain uncertain.

For governments in the Global Majority considering the EU-DSA, UK-OSA and A-OSA as templates for platform regulation, caution is essential. Directly transposing these frameworks into very different geopolitical contexts can lead to unintended consequences for human rights. These frameworks rely heavily on independent regulators and strong judicial systems, making them particularly vulnerable to abuse in environments with weaker rule of law, fewer institutional safeguards or inadequate protections against governmental overreach. In such contexts, stringent content moderation and proactive monitoring requirements may be misused to suppress dissent or target marginalized communities. Additional challenges arise in countries with high linguistic diversity. Where platforms lack the capacity to review content across multiple local languages within strict timeframes, overbroad censorship becomes more likely. This dynamic can also be exploited by bad-faith actors who manipulate reporting systems to silence minoritised groups.

This policy brief sets out the contextual and historical background of the platform regulation frameworks currently in force in Australia, the UK and the EU, alongside six emerging or recently amended frameworks in Brazil, India, Indonesia, Morocco, Nigeria and Sri Lanka. It then examines the extent to which the Global North regulations have shaped the Global Majority initiatives, analyzing how each framework defines:

1. the scope of regulated entities (Section 6.1)
2. platform liability for user-generated content and content moderation requirements (Section 6.2)
3. additional duties placed on online platforms (Section 6.3)
4. the nature of regulatory oversight (Section 6.4), and
5. consideration of human rights concerns (Section 6.5).

We conclude with ten recommendations (p. 38) for policymakers in the Global Majority, offering guidance on how to design online platform regulations that are effective, proportionate and rights-respecting, while accounting for local context.

2. Scope of this work

This section defines key terms guiding the scope and framework of analysis within this policy brief.

We use the term "online platform" to describe internet-based services that enable users to share and post content visible to other users. While regulatory frameworks may refer to these entities as "online services," "service providers," "intermediaries," or other terms, we use "online platform" consistently for clarity.

Although a wide range of laws and policies apply to such platforms, our focus is on those that impose responsibilities on online platforms to manage user-generated content. Specifically, we examine holistic "online safety" frameworks that assign broad duties and responsibilities to platforms, rather than laws narrowly targeting specific content types. We acknowledge, however, that these categories often overlap, as comprehensive frameworks are frequently built upon earlier, issue-specific regulations.

Our analysis centres on the relationship between online platform regulations in the Global North[2] and those in the Global Majority – a term we use to describe countries commonly categorized as low- and middle-income by the World Bank,[3] which account for over 85% of the world's population.[4] We select the EU-DSA, UK-OSA and A-OSA as some of the most influential Global North approaches around the world, while recognizing that other approaches to platform regulation have been explored and implemented elsewhere in the Global North.

We concentrate on the impact of these three regulations on regulatory initiatives in Global Majority countries. However, many countries in the Global Majority were already developing holistic platform regulations prior to the adoption of these Global North models.* Furthermore, similarities between frameworks do not always indicate direct influence or transfer; they may also arise from parallel policy debates, shared global concerns or other common external drivers. Accordingly, we emphasise cases where policymakers or key stakeholders explicitly cite the DSA, UK-OSA, or A-OSA during drafting or consultation processes. Where such evidence is unavailable or drafts of legislation are not yet finalized or publicized, we cautiously infer influence from contextual factors such as timing, substantive alignment and government announcements, while acknowledging that the absence of public documentation weakens claims of direct linkages between two frameworks.

* Examples include: Fiji's Online Safety Act (2018), Argentina's Intermediary Services on the Internet: Providers' Responsibility Guidelines (2012), Sudan's Regulation on content filtering and website blockage (2020) and Senegal's Draft Bill on the Framework of the Use of Social Networks (2020).

3. Platform regulation and human rights

Our analysis of platform regulations is grounded in international human rights law (IHRL). IHRL applies at all times and establishes states' obligations to respect, protect and fulfil human rights, including in the online environment.[5] All countries discussed in this report have ratified both the International Covenant on Civil and Political Rights (ICCPR) and the International Covenant on Economic, Social and Cultural Rights (ICESCR). Additionally, the UN Guiding Principles on Business and Human Rights (UNGPs) provide that states must protect against human rights abuses by third parties, including businesses, and that companies themselves have a responsibility to respect human rights wherever they operate.[6]

Online platforms – and by extension, state regulations which determine their responsibilities – affect the enjoyment of a wide range of human rights, including for people who may not directly use the services. Platforms have become central tools for facilitating individuals' right to express themselves and to access information (Article 19, ICCPR), to access opportunities for education (Article 13, ICESCR), and to take part in cultural life and enjoy the benefits of scientific progress (Article 15, ICESCR). Article 19 of the ICCPR guarantees everyone's right to hold opinions without interference and to seek, receive and impart information and ideas across borders and through any media.[7] It also sets out strict conditions for any restriction on this right, known as the **three-part test**. Restrictions on freedom of expression must:

1. be provided by **law**;
2. pursue a **legitimate aim** (respecting the rights or reputations of others or protecting national security, public order, public health or morals); and
3. be **necessary and proportionate** to achieving that specific legitimate aim.

Even where states do not expressly restrict certain types of online content, overly broad or rigid platform regulations risk incentivising platforms to censor legitimate online expression, undermining rights protected under international law.[8] This may further impact the enjoyment of a range of other rights, as freedom of expression is an enabling right that allows people to secure and defend all the other human rights.[9]

While online platforms can play a vital role in facilitating the enjoyment of human rights, they have also been implicated in rights violations. Weak protections for users' personal data and private communications may undermine the right to

privacy, while failure to promptly remove non-consensual intimate images (NCSII) can impact individuals' rights to freedom from unlawful attacks on their reputation (Article 17, ICCPR). Inconsistent content moderation practices can impact individuals' right to non-discrimination (Article 26, ICCPR), while algorithmic promotion of certain political content can distort democratic processes and impact the right to free and fair elections (Article 25, ICCPR). Failures to address online mis- and disinformation about COVID-19 jeopardized the right to health (Article 12), and not curbing online incitement to hatred or terrorism has, in some cases, contributed to violations of the right to life (Article 6, ICCPR).[10]

Children's rights represent a particular area of concern for many governments seeking to regulate online platforms. Under the Convention on the Rights of the Child (CRC), children and young people are entitled to be involved in decisions affecting them (Article 12) and the same rights to expression and access to information as adults (Article 13). At the same time, the CRC recognises children's needs for special safeguards and care due to their physical and mental immaturity, including protection from physical and psychological harm, exploitation and sexual abuse (Article 19). There is increasing evidence of the effects of age-inappropriate and harmful content, such as cyberbullying, sexual content and the promotion of unhealthy and unrealistic body standards, on child development.[11] As such, the protection of children's rights is a sensitive but increasingly central component of many governments' approaches towards platform regulation.

Multiple sources of international guidance set out how states and online platforms should respect and protect human rights in the online environment through platform regulation initiatives. The United Nations Office of the High Commissioner for Human Rights (OHCHR) has provided extensive guidance on how governments should regulate technology companies in line with the UNGPs via its B-Tech project.[12] The United Nations Educational, Scientific and Cultural Organisation (UNESCO) issued Guidelines for the Governance of Digital Platforms in 2023,[13] which stressed that content regulations must comply with the three-part test, be evidence-based and proportionate, include procedural safeguards, and be implemented by an independent body. In addition, international multi-stakeholder initiatives such as the Manila Principles on Intermediary Liability,[14] the Santa Clara Principles on Transparency and Accountability in Content Moderation[15] and the Global Network Initiative (GNI) Principles on Freedom of Expression and Privacy[16] reinforce core principles of respect for human rights in content moderation decisions, emphasising regulations which focus on disclosure and transparency from platforms rather than sweeping takedown requirements.

4. Global North platform regulations

In this section, we consider the political, legislative and societal context and background of the three Global North platform regulations of focus: Australia's Online Safety Act, the United Kingdom's Online Safety Act, and the European Union's Digital Services Act.

AUSTRALIA

Safeguarding children from harmful and inappropriate material online has been a longstanding policy priority for the Australian government.[17] In 2015, Australia established the "world's first government agency dedicated to keeping people safer online", when the then Coalition government passed the **Enhancing Online Safety for Children Act (EOSCA)**.[18] The eSafety Commissioner was empowered to monitor and promote compliance with the **EOSCA**, which sought to address cyberbullying targeting Australian children. Under the Act, social media services were required to: include prohibitions on cyberbullying in their terms of service; implement user complaint mechanisms for removing cyberbullying content; and designate platform representatives to engage with regulators. The eSafety Commissioner was also tasked with supporting and encouraging the implementation of measures to improve online safety for children (Section 15(1)(c)) and issuing guidelines and statements related to best practices for child online safety (Section 15(1)(p)).

In subsequent years, several further investigations and reports by parliamentary committees and the eSafety Commissioner were published, addressing children's access to gambling and pornography sites.[19] A statutory review of the **EOSCA** in 2018 recommended a more "proactive" regulatory framework for online platforms, requiring the online and digital industry to "implement measures to patrol, detect, remove and deter the posting of and access to illegal and harmful content".[20] Following a year of drafting and consultation, the **A-OSA** was passed in 2021, significantly expanding the Commissioner's mandate and powers.

Under the **A-OSA**, the eSafety Commissioner may order online platforms to remove prohibited content, require compliance reporting, and oversee industry codes and standards on tackling prohibited content. Child online safety remains central to the regulation: the Commissioner is explicitly required to have regard to the CRC in performing its functions (Section 24.1). The Act also extends protections for adult online safety, requiring platforms to take reasonable steps to prevent

users from accessing prohibited materials and maintain reporting and complaints systems. In 2022, the **Basic Online Safety Expectations (BOSE)** set out further responsibilities for platforms across specific content categories.[21]

Since its passage, the **A-OSA** has been amended several times, continuing to reflect Australia's emphasis on child online safety. Most notably, the **Online Safety Amendment (Social Media Minimum Age) Bill 2024** bans under-16s from accessing platforms that facilitate social interaction from December 2025. To support implementation, the Australian government allocated AUD $6.5 million for an Age Assurance Trial to explore appropriate technical options for age verification.[22]

A statutory review of the Act published in 2024 also recommended that Australia go further by introducing a "singular and overarching duty of care" on online platforms, with stronger civil penalties for non-compliance. The review also recommended requiring online platforms to conduct risk assessments and annual transparency reports, in line with other emerging regulatory frameworks in the Global North.[23]

THE UNITED KINGDOM

The UK's path to online platform regulation began in April 2019 with the publication of the Online Harms White Paper by the then-Conservative government.[24] The white paper – co-drafted by the UK Department for Digital, Culture, Media and Sport and the UK Home Office – proposed a statutory duty of care for online platforms, requiring them to put systems and processes in place to address illegal and harmful content. While it referenced risks such as terrorism, disinformation and online criminal activity, there was also strong emphasis on the impact of legal but harmful content, particularly its effect on children's mental health and wellbeing. The white paper also proposed the establishment of an independent regulator to oversee implementation, which – after consultation – was confirmed by the government to be the Office of Communications (Ofcom), the existing regulator for broadcasting, telecommunications and postal industries.[25] While developing the proposed legislation, the government also published two voluntary codes of practice for platforms to address terrorist content and CSAM.[26]

A draft Online Safety Bill was published in May 2021 and scrutinized by a joint Parliamentary Committee before its formal introduction in March 2022. After significant revisions during its passage through Parliament, the bill was passed in October 2023 as the **UK-OSA**. It requires all regulated platforms to assess and mitigate risks of illegal content and activity on their services, as well as from content which is harmful to children. The UK-OSA also introduces and updates criminal communications offences, including sending false or threatening

communications, cyberflashing, showing flashing images to people with epilepsy and encouraging or assisting self-harm.

Under the **UK-OSA**, online platforms must establish reporting and complaints mechanisms, report detected CSAM to the National Crime Agency and have due regard to users' rights to freedom of expression and privacy when implementing content policies. Larger platforms must also give users greater control over the kinds of content they see, enforce their terms of service consistently, implement redress mechanisms for wrongful content removals, and assess the impact of their safety policies and procedures on users' rights to freedom of expression and access to journalistic content.

As regulator, Ofcom is empowered to demand information from platforms, conduct audits, issue enforcement notices, impose financial penalties, and seek court orders for business disruption measures. Ofcom is also tasked with issuing codes of practice to guide platforms' compliance. To date, it has published **codes on Protecting People from Illegal Harms**[27] **and Protection of Children**,[28] which set specific expectations for online platforms regarding risk assessment, automated and manual moderation of illegal content, and the classification of harmful material.

THE EUROPEAN UNION

The EU's supranational character enables it to pursue long-term strategic priorities in regulation, and its consensus- and values-driven approach somewhat elevates the status of its regulatory benchmarks beyond the legal borders of the EU.[29] Combined with the size of its internal market, this gives the EU significant soft power in shaping global debates on online platform governance.

For over two decades, online platforms in the EU were governed by the **Electronic Commerce Directive (2000/31/EC)**. This Directive harmonized rules for online services across EU Member States, promoting e-commerce while limiting platform liability; hosting providers were not liable for illegal third-party content if they removed it promptly once notified (Article 14). The Directive also prohibited Member States from imposing general monitoring obligations on online intermediaries (Article 15), following a ruling by the European Court of Justice that general monitoring obligations are unlawful.[30] As user-to-user online platforms grew in scale and impact, pressure mounted to update the e-Commerce intermediary liability to rebalance the responsibilities of online platforms towards their users. The EU issued the **Code of Practice on Disinformation** (2018) and the **Regulation on Terrorist Content Online** (2022), but the **EU-DSA** represents its most comprehensive intervention in platform governance to date.

The **EU-DSA** was proposed in December 2020, approved in 2022 and came into force in February 2024. While the **e-Commerce Directive** continues to govern intermediary liability for user-generated content, the **EU-DSA** requires online platforms to implement complaint and reporting systems, prioritize reports of illegal content by "trusted flaggers", and promote transparency and freedom of choice for users. Very Large Online Platforms and Services (VLOPs/VLOSEs) – of which there are currently 19[31] – are also required to adhere to additional obligations relating to assessing and mitigating risks emerging from the use of their services, and complying with auditing and reporting requirements.

Enforcement is split between Member States and the European Commission. Each Member State must designate a Digital Services Coordinator (DSC) to oversee compliance nationally, with powers to access platform data, conduct inspections, certify trusted flaggers, and handle user complaints (Article 49). The European Commission directly supervises VLOPs and VLOSEs, with powers to designate them and request information on their implementation of **EU-DSA** requirements. The regulator can impose significant fines (up to 6% of annual turnover) for non-compliance. The **EU-DSA** also established new institutions to strengthen accountability further, including the European Board for Digital Services,[32] the European Centre for Algorithmic Transparency,[33] and the DSA whistleblower tool for monitoring compliance by VLOPs and VLOSEs.[34] The EU Commission has also signed an agreement with Australia's eSafety Commissioner to foster collaboration on the enforcement of online platform regulation, including expert dialogues, joint training of technical staff, and sharing of best practices.[35]

5. Global Majority platform regulations

This section provides an overview of the motivations, background and current status of six recent or emerging online platform regulatory initiatives from Global Majority countries, concentrating on comprehensive regulatory frameworks as opposed to ad hoc reactive measures. We focus, in particular, on frameworks for which there is explicit evidence of influence by one of the three Global North platform regulations described in the previous section (AU-OSA, UK-OSA and EU-DSA).

The term "Global Majority" encompasses countries with diverse cultural, political, economic and social contexts, with considerable variation in the design and motivation of online platform regulation. However, many Global Majority countries share common concerns about the impacts of online platforms, particularly where digital literacy gaps, linguistic diversity, ethnic and religious tensions or risks of government overreach make effective content governance both more difficult and more essential. Responses to these challenges have ranged from outright bans and shutdowns of platforms seen as inactive on issues such as hate speech or disinformation,[36] to more nuanced attempts to craft regulations that balance platform interests with the protection of user rights.

BRAZIL

The **Marco Civil da Internet (MCI)**, passed in 2014, has fundamentally shaped the landscape of online platform regulation in Brazil.[37] The **MCI** exempts platforms from liability for user-generated content, unless they fail to comply with a court order for its removal (Article 19). The only exceptions are for copyright violations and NCSII, where platforms can be held liable upon user notification alone (Article 21).[38] The legislation explicitly references the right to freedom of expression throughout, with a clear intention to ensure that the judiciary – not private companies – determines what content should be prohibited online.

Critics have argued that this liability model is too lenient, allowing large online platforms to avoid responsibility for harmful content which is amplified by their services.[39] Concerns have grown around the spread of online content linked to violence amongst young people,[40] and political instability, such as the attempted overthrow of the legitimately elected Brazilian government in January 2023.[41] As such, there have been a number of legislative proposals to reform the intermediary liability system in the MCI, but none have yet been passed. The most prominent

attempt was **Bill No. 2630/2020 to establish the Brazilian Law of Freedom, Responsibility and Transparency on the Internet**, nicknamed "**The Fake News Bill" (FNB)** due to its original focus on tackling mis- and disinformation during the COVID-19 pandemic.[42] Although approved by the Senate in 2020, a revised version of the **FNB** stalled in the Chamber of Deputies in 2023, due to disputes over the scope of MCI reform and intermediary liability rules.[43]

In the meantime, a landmark ruling by the Brazilian Supreme Court has recently drastically reshaped the Brazilian intermediary liability framework. The Court heard two cases concerning individuals who had requested online platforms to take down content which significantly impacted their privacy or reputation.[44] In its judgment, the Court ruled that Article 19 of the **MCI** is partially unconstitutional for failing to adequately protect constitutional values, specifically fundamental rights and democracy.[45] While the Court upheld the court order requirement for "crimes of honour" (defamation, slander or libel), it expanded the notice-and-takedown procedure to cover all forms of illegal content, not just copyright and NCSII. Furthermore, the Court ruled that platforms are liable for illegal content promoted through paid advertisements or artificial networks regardless of notification. The Court urged the National Congress to update the existing legal framework for platform liability accordingly.[46]

Following the ruling, reports indicate that the government plans to revise and reintroduce the **FNB** or a similar bill.[47] Notably, the **EU-DSA** has had a visible impact on the ongoing online platform regulation debates and recent Supreme Court ruling. For example, the version of the **FNB** introduced by the Brazilian government in May 2023 contained 25 explicit references to the **EU-DSA** in the justification, reflecting both EU–Brazil diplomatic engagement and efforts by EU parliamentarians to share expertise.[48] More broadly, the very existence of the **EU-DSA** has reportedly strengthened domestic campaigns pushing for stricter online platform regulation in Brazil.[49]

INDIA

India's **Information Technology Act (IT Act)**,[50] enacted in 2000, is the primary legislation governing e-commerce and cybercrime in India. Over time, the rules issued under the IT Act have significantly reshaped the liability and responsibility of online platforms for illegal and harmful content. **The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules 2009**[51] empowered the government to restrict Internet services under six broad conditions. More recently, the **Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules 2021**[52] (the **IT Rules**) imposed

strict content filtering and takedown obligations on online platforms. The **IT Rules** also established a government committee with authority to "fact-check" content and order content takedowns.[53] These provisions were widely criticized for granting the government overbroad powers to intervene in platforms' content governance mechanisms, raising serious concerns for freedom of expression and independent online media.[54]

In 2023, the Indian government announced plans to replace the **IT Act** and **Rules** with a new **Digital India Act (DIA)**. The **DIA** will introduce new rules for a wider range of digital intermediaries, including not just online platforms but also AI companies.[55] While no draft has yet been published and the legislative process has been somewhat opaque to date,[56] the Indian Ministry of Electronics and Information Technology (MeitY) have outlined the goals of the **DIA**: fostering an open Internet, enhancing online safety and trust, and creating a new adjudicatory mechanism for online civil and criminal offences designed to provide citizens with more timely and consistent remedies for harms caused by digital services.[57]

Although official documents and ministerial statements have not explicitly cited influence from the **EU-DSA, UK-OSA** or **A-OSA** on the Indian approach to platform regulation, several legal commentators suggest that these frameworks are shaping India's regulatory trajectory, particularly requirements relating to user safety obligations, systemic risk assessments, and stronger accountability mechanisms.[58]

NIGERIA

Early efforts to regulate online platforms in Nigeria were controversial. The **Protection from Internet Falsehood and Manipulations Bill** (2019) sought to address mis- and disinformation, but proposed sweeping powers for government authorities, including the ability to compel online platforms to take down content deemed to be false, and to shut down their services if they did not comply. The bill was widely criticized for potentially enabling censorship and was never passed. Later, the Nigerian Government suspended Twitter's services in June 2021 for approximately six months, partly in response to Twitter's removal of a controversial tweet by the then-Nigerian president.[59]

With the 2019 bill stalled, Nigeria's National Information Technology Development Agency (**NITDA**) issued a **Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries (Code of Practice)** in 2022.[60] The Code aimed to increase platform accountability by requiring them to provide complaints and appeals mechanisms for users, to publish their terms of service, to carry out risk assessments for harmful content and to audit automated content moderation tools for accuracy and fairness. It also included more nuanced provisions on

tackling mis- and disinformation than the 2019 bill, emphasising investment in culturally-sensitive content moderation, digital literacy, and researcher access to data. However, concerns were raised about the Code's strict content takedown deadlines, vague definitions of "harmful" content, and requirements that platforms prevent uploads of illegal content to their services, which would imply a general monitoring requirement widely perceived to be a disproportionate interference with users' privacy.[61]

In response to these criticisms, NITDA launched a new multi-stakeholder consultation process to help reshape its online platform regulation approach. This culminated in a 2024 white paper outlining plans for an **Online Harms Protection Bill (OHPB)**.[62] The proposed **OHPB** adopts a co-regulatory approach designed to secure transparency, responsibility and accountability from online platforms. The white paper also recognised the difficulties of balancing the need to address harmful content with the protection of freedom of expression, highlighting the risks of "the subjective nature of content interpretation… regulatory overreach, and the potential impact on innovation, especially for smaller online platforms."[63]

The white paper drew on comparative regulatory models for online platforms across Africa and globally, but specifically identified lessons and best practices laid out in more proactive approaches to online safety, such as the **EU-DSA** and **UK-OSA**, as shaping the government's current approach.[64] These frameworks appear to have influenced Nigeria's turn towards risk-based, transparency-focused regulation, marking a clear departure from earlier, more punitive approaches to online governance.

INDONESIA

Indonesia's **Electronic Information and Transaction Law (Law No. 11/2008)** provides the foundation of the country's online platform regulation framework.[65] While the original law exempted platforms from liability for user-generated content, successive amendments and regulations have steadily expanded their obligations under the law.[66] In particular, the **Ministerial Regulations on Private Electronic System Operators (MR5)** of 2020 required platforms to register with authorities, prevent the dissemination of "prohibited content" (broadly defined), and remove such content within strict timeframes once notified.[67] The Indonesian Ministry of Communication and Digital Affairs (MOCDA) – previously referred to as Kominfo – enforces the regulations and has used these provisions to fine, throttle and even block online platforms, particularly during times of political unrest.[68]

Indonesia's focus on government-ordered takedowns stands in stark contrast to the independently regulated, risk-focused approaches of the E**U-DSA, UK-OSA**

and **A-OSA**. However, Indonesia's most recent rules issued under the **Electronic Information and Transaction Law** show signs of increased alignment with Global North approaches to child online safety. Specifically, **Government Regulation No. 17 of 2025 on the Governance of Electronic System Implementation in Child Protection (GR17/2025)** imposes binding obligations on both public and private digital platforms and services to protect children who use or access their platforms. Its provisions include mandatory risk assessments, age-appropriate design, and proactive mitigation of harms to children – closely echoing the child-safety-first approach of the **UK-OSA** and the **A-OSA**. Online platforms have until 2027 to comply with the new rules.[69]

This shift illustrates how Global Majority states may selectively draw from Global North frameworks: while Indonesia maintains restrictive, state-led enforcement in some areas, it has incorporated international models into sector-specific regulations, especially where child protection provides political and normative legitimacy.

SRI LANKA

Sri Lanka proposed the **Online Safety Act (OSA)** in September 2023,[70] partially motivated by the concerns around the role of illegal online content inciting terror attacks in the country in 2019 and the need to curb the dissemination of fake news and hate speech targeting marginalized communities.[71] The Act establishes a centralized "Online Safety Commission" to oversee online content and user behaviour, with sweeping powers to regulate speech online. Critics argue that the framework is authoritarian, disproportionate, and heavily geared towards censorship. More than 50 petitions were filed in the Supreme Court during the parliamentary review process for the OSA, warning of its serious risks to freedom of expression.[72] International human rights organisations, domestic civil society groups, and even the UN High Commissioner for Human Rights also condemned the bill.[73] Despite this opposition, the Act was passed in January 2024, even though 51 petitions were presented to the Sri Lankan Supreme Court, motivating 31 recommended amendments; only a handful of them were adopted.[74]

Reports and right-to-information filings show that the Sri Lankan **OSA** drew inspiration from both Singapore's **Protection from Online Falsehoods and Manipulation Act** (2019) and the **UK-OSA**.[75] However, whereas the UK framework is grounded in transparency, co-regulation and accountability, Sri Lanka's adoption has largely stripped these safeguards, reconfiguring the model into a tool for centralized state control. This underscores the risk that Global North regulatory templates, when adapted without robust institutional safeguards, may inadvertently legitimize restrictive approaches in more fragile democratic contexts.

MOROCCO

The Moroccan government has recently announced plans to draft a new legal framework to regulate online platforms and address illegal and harmful content.[76] The proposed law is expected to expand the powers of Morocco's High Authority for Audiovisual Communication (HACA), enabling it to oversee online platforms' compliance with the new regulation and order content removals. The framework will also impose obligations on online platforms regarding content moderation, user and complaints systems and reporting requirements. Early reports indicate that the regulation is explicitly inspired by the **EU-DSA**, reflecting Morocco's interest in aligning its approach with international best practices while adapting them to local governance structures.[77]

6. Influence of Global North platform regulations on Global Majority platform regulations

This section examines the normative impact of the three Global North platform regulation frameworks – the **AU-OSA**, **UK-OSA**, and **EU-DSA** – upon platform regulatory processes in the Global Majority. We focus on the six regulatory frameworks or proposals described in Section 2 (in Brazil, India, Indonesia, Morocco, Nigeria and Sri Lanka), but also include relevant examples from other Global Majority frameworks not explicated in Section 2. We consider specific elements of platform regulations:

1. **The regulatory scope** – which type of services fall under the law, and whether private and end-to-end encrypted (E2EE) messaging services are included.
2. **Platform liability regime for user-generated content** – obligations and responsibilities for the types of user-generated content covered by the regulations and risk assessments.
3. **Additional duties required of online platforms** – including terms of service publication, user complaint and appeals mechanisms, transparency reports, age verification and researcher access to platform data.
4. **The regulatory oversight regime** – the regulatory bodies, enforcement mechanisms, information requirements and penalties designed to ensure platform compliance.
5. **Human rights safeguards** – particularly balancing the prevention of online harms with protections for freedom of expression, privacy and other fundamental rights.

For each analytical category, we first present a comparative analysis of the approaches taken in the **A-OSA**, the **UK-OSA** and the **EU-DSA**. We then identify and discuss approaches to these elements of the regulation in the initiatives in Brazil, India, Indonesia, Morocco, Nigeria and Sri Lanka, discussed in Section 5. Our analysis seeks to highlight how the Global North frameworks are shaping or influencing these approaches.

6.1 Regulatory Scope

6.1.1 Scope of Regulated Entities

A-OSA	UK-OSA	EU-DSA
The A-OSA applies to a range of **electronic services that allow end-users to access online material**, including social media services that facilitate user-to-user interactions and internet search engines. Certain provisions also apply to hosting services and internet service providers [Sections 5, 13, 17].	The UK-OSA applies to **all "user-to-user" platforms**, defined as services where users can encounter content generated by others. It encompasses most platforms operating in the UK or targeting a significant UK audience, with exceptions for email providers and state services [Section 1].	The DSA applies to "**intermediary service providers**" including hosting services and caching services, as well as online platforms and search engines. It is applicable to both EU-based companies and those operating within the EU. The DSA imposes more stringent regulations on VLOPs and VLOSEs, defined as those with over 45 million active users in the EU [Article 2].

The Nigerian 2022 **Code of Practice** did not differentiate between different categories or sizes of online platforms. However, the white paper on the proposed **OHPB** recommends a more nuanced approach, scaling online platforms' responsibilities according to platform size, influence and societal impact.[78]

In India, the **2021 IT Rules** distinguish between significant and regular social media platforms, with the former having more than 5 million users in India. MeitY has also indicated that the upcoming **DIA** will categorise intermediary services according to the severity and nature of the risks they pose to users. However, unlike the Global North frameworks, the **DIA** would also apply to AI-based services, reflecting India's interest in regulating emerging digital technologies alongside traditional platforms.[79]

In their votes on the constitutionality of the **MCI**, Brazilian Supreme Court Justices recommended that future platform regulation should take a tailored, size-sensitive approach to online platform obligations, praising how the **EU-DSA** categorises platforms by type and size and exempts small and micro-businesses in its ruling.[80]

6.1.2 Application to Encrypted Services

A-OSA	UK-OSA	EU-DSA
Online platforms that use encryption are expected to take reasonable steps to develop and implement processes to detect and address unlawful or harmful content on these services, **but this requirement does not require them to decrypt content or implement a systemic vulnerability into an encrypted service** [BOSE, Section 8].	The UK-OSA permits Ofcom – the regulator – to demand that encrypted services use "**accredited technology**" to monitor and remove unlawful content. Despite assurances that encryption will be maintained, there is concern that no such technology currently exists, posing a threat to privacy and encryption [Section 121].	The DSA does not mandate changes to encryption practices and leaves decisions on encryption to individual Member States. **Encrypted messaging services are specifically exempt from the DSA's requirements** [Article 1(4)].

In Brazil, concern about the spread of disinformation and hate speech on private messaging services has influenced platform regulation discussions. The original **FNB** targeted "user-to-user" communication tools, including private ones, and proposed a requirement for private messaging services to be able to trace and identify original senders of messages, provisions which deeply concerned privacy and encryption advocates.[81] Telegram has been blocked twice in Brazil for failure to address fake news and hateful content in mass private messages.[82] However, the recent Supreme Court ruling held that Article 19 of the **MCI** still holds regarding private messaging services, whereby they are only liable for user-generated content if they fail to remove it when ordered to do so by a court.[83]

The Indian government also previously sought to require online platforms to trace the first-senders of messages in the **IT Rules**.[84] The Minister of State for Electronics and Information Technology has also indicated that the forthcoming **DIA** will include similar provisions to address internet-aided distribution of CSAM.[85]

Regarding E2EE messaging services, the Nigerian white paper on the **OHPB** compared the controversial provision about "accredited technology" for monitoring encrypted communications in the **UK-OSA** with the exemption for E2EE private messaging apps as "mere conduits" of online content in the **EU-DSA**.[86] The white paper proposes the **EU-DSA**-style approach to ensure that private communications are exempt from content monitoring and moderation requirements on the basis that "encryption enables privacy and human rights in the digital space."*

* Despite the assertion that private messaging services will be exempt in line with the EU-DSA, we note that elsewhere in the white paper, NITDA recommended that guidelines on online harms protection should clarify "the conditions under which private messages may be reviewed" for content moderation purposes, indicating that perhaps a UK-OSA-influenced approach has not been entirely eliminated from the OHPB.

6.2 Platform liability regime for user-generated content

6.2.1 Type of Content Covered

A-OSA	UK-OSA	EU-DSA
The A-OSA specifically focuses on harms arising from cyberbullying and cyber-abuse, NCSII, and material depicting abhorrent violent conduct [Parts 5-8]. Certain requirements address other types of illegal content (Class 1 material) and age-inappropriate content (Class 2) [Part 9].	The UK-OSA outlines specific "priority illegal content" that platforms must address. Additionally, platforms accessible to children must address content that is harmful to children that is not necessarily illegal, such as content promoting eating disorders. [Sections 59, 61 and 62].	The DSA targets illegal content but does not cover harmful content that is not illegal. However, it includes measures for VLOPs and VLOSEs to tackle disinformation and other content-related risks. [Articles 4, 35.]

Indonesia's **GR17/2025** focuses primarily on legal but harmful content, requiring platforms to consider the risks to children posed by content which may cause them psychological harm, including pornography, violent or otherwise inappropriate content.[87]

In **Morocco**, the upcoming regulation for online platforms is expected to include provisions relating to illegal content such as hate speech, as well as fake news and content harmful to children.[88]

The Sri Lankan **OSA** specifies a range of types of "prohibited statements", including false statements which promote hostility, rioting or mutiny, false statements which disturb religious ceremonies or outrage religious feelings, and false statements which deceive or impersonate others. It also prohibits content which amounts to harassment or NCSII and CSAM. The Online Safety Commission can order both individuals and platforms to remove these prohibited content types.[89]

In Nepal, the Social Media Bill 2081[90] was presented in January 2025 and is currently under review. It proposes requiring platforms to ensure they do not "disseminate content that harms Nepal's sovereignty, territorial integrity, national security, national unity, independence, dignity, or national interests, or that incites social, cultural, or religious disharmony", to develop technological measures to prevent users from posting illegal content, and to remove or prevent content that "severely harms an individual's character, contains hate speech, incites violence, or disrupts communal harmony" (Article 12). Other provisions relate to cyberbullying and content which is gruesome, obscene, false or misleading. While these definitions were extremely broad and posed clear risks to freedom of expression online, UNESCO has since reviewed the bill and provided capacity-building on platform regulation to Nepali stakeholders, who have committed to revising the Bill and the categories of designated content within it to uphold Nepalis' human and constitutional rights.[91]

6.2.2 Platform Liability for User-Generated Content

A-OSA	UK-OSA	EU-DSA
Platforms are not liable for user-generated content but must act within 24 hours of receiving a report of prohibited content from the eSafety Commissioner [Sections 65, 109]. The platform is additionally expected to take reasonable steps to proactively minimize the extent to which content in the service is unlawful or harmful [BOSE, Section 6].	Platforms must proactively manage and remove "priority illegal content," which includes severe offences such as terrorism-related material, CSAM, and violent content. Platforms are not liable for user-generated content but must act swiftly upon becoming aware of illegal content [Section 10].	Providers are not held liable for content hosted on their platforms but must remove illegal content promptly once notified. The DSA does not impose a general monitoring obligation but emphasises the need for a rapid response to reported content [Articles 8 and 9].

In Brazil, the **MCI** originally exempted online platforms from liability for user-generated content unless they had received a court order to remove it and failed to do so, or if they had received a notification from an affected party in the case of NCSII.[92] However, under the recent Supreme Court ruling, platforms are now civilly liable for any illegal content which they do not remove after being notified, *without* needing a court order. There is an exception for content which constitutes crimes against honour (such as defamation), for which the court-ordered takedown regime still applies. Conversely, for advertisements, promotional content or material produced by bots, the platforms are liable for illegal content regardless of user notification. The Supreme Court ruling shields platforms from penalties for removing content which is later deemed legal.[93]

In Sri Lanka, the **OSA** exempts online platforms from liability for prohibited content, except where the platform has played a key role in distributing or editing the content or has failed to comply with an order from the Online Safety Commission relating to the removal of prohibited content.[94]

In India, the **IT Rules 2021** imposed strict content filtering and takedown obligations on online platforms, limiting their ability to claim protection from liability for user-generated content.[95] The upcoming **DIA** is also expected to further amend the intermediary liability framework, with MeitY questioning whether there should be "safe harbour" for all intermediaries in their DIA briefing.[96]

In 2021, the Chilean Congress considered the Digital Platforms Regulation Bill N° 14.561-19.[97] While the bill sought to protect the rights of users online and hold platforms accountable for infringements of users' rights, the proposed intermediary liability framework was confusing and contradictory. Article 6 exempted platforms from liability for illegal user-generated content where they were not aware of it, but Article 15 held that platforms should be liable for financial and moral damages caused to users. These provisions, amongst others, were criticized by a number of digital rights groups for posing risks to freedom of expression,[98] and the bill was discarded and never passed.

6.2.3 Content Moderation Requirements

A-OSA	UK-OSA	EU-DSA
Platforms are required to take reasonable steps to proactively minimize unlawful and harmful material on their service, including by developing and implementing processes to detect and remove such content. [BOSE, Section 6].	Platforms must have clear content moderation policies, proportionate systems and processes that address illegal content and content harmful to children. They must also empower adult users to actively manage the moderation of content, especially concerning priority illegal content. [Sections 10, 12 and 15].	Platforms must implement transparency measures for their content moderation practices and provide specific requirements for addressing illegal content, particularly for VLOPs and VLOSEs. [Articles 15, 16 and 17].

The Nigerian **Code of Practice** requires online platforms to respond to notices of illegal content within 48 hours; these strict takedown timelines have been criticized by digital rights groups for incentivising over-removal of content.[99] The upcoming **OHPB** seeks instead to propose "reasonable" and "fair" timeframes for platforms to respond to reports of illegal and harmful content, and will also provide a threshold to determine the qualification and scale of human content moderation efforts that must be utilized on platforms, particularly during elections or other situations or happenings that may call for urgent action. Large platforms will also be subject to additional content moderation responsibilities for content and behaviour that is harmful to children.[100]

Morocco's upcoming regulation for digital platforms may include requirements for platforms to implement automated detection systems for harmful content, particularly that which affects children. The focus on proactive content moderation and child safety hints at influence from the **A-OSA** and **UK-OSA**.

The Brazilian Supreme Court's recent ruling on the **MCI** holds that platforms must act diligently to moderate illegal content and behaviour (Paragraph 5.2). However, several Justices noted that any future platform regulation should follow the European model in exempting online platforms from any requirements for proactive general monitoring of all online communications for content infringements, to safeguard individuals' rights to privacy and freedom of expression.[101]

Sri Lanka's **OSA** requires platforms to remove flagged content within 24 hours of notification – requirements that several major technology companies have called "unworkable"[102] and which digital rights organisations have argued will lead to over-censorship of legitimate speech.[103]

Tanzania recently issued an amendment to the Electronic and Postal Communications (Online Content) Regulations of 2021,[104] rules which have been extensively criticized by digital rights groups for adverse impacts on human rights.[105] The 2025 amendments require social media platforms to "deploy a mechanism of filtering and removing prohibited content from their platforms",[106] further exacerbating concerns of overbroad censorship and a chilling effect of the regulation on freedom of expression.

6.2.4 Risk Assessments

A-OSA	UK-OSA	EU-DSA
Risk assessments, including child safety risk assessments, are included as potential measures that platforms can take to meet their online safety obligations, but are not specifically required under the legislation [BOSE Section 6, 8A].	Platforms are required to perform risk assessments to identify and mitigate illegal content, particularly when releasing new features. [Sections 9, 26]. Platforms accessible to children must undertake stricter risk assessments, which raises concerns about age verification and privacy. [Sections 11, 28].	VLOPs and VLOSEs are required to conduct and publish annual risk assessments concerning their platform's design, functionality and use, focusing on systemic risks. Smaller platforms are exempt from the most intensive risk assessments [Article 34].

The 2023 draft of Brazil's **FNB** proposed a duty of care for online platforms, inspired by the **EU-DSA** and **UK-OSA**, requiring them to analyze and mitigate systemic risks stemming from their service design and operation.[107] The recent Supreme Court ruling on the **MCI** also indicates a risk-focused approach to platform regulation, focusing on the prevention and mitigation of illegal content and noting that platforms' local representatives may be required to share information about monitoring of systemic risks with local authorities.[108]

India's IT Rules (2021) introduced due diligence requirements for significant social media intermediaries, and the upcoming **DIA** is expected to embed periodic risk assessments as a core duty of all regulated online platforms.[109]

Nigeria's **Code of Practice** and proposed **OHPB** require platforms to actively monitor and mitigate risks associated with their services, and the OHPB will also require large platforms to regularly publish comprehensive risk analyses of potential harms to children.[110]

Thailand produced a draft Platform Economy Act in 2022. The proposal incorporated a range of features mirroring the EU-DSA and the EU Digital Markets Act, including requiring large online platforms to evaluate system risks annually with external experts.[111] The draft bill is still under consideration. [112]

6.3 Additional duties of online platforms

6.3.1 Public Transparency Measures

A-OSA	UK-OSA	EU-DSA
Publication of Terms of Service		
Platforms must publish up-to-date Terms of Use and ensure these are accessible to end-users.	The UK-OSA outlines specific "priority illegal content" that platforms must address. Additionally, platforms accessible to children must address content that is harmful to children that is not necessarily illegal, such as content promoting eating disorders. [Sections 59, 61 and 62].	The DSA targets illegal content but does not cover harmful content that is not illegal. However, it includes measures for VLOPs and VLOSEs to tackle disinformation and other content-related risks. [Articles 4, 35.]
Transparency Reporting		
Platforms must publish transparency reports that outline how the service is enforcing its terms of use [BOSE 14, 17, 18].	Platforms are required to inform users about policies, functionalities and content moderation policies and how decisions are made [Section 10 (7-9) and 12 (11-14)].	Platforms must make publicly available annual reports on content moderation [Articles 15 and 42].
Transparency Reporting Data Access for Research		
The A-OSA and BOSE do not include any provisions relating to data access by researchers.	Ofcom is required to produce a report on data access for researchers and consider methods to enhance it. However, the UK-OSA does not provide specific new provisions to expand researcher data access beyond this report. [Section 162]	VLOPs and VLOSEs will be required to offer data access for researchers seeking to assess "systemic risks" that might affect the EU, which broadly refers to the risks of how illegal content might impact or undermine human rights. [Article 40]

In Brazil, the Supreme Court ruling on the **MCI** requires platforms to release annual transparency reports detailing content notifications and information about paid advertising.[113]

Morocco's upcoming online platform regulation will reportedly require platforms to periodically report on their moderation systems, complaint handling processes and content removals, inspired by transparency provisions in the **EU-DSA**.[114]

In Nigeria, the **Code of Practice** requires platforms to publish clear terms of service and to provide scientists, academics, journalists, CSOs and government agencies access to necessary data to facilitate research countering disinformation.[115] The white paper on the forthcoming **OHPB** also emphasises transparency reporting as a central mechanism of platform accountability, outlining anticipated responsibilities for platforms to publish their risk assessments, harmful and illegal content reports and effectiveness of their content moderation mechanisms.[116]

In **India**, the **IT Rules** (2021) require certain social media companies to publish monthly compliance reports, complaints received, actions taken, content removal, automated tools, or "any other relevant information" as may be specified.[117] These requirements could be expanded in the **DIA** to include information on content moderation practices, particularly regarding online platforms' language capabilities across India's 700 languages.[118]

6.3.2 Procedures for Redress

A-OSA	UK-OSA	EU-DSA
Platforms must have mechanisms for user complaints about breaches of the terms of use or platform policies and must have procedures for dealing with such reports and complaints. Platforms must also inform users how to make complaints to the Commissioner [BOSE 14-16].	Platforms must establish effective procedures for users to flag illegal content, to appeal moderation decisions, including clear channels for complaints. [Sections 20 and 21].	Platforms must have mechanisms for users to notify illegal content and seek redress when affected by content moderation decisions, ensuring users can contest and seek review of such actions. [Articles 16,17, and 20].

The **MCI** has long required platforms to inform Brazilian users when their content is removed because of a court order, enabling appeals.[119] The recent Supreme Court judgement expands these duties, requiring platforms to provide accessible notification systems and clear mechanisms for users to challenge content restrictions.[120]

The Nigerian **Code of Practice** requires platforms to provide users and government agencies with accessible complaints and reporting mechanisms, and the forthcoming **OHPB** is expected to strengthen these requirements.[121] The white paper also recommends the creation of a special Centre for Online Harms Research and Coordination, which will help to facilitate redress processes for individuals or entities affected by harmful content or behaviour online.[122]

Indonesia's **GR17/2025** requires platforms to establish reporting mechanisms to address misuse of products, services or features that may violate children's rights; information about these mechanisms and the terms of service should be provided in the Indonesian language, using a format that is understandable and accessible.[123]

Pakistan's Prevention of Electronic Crimes (Amendment) Act 2025 requires online platforms to provide complaint redress mechanisms against unlawful or offensive content, but also to establish a Social Media Complaint Council with the capacity to handle social media complaints and user appeals.[124] The Act and its 2025 amendments have been widely criticized by the media and digital rights organisations for facilitating overbroad government overreach to suppress political dissent and stifle freedom of expression[125]

6.3.3 Age Assurance

A-OSA	UK-OSA	EU-DSA
Certain social media platforms are now required to take reasonable steps to make sure under-16s cannot create or keep accounts. [Section 4A].	All service providers which allow pornographic content must implement age assurance mechanisms to ensure that children are not able to encounter such content. [Section 81]. Age verification is listed as a potential measure that platforms may take to fulfil child safety duties [Article 12 (7)].	While the DSA requires online platforms to take steps to ensure high levels of privacy and safety of minors, they are not obliged to process additional personal data to assess whether a user is a minor or not. [Article 28]. Age verification is listed as a potential measure that platforms may take to protect the rights of the child [Article 35].

Indonesia's **GR17/2025** is almost exclusively focused on children's online safety, requiring platforms to assess the risks of children accessing their services and then establish a minimum age requirement based on the risks identified. Under the new regulations, platforms must also implement robust age verification mechanisms and parental consent mechanisms for users under 18.[126]

While **Morocco's** upcoming platform regulation is inspired by the **EU-DSA**, reports from Moroccan authorities indicate that the framework will place much more emphasis on protecting minors than the **EU-DSA**. The new regulation is expected to require content classification by age, parental control tools, and restrictions on ads targeting children or promoting harmful products.[127]

The Nigerian white paper on the upcoming **OHPB** clearly reflects the **A-OSA** and **UK-OSA** approaches to child safety. The **OHPB** will require all platforms to implement age assurance and verification mechanisms to prevent underage access and safeguard minors from age-inappropriate content. It will also require platforms to develop robust parental supervision features, time limits, and stricter privacy settings for children.

Chile's Digital Platforms Regulation Bill N° 14.561-19 of 2021 proposed the introduction of "appropriate age verification mechanisms" and protective measures for children, including content warnings and age-appropriate content filters (Article 8). At the time, civil society organisations raised concerns about the need for excessive data collection that such a requirement would impose, threatening anonymity and privacy online.[128]

6.4 Regulatory mechanisms

6.4.1 Regulatory Oversight and Independence

A-OSA	UK-OSA	EU-DSA
The eSafety Commissioner is an independent statutory office supported by the Australian Communications and Media Authority, an independent statutory regulator funded primarily by licensing fees. The Commissioner is responsible for administering complaints systems for prohibited content, coordinating Australia's Online Safety efforts and issuing notices and requests to online platforms.	The UK-OSA is overseen by the UK's independent Telecommunications Regulator, Ofcom, which is funded primarily by fees from regulated entities, including online platforms [Section 84]. Under the UK-OSA, Ofcom must prepare and issue codes of practice for online platforms that set out how they can meet their duties, categorise online platforms according to the UK-OSA and assess the risks posed by certain platforms.	Member States must nominate DSCs with the necessary resources to implement the DSA completely independently from public authorities and private parties [Article 30]. They can request access to data, order inspections and certify "trusted flaggers" from regular platforms. The European Commission has investigative and sanctioning powers for VLOPs and VLOSEs.

In Brazil, the original draft of the **FNB** proposed the multi-stakeholder Brazilian Internet steering committee as a monitoring body; however, it is a voluntary, budget-constrained organisation subject to interference by presidential decree, rendering it inappropriate for the scope of duties now foreseen for online platforms in the Supreme Court's recent judgment.[129] The Supreme Court have instead suggested the National Data Protection Authority as a possible institution with the requisite mandate and expertise to oversee a future platform regulatory framework.[130]

Nigeria's white paper on the prospective **OHPB** foresees that the regulation will be implemented by a multi-stakeholder Centre for Online Harms Research, Prevention and Coordination, which will oversee and enforce the obligations created in the bill and coordinate the response of public agencies. The Centre will include representatives from the Nigerian Police, the Nigerian Human Rights Commission (NHRC), and other government agencies and independent national institutions.

In Indonesia, MOCDA supervises platform compliance with the **Electronic Systems and Transactions Rules** and related regulations. MOCDA may receive and investigate complaints, examine platforms, access systems and documentation, summon providers for clarifications, and impose administrative sanctions.

Sri Lanka's **OSA** established a new Online Safety Commission (OSC), a five-member body nominated by the President and approved by the Constitutional Council. The OSC is responsible for investigations, enforcement, and advising the government on subsequent regulations.[131]

In **India**, MeitY and the Ministry of Information and Broadcasting administer the **IT Rules** and will likely also oversee the upcoming **DIA**.[132] MeitY have the power to introduce fines, restrictions and even criminal liability for social media managers for non-compliance.

6.4.2 Providing Information to the Regulator

A-OSA	UK-OSA	EU-DSA
Reporting Requirements		
Online platforms can be required by the Commissioner to report on their compliance with the Expectations [Section 49, 56], or provide documents or information relating to specific investigations [Part 14].	Online platforms are required to produce annual transparency reports as directed by Ofcom. Ofcom can also require specific information from online platforms to help them assess compliance with the UK-OSA or investigate the death of a child, and can also request reports, investigations and audits [Section 77].	VLOPs and VLOSEs must conduct annual independent audits and transmit them to the DSC jointly with a report setting out the results of the systemic risk assessments mandated by Article 34 [Article 42].
Local Presence and Responsiveness to Government Authorities		
There is no legal requirement for platforms to have a local presence; however, the statutory review[133] of the A-OSA recommends requiring major online platforms to establish domestic legal presence in Australia as a condition of operating in the country.	There is no legal requirement for platforms to have a local presence, but Ofcom can require online platforms to name a senior manager who is in a position to comply with information requests [Section 103].	Online platforms which do not have establishments in the EU but which offer services to EU users must appoint a legal representative with a physical address in at least one EU member state [Article 13].

The Brazilian Supreme Court ruling on the **MCI** requires that online platforms operating in Brazil must establish and maintain headquarters and a representative in the country, with authority to respond to legal and judicial requests, and to provide competent authorities with information on the platform's operations, content moderation and complaint procedures, and risk management processes.[134]

Under Nigeria's **Code of Practice**, online platforms are required to file annual reports with NITDA specifying details about their number of users, content removal and appeal statistics, and efforts to protect children and adults from harmful content, including misinformation and disinformation. Platforms with more than 100,000 Nigerian users are also required to be incorporated and have a physical address in Nigeria, to appoint a Liaison Officer, and provide information on content moderation procedures to government agencies when required.

Morocco's upcoming regulation for online platforms will reportedly allow the High Authority for Audiovisual Communication (HACA) to monitor platforms even without a physical presence in Morocco. There are also chances that a requirement for a local representative could be included in the regulation. HACA will reportedly be able to demand periodic reports on content moderation policies, complaint handling mechanisms, and statistics on removed content.[135]

6.4.3 Penalties and Compliance

A-OSA	UK-OSA	EU-DSA
The Commissioner can issue removal notices, blocking notices, and directions to comply with industry codes. Where an infringement occurs, the Commissioner can give platforms formal warnings or notices and seek court-ordered injunctions or civil penalties.	Non-compliance with the UK-OSA can result in fines of up to £18 million or 10% of global turnover, whichever is greater. Ofcom can also hold companies and senior managers criminally liable for failure to comply with regulatory interventions. Ofcom can also prohibit access to non-compliant services in the UK, subject to judicial approval [Schedule 13].	Non-compliance with the DSA can result in fines of up to 6% of global turnover. The DSC may request judicial permission to temporarily restrict access to non-compliant services [Article 58].

In Indonesia, MOCDA has authority under the **Electronic Information and Transaction Law** and related regulations to issue written warnings and temporary suspensions, or terminate services altogether – powers which it has used extensively in the past.[137]

Under Sri Lanka's **OSA**, if online platforms do not comply with takedown orders from the Commission, the Commission can apply for a court order for the removal of the content in question. If the online platform does not comply with the court order, the owner or operator of the social media platform can be held criminally liable, and the Commission can block the platform entirely.[138]

Under the **IT Rules**, relevant state agencies in India can block access to a broad range of prohibited content types without a court hearing.[139] These powers have been extensively used by authorities; for example, during COVID-19, the government ordered Meta and X to take down or block content that criticized the government's handling of the pandemic on grounds of being either misleading or false content.[140]

In December 2024, Vietnam implemented Decree 147/2024, a new regulatory framework for online platforms and online content. The Decree included requirements for online platforms to provide the Vietnamese Ministry of Information and Communications (MIC) with access to user data and access to platforms' internal search and scanning tools to identify offending content. The law has been described as "draconian" by human rights groups, given its sweeping restrictions on online expression and overbroad powers given to government authorities to censor online speech.[136]

6.5 Consideration of human rights

6.5.1 References to human rights

A-OSA	UK-OSA	EU-DSA
There are no specific references to online platforms' duties regarding human rights.	Protecting users' rights to freedom of expression and privacy is a core duty imposed on online platforms under the UK-OSA [Section 1, 22, 33].	Online platforms are required to have due regard to human rights in the enforcement of their terms of service [Article 14] and to analyze the potential impact of their services on fundamental rights in their efforts to assess and mitigate risks [Articles 34, 35]. The Commission must also have due regard for fundamental rights in the exercise of their responsibilities.

Brazil's approach to platform regulation has been guided by a central commitment to safeguarding human rights online. The **MCI** itself affirms that Internet use in Brazil should be based on respect for freedom of expression and other human rights, and emphasises the right of all to access the Internet, to access information, to participate in cultural life and to privacy. In the recent ruling on the **MCI**, the Supreme Court held that Article 19 was unconstitutional because it failed to provide adequate protection for fundamental rights and democratic freedoms. This human-rights-driven approach to regulating online platforms closely mirrors the principles underpinning the **EU-DSA**.[141]

In India, MeitY's proposals for the **DIA** list protection of citizens' rights as one of seven core goals of the proposed regulation. Publicly available material outlining the approach to the **DIA** also mentions the rights to be forgotten, to redress and to non-discrimination.[142]

The Sri Lankan **OSA** makes no mention of rights and democratic freedoms, even in relation to the Commission's enforcement duties.[143]

6.5.2 Freedom of Expression

A-OSA	UK-OSA	EU-DSA
The Act may not infringe upon the constitutional freedom of political communication [Section 233].	Ofcom must consider the impact of their decisions and codes on users' rights to freedom of expression [Sections 41 & 42]. Eligible entities can make super-complaints to Ofcom if they believe that an online platform is significantly adversely affecting individuals' rights to freedom of expression [Section 169].	Online platforms must respect the freedom of expression of their users [Articles 14, 17] and VLOPs and VLOSEs must assess risks to freedom of expression and information, including the freedom and pluralism of the media, in their systemic risk assessments [Article 34].

Nigeria's white paper on the **OHPB** emphasises the importance of protecting fundamental human rights, including free speech, freedom of association, political participation, and privacy. The **OHPB** will be designed to avoid overly restrictive measures that could stifle legitimate expression, drawing on best practices for content moderation requirements and proportionate penalties from the Manila Principles and international human rights standards. Larger platforms will also have obligations to protect content with civic, democratic or journalistic significance.[144]

- While no draft is publicly available yet, **Morocco's** Minister for Culture, Youth and Communication has indicated that protecting freedom of expression will be central to the proposed regulatory approach for online platforms, citing the need to balance public safety concerns with protection of legitimate speech.[145]

- MeitY claim that disinformation is being "weaponized" in the name of free speech in India, and proposes that the upcoming **DIA** should address discretionary moderation of fake news by online platforms, which infringes on individuals' freedom of expression.[146]

6.5.3 The Rights of the Child

A-OSA	UK-OSA	EU-DSA
The Commissioner must have regard to the CRC in the performance of its function [Section 24].	There is no explicit reference to the rights of the child.[147]	VLOPs and VLOSEs must assess risks to the rights of the child in their systemic risk assessments [Article 34], and take targeted measures to protect these rights, including age verification and parental control tools [Article 35].

Indonesia's **GR17/2025** requires online platforms to implement measures that protect children's personal data and uphold their digital rights, including implementing mechanisms for users to report content that risks children's rights.[148]

The Nigerian white paper on the **OHPB** specifically notes the relevance of Nigeria's Act on the Rights of the Child (2003) to the online environment. The proposal for the **OHPB** also includes a Child Online Protection Strategy, which would specifically focus on the needs of child users through age verification and parental control mechanisms.

7. | Discussion

The comparative analysis reveals areas of significant convergence between Global North and Global Majority approaches to online platform regulation. In several cases, there is explicit evidence of policy transfer, with lawmakers examining and citing the Global North regulations as models or examples when drafting their own frameworks. The **EU-DSA**'s strong auditing and transparency obligations, in particular, have established a global precedent by compelling platforms to make provisions for these obligations, meaning that policymakers in other jurisdictions can also make similar demands of online platforms by pointing to the **EU-DSA** as a precedent.[149] Similarly, the systemic, risk-based approach to managing online harms demonstrated by the Global North regulations is now being mirrored across many emerging platform regulations worldwide.

However, even where provisions look similar on paper, their impact in practice may differ sharply in Global Majority and Global North contexts. Effective enforcement of platform obligations depends on regulatory independence, institutional capacity and technical and legal resources. In countries such as India, Indonesia and Sri Lanka, regulators are closely tied to government, enabling censorship of political dissent and marginalized voices under the guise of "online safety".[150] Weak or absent human rights safeguards in the regulations compound these risks. For example, India's **IT Rules (2021)** introduce user-tracing requirements that pose risks to individuals' right to privacy and have a chilling effect on freedom of expression,[151] and statements from Moroccan authorities indicate that they may require platforms to monitor all user communications for illegal and harmful content in their upcoming regulation for online platforms.[152] Both measures starkly contradict the rights-respecting principles that policymakers in these jurisdictions claim to emulate (See Section 6.5), illustrating how policymakers may make rhetorical commitments to human rights while implementing frameworks which undermine them.

There are three areas in particular which pose concerns for how Global North provisions may be adopted and implemented in Global Majority contexts:

- Shifting towards **a systemic duty of care or due diligence requirement** for online platforms to address illegal and harmful content can help establish clearer accountability frameworks and incentivise proactive risk management. However, such approaches risk overbroad or vague obligations that may incentivise platforms to overcensor if the obligations

are not carefully defined. For example, the **UK-OSA's** duty of care principles significantly influenced the Nigerian approach to risk management and mitigation. However, the proposed duty of care for the **OHPB** echoes the more classical duty of care for online platforms proposed in the original UK Online Harms White Paper, whereas the final version of the duty of care defined in the **UK-OSA** is more specific and proportionate to prevent excessive burdens on online platforms and safeguard freedom of expression.

- Introducing **obligations for platforms to share information with regulators** helps to increase transparency and enable effective oversight. Particularly for Global Majority countries, provisions requiring platforms to have local contact points or offices may be essential for establishing open communications with companies which have traditionally been unresponsive to regulatory enquiries or complaints from users. However, without clearly defined limits, accountability mechanisms and safeguards, such requirements may result in governments placing undue pressure on local staff to comply with unlawful or politically motivated demands, or requesting sensitive user information, undermining individuals' human rights.
- Measures to **protect children from harmful content online** are gaining traction, but age verification is a complex issue that introduces huge risks for user privacy and access to legal content online by individuals who do not want to be identified for legitimate reasons or lack the credentials to interact with the system.[153] The **UK-OSA's** age verification requirements and **Australia's** proposed ban on under-16 social media use have drawn sharp criticism for jeopardizing privacy and restricting legitimate access.[154] In contrast, the **EU-DSA** treats age verification as part of due diligence, paired with efforts to develop privacy-preserving tools such as the Digital Identity Wallet and an open-source verification kit.[155] While resource-intensive, this model points to ways Global Majority countries might better reconcile child protection with privacy and access considerations.

8. | Recommendations

The comparative analysis of Global North and Global Majority approaches demonstrates the need to balance platform accountability and user safety with the protection of fundamental freedoms. Without robust rights, safeguards and independent oversight, platform regulation risks becoming a vehicle for control rather than empowerment in many Global Majority contexts. Drawing on these findings, the following recommendations outline key principles to guide policymakers, regulators, and civil society in designing frameworks that strengthen accountability while safeguarding fundamental rights:

1
Anchor platform regulation in human rights

Platform regulations should be designed first and foremost to safeguard the fundamental rights of individuals –rather than to serve corporate interests or provide cover for authoritarian overreach. States should draw on the UN Guiding Principles on Business and Human Rights (UNGPs) to ensure that regulations require online platforms to respect human rights while also creating an enabling environment for freedom of expression, privacy, political participation, and non-discrimination. Regulations which require platforms to weaken encryption or impose intrusive age assurance requirements risk undermining individuals' human rights and may disproportionately impact vulnerable groups who lack accredited credentials or wish to remain anonymous online.

2
Align with global norms and frameworks

International standard-setting bodies are already shaping best practices for platform governance. Relevant initiatives include UNESCO's Guidelines for the Governance of Digital Platforms[156] and the Global Forum of Regulators.[157] The Global Online Safety Regulators Network is also rapidly becoming a source of normative guidance for independent regulators around the world.[158] Borrowing selectively from individual state-based models risks importing inappropriate provisions; instead, states should draw from these emerging loci of international consensus, adapting guidelines to their specific political, legal and cultural contexts.

3
Contextualise regulatory approaches

Copying Global North frameworks without adaptation may lead to very different – and potentially harmful –outcomes in Global Majority contexts.[159] Internet penetration rates, patterns of online use, levels of digital literacy, platform dominance, and the strength of constitutional safeguards vary significantly across regions. Regulatory design must be tailored to these realities to avoid unintended consequences, including restrictions on access, privacy violations, or disproportionate burdens on smaller platforms. One key element for achieving a balanced regulation, as seen in the Global North experiences and global guidance, is adopting a systemic approach that addresses the structural elements for platforms to deal with systemic risks, without focusing on specific pieces of content.

4
Establish an enabling regulatory ecosystem

Governments should seek to build an enabling regulatory ecosystem encompassing personal data protection, electoral regulation, consumer protection and competition law to ensure that regulatory incentives for platforms align with respect for human rights. The current attention-driven business models of online platforms have resulted in the widespread collection and use of data by online platforms. Data concentrated by dominant platforms is used to personalize experiences and keep audiences engaged, even at the expense of prioritizing content that can be harmful to the exercise of human rights; such practices are the underlying causes of many of the problems that platform regulations are designed to address. While many countries still lack baseline protections in these areas, there is a need to ensure that any attempt to address platforms' impacts on information ecosystems must be underpinned by holistic and effective privacy and data governance rules. This holistic approach, which acknowledges the interaction of online content regimes with the broader regulatory ecosystem, will be essential to underpin any credible system of platform regulation and to guard against misuse of user data in the name of safety or compliance.[160]

5

Create independent and well-resourced regulators

Regulation will fail without effective oversight bodies. States should establish, or adequately resource existing independent regulators – such as data protection authorities, telecommunications regulators, electoral bodies, or ombudspersons – ensuring they have the mandate and capacity to enforce platform obligations.[161] In particular:

- Appointments of individuals to the regulatory body should follow clear, transparent, and merit-based processes.
- Regulators must be accountable to parliaments or independent oversight mechanisms, not to the executive branch.
- Regulatory decisions should be subject only to judicial appeal, safeguarding independence.

6

Require transparency from online platforms

Regulation should require greater transparency from online platforms around their policies and services, data handling practices, and decision-making processes. This allows states and users to understand the risks they may pose to human rights, and hold them accountable for ineffective or discriminatory practices, such as disproportionate content moderation practices. Online platforms should be required to develop fair, straightforward and transparent oversight mechanisms for removal requests and appeals, in line with the Santa Clara Principles on Transparency and Accountability in Content Moderation.[162]

7

Adopt inclusive, multi-stakeholder processes

Effective regulation must involve diverse perspectives from the outset. Governments should include civil society, academia, journalists, and technical experts in consultations, as well as those communities most affected by digital harms and repression – such as women, LGBTQ+ individuals, ethno-religious minorities, and rural populations.[163] This approach ensures that platform regulations respond to real harms while safeguarding against reinforcing systemic inequalities. In particular, independent national human rights institutions should play a central role in both drafting and enforcing platform regulations. Their involvement helps ensure that frameworks remain anchored in international standards and not captured by political agendas. The establishment of data

access for research rules benefits evidence-based interventions and allows a range of stakeholders to contribute to improving online platform regulation.

8
Carefully calibrate duty of care frameworks

Duty of care obligations can help ensure platforms act responsibly, but poorly designed frameworks risk incentivising over-removal of content and chilling legitimate expression. States must carefully balance platform accountability with protections for freedom of expression and media pluralism.

9
Enhance the resilience of the information ecosystem

Supporting independent, economically viable and pluralistic journalism and media, and promoting information and media literacy are key to building a sustainable and healthy information environment. This includes equitable monetization schemes, prioritizing rigorous independent journalism in users' feeds over clickbait articles, strengthening user control features, and integrating third-party fact-checking and content provenance mechanisms.

10
Foster transnational dialogue and Global Majority leadership

The establishment of initiatives such as the *Global Majority House* in Brussels illustrates the importance of South–South and South–North collaboration in shaping the future of digital governance.[164] Regulators, civil society, and researchers from the Global Majority should leverage such spaces to influence how major frameworks like the EU-DSA are implemented and to ensure that Global North regulatory norms are not simply exported uncritically.

Footnotes

1 Anu Bradford, The Brussels effect: How the European Union rules the world, Oxford University Press, 2019, https://academic.oup.com/book/36491; Annegret Bendiek & Isabella Stuerzer, "The Brussels effect, European regulatory power and political capital: Evidence for mutually reinforcing internal and external dimensions of the Brussels effect from the European digital policy debate," Digital Society, 2(1), 5, 23 January 2023, https://link.springer.com/article/10.1007/s44206-022-00031-1.

2 The term "Global North" refers here to rich, industrialised countries with high levels of education and internet penetration. These are also referred to as W.E.I.R.D. societies (Western, Educated, Industrialised, Rich and Democratic); see Joseph Henrich, Steven Heine & Ara Norenzayan, "Beyond WEIRD: Towards a broad-based behavioral science," Behavioral and brain sciences, 33(2-3), 111, 15 June 2010, https://www.cambridge.org/core/journals/behavioral-and-brain-sciences/article/beyond-weird-towards-a-broadbased-behavioral-science/D85708615F8516EB1B9D4332D1669A72.

3 "The World by Income and Region," The World Bank, https://datatopics.worldbank.org/world-development-indicators/the-world-by-income-and-region.html (accessed 4 September 2025).

4 By using the term "Global Majority", we seek not to simplify the differences between countries in this group but to emphasise shared economic and political concerns that many Global Majority countries share with regards to regulating online platforms, and to highlight potential differences with Global North worldviews. See Rosemary Campbell-Stephens, "Investing in diversity: Changing the face (and the heart) of educational leadership," School Leadership and Management, 29(3), 321-331, July 2009, https://eric.ed.gov/?id=EJ871005; Soizic Le Courtois, Chika R. Ezeugwu, Dina D. Fajardo-Tovar, Stephanie K. Nowack, Domnick O. Okullo, Stephen Bayley, "Learning through play in Global Majority countries: reflections from the PEDAL centre on understanding and adapting the concept in four different contexts", International Journal of Play, 13(3), 228-253, 23 August 2024, https://www.tandfonline.com/doi/full/10.1080/21594937.2024.2388952.

5 UN Human Rights Council (UNHRC), "Resolution on the promotion, protection and enjoyment of human rights on the Internet", A/HRC/RES/20/8, 2012, https://ap.ohchr.org/documents/dpage_e.aspx-?si=a/hrc/res/20/8; UNHRC, "Resolution on the promotion, protection and enjoyment of human rights on the Internet", A/HRC/RES/26/13, 2014, https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/26/13; UNHRC, "Resolution on the promotion, protection and enjoyment of human rights on the Internet", A/HRC/RES/32/13, 2016, https://ap.ohchr.org/documents/dpage_e.aspx?si=a/hrc/res/32/13; UN General Assembly (UNGA), "Promotion and protection of the right to freedom of opinion and expression", A/66/290, 2011, https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/A.66.290.pdf, para 15.

6 Office of the United Nations High Commissioner for Human Rights (OHCHR), "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework", 2011, https://www.ohchr.org/sites/default/files/documents/publications/guiding-principlesbusinesshr_en.pdf.

7 ICCPR, Article 19.

8 UNGA, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression", A/71/373, 2016, https://www.refworld.org/reference/themreport/unga/2016/en/112959, para. 28.

9 "What is Freedom of Expression?" ARTICLE 19, https://www.article19.org/what-is-freedom-of-expression/, accessed 4 September 2025.

10 Reuters, "Myanmar: UN blames Facebook for spreading hatred of Rohingya", The Guardian, 13 March 2018, https://www.theguardian.com/technology/2018/mar/13/myanmar-un-blames-facebook-for-spreading-hatred-of-rohingya; Kalkidan Yibeltal & Wycliffe Muia, "Facebook's algorithms 'supercharged' hate speech in Ethiopia's Tigray conflict", BBC News, 31 October 2023, https://www.bbc.co.uk/news/world-africa-67275219; Jane Wakefield, "Christchurch shootings: Social media races to stop attack footage", BBC News, 16 March 2019, https://www.bbc.co.uk/news/technology-47583393.

11 "UNESCO report spotlights harmful effects of social media on young girls", UN News, 25 April 2024, https://news.un.org/en/story/2024/04/1149021.

12 OHCHR, "Guiding Principles on Business and Human Rights: Implementing the United Nations 'Protect, Respect and Remedy' Framework".

13 UNESCO, "Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach", 2023, https://www.unesco.org/en/internet-trust/guidelines.

14 Manila Principles on Intermediary Liability, 2015, https://manilaprinciples.org/index.html.

15 The Santa Clara Principles on Transparency and Accountability in Content Moderation, 2018, https://santaclaraprinciples.org/.

16 Global Network Initiative Principles on Freedom of Expression and Privacy, 2018, https://globalnetworkinitiative.org/wp-content/uploads/2018/04/GNI-Principles-on-Freedom-of-Expression-and-Privacy.pdf.

17 "Children, online safety, and age verification", Parliament of Australia, 21 August 2024, *https://www.aph.gov.au/About_Parliament/Parliamentary_departments/Parliamentary_Library/Research/Research_Papers/2024-25/Children_online_safety*.

18 *Enhancing Online Safety for Children Act 2015*, Parliament of Australia, *https://www5.austlii.edu.au/au/legis/cth/num_act/eosfca2015321/*.

19 "Harm being done to Australian children through access to pornography on the Internet", Commonwealth of Australia, 23 November 2016, *https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Environment_and_Communications/Onlineaccesstoporn45/Report*; Antonia Quadara, Alissar El-Murr and Joe Latham, "The effects of pornography on children and young people: an evidence scan", Australian Institute of Family Studies, 1 January 2017, *https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22library%2Flcatalog%2F012O5115%22*; "Parenting and Pornography: Findings from Australia, New Zealand and the United Kingdom", eSafety Research, 10 December 2018, *https://www.esafety.gov.au/research/digital-parenting/pornography*; "Protecting the age of innocence", Commonwealth of Australia, February 2020, *https://www.aph.gov.au/Parliamentary_Business/Committees/House/Social_Policy_and_Legal_Affairs/Onlineageverification*.

20 Lynelle Briggs, "Report of the Statutory Review of the Enhancing Online Safety Act 2015 and the Review of Schedules 5 and 7 to the Broadcasting Services Act 1992 (Online Content Scheme)", Commonwealth of Australia, 2018, https://www.infrastructure.gov.au/sites/default/files/briggs-report-stat-review-enhancing-online-safety-act2015.pdf.

21 *Online Safety (Basic Online Safety Expectations) Determination 2022,* Parliament of Australia, https://www.legislation.gov.au/F2022L00062/latest/text.

22 *Age Assurance Technology Trial,* https://ageassurance.com.au/ (accessed 4 September 2025).

23 Delia Rickard, "Report of the Statutory Review of the Online Safety Act 2021", Commonwealth of Australia, 2024, *https://www.infrastructure.gov.au/department/media/publications/report-statutory-review-online-safety-act-2021.*

24 "Online Harms White Paper", Department for Digital, Culture, Media and Sport (DCMS) and Home Office, 2019, https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper.

25 "Online Harms White Paper: Full government response to the consultation", DCMS and Home Office, 15 December 2020, https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response.

26 "Online harms: interim codes of practice", DCMS and Home Office, 15 December 2020, https://www.gov.uk/government/publications/online-harms-interim-codes-of-practice.

27 "Quick guide to illegal content codes of practice", Ofcom, 9 November 2023, https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/codes-of-practice.

28 "Quick guide to Protection of Children Codes", Ofcom, 7 May 2024, https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/quick-guide-to-childrens-safety-codes.

29 Yasmin Afina, Marjorie Buchser, Alex Krasodomski, Jacqueline Rowe, Nikki Sun and Rowan Wilkinson, "Towards a global approach to digital platform regulation", Chatham House and Global Partners Digital, January 2024, https://www.chathamhouse.org/sites/default/files/2024-01/2024-01-17-towards-global-approach-digital-platform-regulation-afina-et-al.pdf; Thales Martini Bueno and Renan Gadoni Canaan, "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), June 2024, https://www.sciencedirect.com/science/article/pii/S0308596124000545; Bendiek & Stuerzer, "The Brussels effect, European regulatory power and political capital", 2023.

30 Gwen Hinze, "EU Court of Justice: Social Networks Can't Be Forced to Monitor and Filter to Prevent Copyright Infringement", Electronic Frontier Foundation, 17 February 2012, https://www.eff.org/deeplinks/2012/02/eu-court-justice-social-networks.

31 "The enforcement framework under the Digital Services Act," European Commission, 12 February 2025, https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement.

32 The European Board for Digital Services, https://digital-strategy.ec.europa.eu/en/policies/dsa-board#_blank (accessed 4 September 2025).

33 The European Centre for Algorithmic Transparency, https://algorithmic-transparency.ec.europa.eu/index_en#_blank (accessed 4 September 2025).

34 Polona Car, "Enforcing the Digital Services Act: State of play", European Parliament Research Services, 21 November 2024, https://epthinktank.eu/2024/11/21/enforcing-the-digital-services-act-state-of-play/; DSA whistleblower tool, https://digital-strategy.ec.europa.eu/en/policies/dsa-whistleblower-tool (accessed 4 September 2025).

35 Jordi Calvet-Bademunt, "Digital Services Act Roundup: June – July 2024", Tech Policy Press, 6 August 2024, https://www.techpolicy.press/digital-services-act-roundup-june-july-2024/.

36 Emmanuel Akinwotu, "Nigeria lifts Twitter ban seven months after site deleted president's post", The Guardian, 13 January 2022, https://www.theguardian.com/world/2022/jan/13/nigeria-lifts-twitter-ban-seven-months-after-site-deleted-presidents-post; Ben Derico & Ione Wells, "Brazil lifts ban on Musk's X after it pays $5m fine", BBC News, 8 October 2024, https://www.bbc.com/news/articles/c5y06vzk3yjo; "TikTok Still Blocked: Government Sources On Buzz About Ban Being Lifted", NDTV, 22 August 2025, https://www.ndtv.com/india-news/tiktok-still-blocked-government-sources-on-buzz-about-ban-being-lifted-9141725.

37 *Marco Civil Law of the Internet in Brazil, Law No. 12.965*, Presidency of the Republic of Brazil, 23 April 2014, https://www.cgi.br/pagina/marco-civil-law-of-the-internet-in-brazil/180.

38 Francisco Brito Cruz, Beatriz Kira and Ivar A. Hartmann, "Duty of care and regulation of digital platforms: a Brazilian perspective", University of Sussex, January 2025, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5176187 p.103; Carolina Rossini, Francisco Brito Cruz and Danilo Doneda, "The Strengths and Weaknesses of the Brazilian Internet Bill of Rights: Examining a Human Rights Framework for the Internet," CIGI and Chatham House, September 2015, https://www.cigionline.org/static/documents/no19_0.pdf.

39 James Görgen, "Brazil Has a Bridge to Defending the Internet", Tech Policy Press, 18 July 2025, https://www.techpolicy.press/brazil-has-a-bridge-to-defending-the-internet/.

40 Veridiana Alimonti, "Brazil's Internet Intermediary Liability Rules Under Trial: What Are the Risks?", Electronic Frontier Foundation, 11 December 2024, https://www.eff.org/deeplinks/2024/10/brazils-internet-intermediary-liability-rules-under-trial-what-are-risks.

41 Bueno and Canaan, "The Brussels Effect in Brazil," 2024.

42 *Projeto de Lei nº 2630/2020*, Câmara dos Deputados, 3 July 2020, https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2256735.

43 Brito Cruz, Kira and Hartmann, "Duty of care and regulation of digital platforms," 2025.

44 Alimonti, "Brazil's Internet Intermediary Liability Rules Under Trial," 2024.

45 "Brazil: The Supreme Court (STF) establishes that Article 19 of the Brazilian Internet Legal Framework is partially unconstitutional, creating a new regime of civil liability," Baker McKenzie, 1 July 2025, https://insightplus.bakermckenzie.com/bm/intellectual-property/brazil-the-supreme-court-stf-establishes-that-article-19-of-the-brazilian-internet-legal-framework-is-partially-unconstitutional-creating-a-new-regime-of-civil-liability.

46 "Brazil: The STF establishes that Article 19 of the Brazilian Internet Legal Framework is partially unconstitutional," Baker McKenzie, 2025.

47 Fernando Galucci, "Brazilian Supreme Court modifies the Internet Civil Framework and expands platform liability", Cham-

bers and Partners, 21 July 2025, https://chambers.com/articles/brazilian-supreme-court-modifies-the-internet-civil-framework-and-expands-platform-liability.

48 Bueno and Canaan, "The Brussels Effect in Brazil," 2024, p. 9, 13.

49 Ibid, p.8.

50 *The Information Technology Act 2000,* Ministry of Law, Justice and Company Affairs of the Government of India, 9 June 2000, https://www.MeitY.gov.in/static/uploads/2024/03/ITbill_2000.pdf.

51 *The Information Technology (Procedure and Safeguards for Blocking for Access of Information by Public) Rules, 2009,* Ministry of Electronics and Information Technology, Central Government of India, 27 October 2009, https://www.MeitY.gov.in/static/uploads/2024/10/91f628cb778f94e76df356bc3fd3ac60.pdf

52 *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021,* Ministry of Electronics and Information Technology, Central Government of India, 25 February 2021, https://www.MeitY.gov.in/static/uploads/2024/02/Information-Technology-Intermediary-Guidelines-and-Digital-Media-Ethics-Code-Rules-2021-updated-06.04.2023-.pdf

53 "India: New Amendment to the Information Technology Rules that Threatens Press Freedoms must be Withdrawn", Access Now, 2 May 2023, https://www.accessnow.org/press-release/withdraw-india-it-rules/;

54 Ibid.; "End the wave of digital censorship in India," Association for Progressive Communications, 11 June 2021, https://www.apc.org/en/pubs/end-wave-digital-censorship-india.

55 "Proposed Digital India Act, 2023", Ministry of Electronics and Information Technology (MeitY), Central Government of India, 9 March 2023, https://www.tcs.com/content/dam/tcs/pdf/discover-tcs/investor-relations/faq/proposed-digital-india-act.pdf.

56 Tejasi Panjiar and Prateek Waghre, "Many mysters of 'Digital India Bill'", Internet Freedom Foundation, 20 February 2023, https://internetfreedom.in/many-mysteries-of-the-digital-india-bill/.

57 "Proposed Digital India Act, 2023", MeitY.

58 Aahil Sheikh, "Transparency Must be a Cornerstone of the Digital India Act", Tech Policy Press, 23 April 2024, https://www.techpolicy.press/transparency-must-be-a-cornerstone-of-the-digital-india-act/; Sanhita Chauriha, "Explained: The Digital India Act 2023", Vidhi Centre for Legal Policy, 8 August 2023, https://vidhilegalpolicy.in/blog/explained-the-digital-india-act-2023/.

59 Emmanuel Akinwotu, "Nigeria lifts Twitter ban seven months after site deleted president's post", 2022.

60 *Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries,* Nigerian National Information Technology Development Agency (NITDA), October 2022, https://nitda.gov.ng/wp-content/uploads/2022/10/APPROVED-NITDA-CODE-OF-PRACTIVE-FOR-INTERACTIVE-COMPUTER-SERVICE-PLATFORMS-INTERNET-INTERMEDIARIES-2022-002.pdf.

61 "Nigeria: NITDA Code of Practice must comply with International Human Rights Law," Amnesty International, 24 June 2022, https://www.amnesty.org/en/documents/afr44/5818/2022/en/; "Civil Society Coalition Memo to the National Information Technology Development Agency (NITDA) on the Draft Code of Practice for Interactive Computer Service Platforms/Internet Intermediaries", Paradigm Initiative, 24 June 2022, https://paradigmhq.org/wp-content/uploads/2022/06/NITDA-Code-Response-Memo.pdf.

62 *White Paper on the Framework for an Online Harms Protection Bill in Nigeria,* Advocacy for Policy and Innovation and NITDA, 2024, https://nitda.gov.ng/wp-content/uploads/2024/12/Updated-OHP-WHITE-PAPER-copy-compressed.pdf.

63 Ibid., p. 64.

64 Ibid., p. 44, 53.

65 Muhammad Nidhal, Rasya Athalla and Aldrich Alfarisi, "Shadows of Censorship: Indonesia's Content Moderation Policy Development," Center for Indonesian Policy Studies, July 2025, https://repository.cips-indonesia.org/media/publications/619819-shadows-of-censorship-indonesias-content-bad635c0.pdf.

66 *GR 71/2019 on the Implementation of Electronic Systems and Transactions*; *MR5/2020 on Private Electronic System Operators*; *MR10/2021 Amendments to MR5/2020*; *Ministerial Decree 172/2024*, later amended by the Minister of Communication and Informatics' *Decree No. 522/2024* (Decree 522/2024).

67 "Indonesia: Suspend, Revise New Internet Regulation", Human Rights Watch, 21 May 2021, https://www.hrw.org/news/2021/05/21/indonesia-suspend-revise-new-internet-regulation.

68 Sophie Syarief, "The Declining Freedoms of Speech and Press in Indonesia: New President, Same Problem?", Fulcrum, 23 October 2024, https://fulcrum.sg/the-declining-freedoms-of-speech-and-press-in-indonesia-new-president-same-problem/.

69 "GR 17/2025: Indonesia Imposes Child Protection Duties on Online Platforms," ssek, 3 June 2025, https://ssek.com/blog/gr-17-2025-indonesia-imposes-child-protection-duties-on-online-platforms/.

70 *Online Safety Act, No. 9 of 2024,* Parliament of the Democratic Socialist Republic of Sri Lanka, 1 February 2024, https://www.parliament.lk/uploads/acts/gbills/english/6311.pdf.

71 Soorya Balendra, "Continuing Repression: The Online Safety Act of Sri Lanka," *Free Speech in the Puzzle of Content Regulation,*24 November 2024, https://link.springer.com/chapter/10.1007/978-3-031-75813-3_10.

72 Ibid.; Pathum Wickramarathne, "Shielding Citizens or Silencing Dissent in Sri Lanka", 16 June 2025, https://pen.org.au/sri-lanka-online-safety-act-silencing-dissent/.

73 "Human rights concerns over two draft laws in Sri Lanka", OHCHR, 13 October 2023, https://www.ohchr.org/en/press-briefing-notes/2023/10/human-rights-concerns-over-two-draft-laws-sri-lanka.

74 Wickramarathne, "Shielding Citizens or Silencing Dissent in Sri Lanka", 2025, https://pen.org.au/sri-lanka-online-safety-act-silencing-dissent/

75 Ibid.

76 "Morocco plans regulatory framework to monitor social media and digital platforms", Hespress, 14 May 2025, https://en.hespress.com/110752-morocco-plans-regulatory-framework-to-monitor-social-media-and-digital-platforms.html.

77 Ibid.

78 *White Paper on the Framework for an Online Harms Protection Bill in Nigeria,* NITDA, December 2024.

79 "Proposed Digital India Act, 2023", MeitY.

80 Ministro Dias Toffoli, "Voto in Recurso Extraordinário 1.037.396 (Tema 987 da Repercussão Geral)," Supremo Tribunal Federal, June 2025, https://noticias-stf-wp-prd.s3.sa-east-1.amazonaws.com/wp-content/uploads/wpallimport/uploads/2025/06/11212444/RE-1037396-Voto-DT.pdf; https://portal.stf.jus.br/processos/downloadPeca.asp?id=15378980592&ext=.pdf

81 Namrata Maheshwari, "Traceability Under Brazil's Proposed Fake News Law Would Undermine Users' Privacy and Freedom of Expression", Center for Democracy and Technology, 23

June 2020, *https://cdt.org/insights/traceability-under-brazils-proposed-fake-news-law-would-undermine-users-privacy-and-freedom-of-expression/*.

82 Ricardo Brito and Lisandra Paraguassu, "Brazil's Supreme Court suspends Telegram, a key Bolsonaro platform," Reuters, 19 March 2022, *https://www.reuters.com/world/americas/brazil-supreme-court-orders-suspension-telegram-app-country-reports-2022-03-18/*; "Brazil court lifts suspension of Telegram app", DW, 30 April 2023, *https://www.dw.com/en/brazil-court-lifts-telegram-suspension-despite-non-compliance-for-neo-nazi-group-data/a-65474168*.

83 "Reconhecimento da inconstitucionalidade parcial e progressiva do art. 19 do MCI [Recognition of the partial and progressive unconstitutionality of Article 19 of the MCI]", Supremo Tribunal Federal, June 2025, *https://noticias-stf-wp-prd.s3.sa-east-1.amazonaws.com/wp-content/uploads/wpallimport/uploads/2025/06/26205223/MCI_tesesconsensuadas.pdf*, paragraph 3.1.

84 Hannah Ellis-Petersen, "WhatsApp sues Indian government over 'mass surveillance' internet laws", The Guardian, 26 May 2021, *https://www.theguardian.com/world/2021/may/26/whatsapp-sues-indian-government-over-mass-surveillance-internet-laws*.

85 "Digital India Act will curb circulation of online criminal, child sexual abuse material: MoS IT Rajeev Chandrasekhar", Economic Times India, 4 March 2023, *https://government.economictimes.indiatimes.com/news/digital-india/digital-india-act-will-curb-circulation-of-online-criminal-child-sexual-abuse-material-mos-it-rajeev-chandrasekhar/98402275*.

86 *White Paper on the Framework for an Online Harms Protection Bill in Nigeria,* NITDA, 2024.

87 "GR 17/2025: Indonesia Imposes Child Protection Duties on Online Platforms," ssek, 2025.

88 "Morocco plans regulatory framework to monitor social media and digital platforms", Hespress, 2025.

89 *Online Safety Act,* Sri Lanka, 2024, Sections 12-21.

90 *Social Media Act (Bill), 2081,* Communication Minister of Nepal [translated by Law Democracy], 28 January 2025, https://www.law-democracy.org/wp-content/uploads/2025/02/Nepal.Social-Media-Bill_2025_Eng.pdf.

91 "Nepal's Social Media Bill 2081: Review and Discussion", UNESCO, 7 March 2025, https://www.unesco.org/en/articles/nepals-social-media-bill-2081-review-and-discussion.

92 *Marco Civil Law,* Brazil, 2014, Articles 18, 19 and 21.

93 "Recognition of the partial and progressive unconstitutionality of Article 19 of the MCI," Supremo Tribunal Federal, 2025.

94 *Online Safety Act,* Sri Lanka, 2024, Section 27.

95 Neeti Biyani and Amrita Choudhury, "Internet Impact Brief: 2021 Indian Intermediary Guidelines and the Internet Experience in India", Internet Society, 8 November 2021, *https://www.internetsociety.org/resources/2021/internet-impact-brief-2021-indian-intermediary-guidelines-and-the-internet-experience-in-india/*.

96 "Proposed Digital India Act, 2023", MeitY.

97 *Boletín N° 14.561-19, Proyecto de ley sobre regulación de plataformas digitales [Digital Platforms Regulation Bill],* Congress of Chile, 1 September 2021. *https://www.camara.cl/legislacion/ProyectosDeLey/tramitacion.aspx?prmID=15047&prmBOLETIN=14561-19*.

98 "International civil society warns about the dangers to the exercise of rights of the bill to regulate digital platforms presented in Chile", Association for Progressive Communications, 24 November 2021, *https://www.apc.org/en/pubs/international-civil-society-warns-about-dangers-exercise-rights-bill-regulate-digital*.

99 Civil Society Coalition Memo to the National Information Technology Development Agency (NITDA) On The Draft Code Of Practice For Interactive Computer Service Platforms/Internet Intermediaries, Paradigm Initiative, 24 June 2022, *https://paradigmhq.org/wp-content/uploads/2022/06/NITDA-Code-Response-Memo.pdf*.

100 *White Paper on the Framework for an Online Harms Protection Bill in Nigeria,* NITDA, 2024.

101 Toffoli, "Voto in Recurso Extraordinário 1.037.396," STF, 2025; Ministro Luiz Fux, "Voto in Recurso Extraordinário 1.057.258 Minas Gerais," STF, 13 August 2025, *https://portal.stf.jus.br/processos/downloadPeca.asp?id=15378980592&ext=.pdf*; Veridiana Alimonti, "Brazil's Internet Intermediary Liability Rules Under Trial: What Are the Risks?", Electronic Frontier Foundation, 11 December 2024, *https://www.eff.org/deeplinks/2024/10/brazils-internet-intermediary-liability-rules-under-trial-what-are-risks*.

102 Pathum Wickramarathne, "Shielding Citizens or Silencing Dissent in Sri Lanka," PEN, 16 June 2025, *https://pen.org.au/sri-lanka-online-safety-act-silencing-dissent/*.

103 "Sri Lanka: Withdraw the Online Safety Bill", ARTICLE19, 19 January 2024, *https://www.article19.org/resources/sri-lanka-withdraw-online-safety-bill/*.

104 *The Electronic and Postal Communications (Online Content) Regulations, 2020,* United Republic of Tanzania, 17 July 2020, *https://www.tcra-ccc.go.tz/uploads/documents/en-1637908806-The%20Electronic%20and%20Postal%20Communications%20(Online%20Content)%20Regulations,%202020.pdf*; *The Electronic and Postal Communications (Online Content) (Amendment) Regulations, 2025,* United Republic of Tanzania, 28 January 2025, *https://www.tcra.go.tz/uploads/documents/sw-1738833320-Online%20Content%20Amendment%20Regulations,%202025%20GN%20No%2057%20of%2028%20January%202025.pdf*.

105 "Tanzania: Online Content Regulations 2020 extremely problematic in the context of COVID-19 pandemic", ARTICLE19, 19 January 2021, *https://www.article19.org/resources/tanzania-online-content-regulations-problematic-covid-19-pandemic/*.

106 *The Electronic and Postal Communications (Online Content) (Amendment) Regulations,* Tanzania, 2025, Regulation 15A.

107 Brito Cruz, Kira and Hartmann, "Duty of care and regulation of digital platforms," 2025; Bueno and Canaan, "The Brussels Effect in Brazil," 2024.

108 "Recognition of the partial and progressive unconstitutionality of Article 19 of the MCI," STF, 2025, paragraph11.

109 "Proposed Digital India Act, 2023", MeitY; Sheikh, "Transparency Must be a Cornerstone of the Digital India Act", Tech Policy Press, 2024.

110 *White Paper on the Framework for an Online Harms Protection Bill in Nigeria,* NITDA, 2024, p.68.

111 "New Digital Law Implications for Thailand," Asia Internet Coalition, *https://aicasia.org/policy-advocacy/new-digital-law-implications-for-thailand/*.

112 "Latest Updates on the Digital Platform Economy Bill," Bangkok Global Law, February 2025, https://www.bgloballaw.com/wp-content/uploads/2025/04/Latest-Updates-on-the-Digital-Platform-Economy-Bill_Bangkok-Global-Law.pdf.

113 "Recognition of the partial and progressive unconstitutionality of Article 19 of the MCI," STF, 2025, paragraph 8.

114 Adil Faouzi, "Morocco's New Social Media Law: HACA to Expand Authority Under Bensaid's Plan," Morocco World News, 16 May 2025, https://www.moroccoworldnews.com/2025/05/200662/moroccos-new-social-media-law-haca-to-expand-authority-under-bensaids-plan/.

115 *Code of Practice for Interactive Computer Service Platforms/ Internet Intermediaries,* NITDA, 2022, Part V, Article 2.

116 *White Paper on the Framework for an Online Harms Protection Bill in Nigeria,* NITDA, 2024.

117 Sheikh, "Transparency Must be a Cornerstone of the Digital India Act", Tech Policy Press, 2024.

118 Ibid.

119 *Marco Civil Law,* Brazil, 2014, Article 20.

120 "Recognition of the partial and progressive unconstitutionality of Article 19 of the MCI," STF, 2025, paragraphs 9 and 10.

121 *Code of Practice for Interactive Computer Service Platforms/ Internet Intermediaries,* NITDA, 2022, Part I, paragraphs 8 and 9.

122 *White Paper on the Framework for an Online Harms Protection Bill in Nigeria,* NITDA, 2024, p.70.

123 "New regulation strengthens online safety for children," Herbert Smith Freehills Kramer, 19 June 2025, https://www.hsfkramer.com/insights/2025-06/new-regulation-strengthens-online-safety-for-children.

124 Kamran Adil, "2025 Amendments to The Prevention Of Electronic Crimes Act, 2016: An Introduction", Research Society of international Law, 25 February 2025, https://rsilpak.org/2025/2025-amendments-to-the-prevention-of-electronic-crimes-act-2016-an-introduction/.

125 "Briefing: Pakistan media decry controversial bill to regulate social media", BBC Monitoring, 24 January 2025, https://monitoring.bbc.co.uk/product/b00037oq.

126 "GR 17/2025: Indonesia Imposes Child Protection Duties on Online Platforms," ssek, 2025.

127 Faouzi, "Morocco's New Social Media Law: HACA to Expand Authority Under Bensaid's Plan," Morocco World News, 2025.

128 "International civil society warns about the dangers to the exercise of rights of the bill to regulate digital platforms presented in Chile", Derechoes Digitales, 24 November 2021, https://www.apc.org/en/pubs/international-civil-society-warns-about-dangers-exercise-rights-bill-regulate-digital.

129 Júlia Mendonça, Rafael Zanatta, Thaís Aguiar and Victor Durigа, "O Dilema da Autoridade: Alternativas Regulatórias No Debate Do Projeto Lei 2630/2020," Data Privacy BR Research, 26 July 2023, https://assets-global.website-files.com/60244423a672eb5c9027e063/64ca96a4e38438560dd000a5_o-dilema-da-autoridade-no-2630.pdf; Kira Beatriz, "Regulatory intermediaries in content moderation", Internet Policy Review, 31 March 2025, https://www.econstor.eu/bitstream/10419/315581/1/1923068024.pdf.

130 Alimonti, "Brazil's Internet Intermediary Liability Rules Under Trial", EFF, 2024; Bueno and Canaan, "The Brussels Effect in Brazil," 2024.

131 "Sri Lanka's Online Safety Act, No. 9 of 2024," Geneva Internet Plaform, February 2024, https://dig.watch/resource/sri-lankas-online-safety-act-no-9-of-2024.

132 Prateek Waghre, "A Lack of Sense, and Censor-ability in India," Tech Policy Press, 6 March 2025, https://www.techpolicy.press/a-lack-of-sense-and-censorability-in-india/.

133 "Report of the Statutory Review of the Online Safety Act 2021", Australian Government, Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts, 4 February 2025, https://www.infrastructure.gov.au/department/media/publications/report-statutory-review-online-safety-act-2021, p.146.

134 "Recognition of the partial and progressive unconstitutionality of Article 19 of the MCI," Supremo Tribunal Federal, 2025, Section 11.

135 Faouzi, "Morocco's New Social Media Law: HACA to Expand Authority Under Bensaid's Plan," Morocco World News, 2025.

136 "Vietnam: Repeal Harmful Internet Laws," Human Rights Watch, 10 December 2024, https://www.hrw.org/news/2024/12/11/vietnam-repeal-harmful-internet-laws.

137 "Indonesia's Ministry of Communications sued after blocking 8 digital platforms", Aliansi Jurnalis Independen, 20 December 2022, https://aji.or.id/informasi/indonesias-ministry-communications-sued-after-blocking-8-digital-platforms.

138 *Online Safety Act,* Sri Lanka, 2024, Section 24.

139 *The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021,* MeitY, Section 69A.

140 Janjira Sombatpoonsiri and Sangeeta Mahapatra, "Regulation or Repression? Government Influence on Political Content Moderation in India and Thailand", Carnegie Endowment for International Peace, 31 July 2024, https://carnegieendowment.org/research/2024/07/india-thailand-social-media-moderation?lang=en.

141 Bueno and Canaan, "The Brussels Effect in Brazil," 2024.

142 "Proposed Digital India Act, 2023," MeitY, Slide 18.

143 "The UK and Sri Lanka: A comparison of two online safety bills", Global Voices, 26 October 2023, https://globalvoices.org/2023/10/26/the-uk-and-sri-lanka-a-comparison-of-two-online-safety-bills/.

144 *White Paper on the Framework for an Online Harms Protection Bill in Nigeria,* NITDA, 2024, p.36, 64.

145 Faouzi, "Morocco's New Social Media Law: HACA to Expand Authority Under Bensaid's Plan," Morocco World News, 2025.

146 "Proposed Digital India Act, 2023," MeitY, Slides 18, 21.

147 An amendment to include reference to the rights of the child was proposed during the Online Safety Act's negotiation in Parliament, but not passed. See Lord Russell of Liverpool's amendment, Clause 25, available at https://bills.parliament.uk/bills/3137/stages/17371/amendments/94939?utm_source=chatgpt.com.

148 "Indonesia: Safeguarding Children's Data in the Digital Age: Highlights of Government Regulation No. 17 of 2025," One Asia Lawyers, June 2025, https://oneasia.legal/en/6419.

149 Bueno and Canaan, "The Brussels Effect in Brazil," 2024.

150 "Indonesia: Suspend, Revise New Internet Regulation," Human Rights Watch, 21 May 2021, https://www.hrw.org/news/2021/05/21/indonesia-suspend-revise-new-internet-regulation.

151 Divyank Katira and Gurshabad Grover, "How message tracing regulations subvert encryption," Internet Policy Review, 24 March 2022, https://policyreview.info/articles/news/how-message-tracing-regulations-subvert-encryption/1642; "Proposed amendments to IT Rules in India threaten freedom of expression and privacy beyond borders", Association for Progressive

Communications, 6 July 2022, https://www.apc.org/en/press/proposed-amendments-it-rules-india-threaten-freedom-expression-and-privacy-beyond-borders; Meri Baghdasaryan, "New Amendments to Intermediary Rules threaten Free Speech in India," 21 July 2022, https://www.eff.org/deeplinks/2022/07/new-amendments-intermediary-rules-threaten-free-speech-india.

152 *"Platforms must implement "efficient content moderation systems" using algorithms that automatically detect problematic material."* See Faouzi, "Morocco's New Social Media Law: HACA to Expand Authority Under Bensaid's Plan," Morocco World News, 2025.

153 "Ofcom Consultation: Protecting people from illegal harms online," Global Partners Digital, February 2024, https://www.ofcom.org.uk/siteassets/resources/documents/consultations/category-1-10-weeks/270826-consultation-protecting-people-from-illegal-content-online/responses/global-partners-digital.pdf?v=369869.

154 Chiara Castro, "Over 450,000 Brits want to repeal the UK Online Safety Act – here's how to have your say," Tech Radar, 5 August 2025, https://www.techradar.com/vpn/vpn-privacy-security/over-340-000-brits-want-to-repeal-the-uk-online-safety-act-heres-how-to-get-your-say; "Tech giants push back against Australia's social media ban for children," DigWatch, 27 November 2024, https://dig.watch/updates/tech-giants-push-back-against-australias-social-media-ban-for-children; Zoe Jay Hawkins, "Australia's Online Safety Populism: New Social Media Age Restrictions a Symptom of a Larger Problem with Policy Approach," 9 December 2024, https://www.techpolicy.press/australias-online-safety-populism-new-social-media-age-restrictions-a-symptom-of-a-larger-problem-with-policy-approach/.

155 "eIDAS 2: the countdown to a single European Digital ID Wallet has begun," Thales, https://www.thalesgroup.com/en/markets/digital-identity-and-security/government/identity/eidas-regulations, accessed 9 September 2025; Pedro Lomba and Francisca Caldeira Cardoso, "Guidelines for the protection of minors under the Digital Services Act," PLMJ, 12 June 2025, https://www.plmj.com/en/knowledge/informative-notes/Guidelines-for-the-protection-of-minors-under-the-Digital-Services-Act/33972/.

156 "Guidelines for the governance of digital platforms: safeguarding freedom of expression and access to information through a multi-stakeholder approach," UNESCO, 2023, https://unesdoc.unesco.org/ark:/48223/pf0000387339;

157 "Regulatory authorities", UNESCO, 22 April 2025, https://www.unesco.org/en/digital-platform-governance/regulatory-authorities.

158 Ramsha Jahangir, "Amid Flurry of Online Safety Laws, the Global Online Safety Regulators Network is Growing," 19 March 2024, https://www.techpolicy.press/amid-flurry-of-online-safety-laws-the-global-online-safety-regulators-network-is-growing/.

159 "Platform Accountability: A Rule-Of-Law Checklist for Policymakers," Access Now, December 2024, https://www.accessnow.org/wp-content/uploads/2024/12/Platform-accountability-a-rule-of-law-checklist-for-policymakers-report-2024.pdf.

160 Ibid.

161 "Guidelines for the governance of digital platforms," UNESCO, 2023; Jahangir, "Amid Flurry of Online Safety Laws, the Global Online Safety Regulators Network is Growing," 2024; "Platform Accountability: A Rule-Of-Law Checklist for Policymakers," Access Now, 2024.

162 Ian Barber and Maria Paz Canales, "What would a human rights-based approach to platform regulation look like?", Global Partners Digital, 30 July 2024, https://www.gp-digital.org/what-would-a-human-rights-based-approach-to-platform-regulation-look-like/.

163 Mai Van Tran, "Lessons from Resisting Big Tech Power in Southeast Asia," 19 June 2025, https://www.techpolicy.press/lessons-from-resisting-big-tech-power-in-southeast-asia/.

164 Ramsha Jahangir, "Advocates and Researchers Set Up "Global Majority House" in Brussels to Engage on Digital Services Act," 14 November 2024, https://www.techpolicy.press/advocates-and-researchers-set-up-global-majority-house-in-brussels-to-engage-with-dsa/

GLOBAL
PARTNERS
DIGITAL