Policy Brief: The constitutionality of article 19 of the Marco Civil da Internet (Civil Rights Framework for the Internet)

Coordinators

Camila Akemi Tsuzuki

Laura Gabrieli Pereira da Silva

Reviewers

Danielle Sanchez

Gabriela Paz

Gabriela Nardy

Paulo Rená

1. Introduction

In Brazil, the Federal Supreme Court (STF) is currently reviewing the constitutionality of article 19 of the Civil Rights Framework for the Internet (MCI), which establishes the liability framework for Internet application providers regarding third-party content. This analysis is part of the ongoing judgment of Extraordinary Appeals (RE, in Portuguese) 1037396 and 1057258. Following the initial votes by the two reporting justices in these cases, ISOC Brasil publicly expressed concerns in a Technical Note. With the expectation that the trial will resume in 2025 – amid new developments that have intensified the debate – we reiterate the risks of a ruling that could negatively impact the Internet in Brazil. This document reaffirms our opposition to a potential declaration of unconstitutionality of article 19 and explores possibilities, limitations, and risks for an interpretation that preserves an open, secure, technologically neutral, globally connected, and trustworthy Internet.

In 2014, article 19 of the MCI emerged from a broad and complex multistakeholder debate involving academics, civil society representatives, industry stakeholders, and the government. It established a notice and judicial takedown liability model for digital intermediaries classified as application providers. Under this framework, such providers can only be held liable for third-party content if they fail to remove it after a court order. The primary intent was to balance freedom of expression and protection against abuses, fostering a liability regime that avoids arbitrary censorship through content removal.

From the outset of the MCI debates, there was a deliberate effort to explicitly enshrine freedom of expression – not as an absolute priority over other fundamental rights, but in recognition of the Internet's role as a technology centered on communication and information. The legislature's balancing of these rights resulted from years of deliberation and reflected the factual context of the time, with significant attention to protecting Internet users. It is therefore misguided to frame this model as favoring the profit-driven interests of technology companies – a view that overlooks the depth of the original discussions.

Over the years, as Internet access expanded, content moderation has grown increasingly complex. Digital platforms' moderation practices have faced widespread criticism for inadequately addressing illegal content, disinformation, and hate speech, particularly due to a lack of transparency. After four years of intense debate in the National Congress, Legislative

Proposal 2.630/2020[1] – the most discussed legislative proposal to address digital challenges – was shelved in 2024. The STF's review of the REs now unfolds in this context: legislative inaction and a perceived insufficiency of existing regulations to address evolving digital dynamics.

In the 2010s, the MCI filled a regulatory gap and established clear guidelines for intermediary liability, providing legal certainty to the sector and fostering Internet development in Brazil. Before its enactment, judicial rulings on the issue were often contradictory. By introducing the possibility of notice and judicial takedown liability for application providers under two defined scenarios –and in cases of non-compliance with court orders –article 19 marked a significant step forward. Since then, Internet usage have transformed dramatically. While the benefits to economic, social, and political development are undeniable, challenges to democratic stability have also emerged.

Attempting to resolve all issues under review in the judgment of Extraordinary Appeals 1037396 and 1057258 is a risky endeavor, as it could penalize the entire Internet ecosystem. Given the historical expertise of the Internet Society's Brazilian Chapter in knowledge production and advocacy for this ecosystem, we reaffirm that any measures must necessarily consider impacts on the vast diversity of Internet providers – far beyond the social media platforms primarily targeted by these REs.

This judgment represents a pivotal moment for the Internet in Brazil. Its outcome could redefine the balance between freedom of expression, intermediary liability, and protection against harms caused by illegal content, as well as alter the Internet as we know it.

We recommend close monitoring of the STF proceedings and a thorough debate on potential legislative adjustments to mitigate risks, ensuring that any changes preserve the fundamental principles of the MCI and the critical properties of the Internet[2].

---

[1] Legislative Project 2.630/2020 was a bill aimed at establishing the Brazilian Law on Freedom, Responsibility, and Transparency on the Internet, introducing regulatory rules for social media platforms and private messaging services. Proposed by Senator Alessandro Vieira, its original version sparked significant controversy, particularly due to proposed traceability and surveillance measures designed to combat online disinformation. Between 2020 and 2024, it underwent extensive debate and revisions, drawing inspiration from European regulations such as the Digital Services Act (DSA). However, in April 2024, lacking sufficient support for approval, it was shelved by the President of the Chamber of Deputies.

[2] The Internet is a global, decentralized network that interconnects smaller networks without a central control point. It operates through open and common protocols, enabling seamless communication between all devices. Its modular

Amid growing discussions about reforming intermediary liability in the digital environment, we highlight that the Internet Society's Brazilian Chapter developed a Decalogue of Recommendations on the Brazilian Intermediary Liability Model in 2021, following multistakeholder debates.

These recommendations, detailed in the cited document and summarized below, are reiterated in this policy brief.

1. The complexity of the Internet service provider ecosystem must be acknowledged;
2. Internet infrastructure must be protected;
3. Full participation of all relevant sectors must be ensured in any policymaking or regulatory process for the Internet;
4. All policies or regulations must account for existing asymmetries across multiple dimensions among digital ecosystem actors;
5. The liability framework of the Civil Rights Framework for the Internet requires no reforms;
6. Any improvements to the Civil Rights Framework for the Internet must preserve its principles and follow its collaborative development model;
7. The Internet must be respected as a network of multiple purposes;
8. Transparency, accountability, and due process must be required of Internet access and application providers;
9. Internet application providers' terms of service must ensure broad access to information and include due process measures;
10. Impact assessments must be prioritized in public and private sector decision-making.

ISOC's technical assessment of the judgment and its implications is detailed in this policy brief. In the **first section**, we revisit the context of the case and analyze the constitutional review mechanisms the STF may employ to rule on article 19's validity. In the **second section**, we outline the risks of declaring article 19 unconstitutional. Finally, we explore

structure relies on standardized components that can be combined to create new services, fostering innovation. Each device has unique identifiers to ensure connectivity. The Internet is technologically neutral, supporting a vast range of uses. Ideally, it should be accessible (open to all), secure (protecting data integrity), and reliable (functioning consistently). These ideals are its Aspirational Goals, achieved through Enablers (features that advance these goals). Critical Properties are the fundamental characteristics that ensure the Internet's functionality.

possibilities and limits for an interpretation that offers a balanced solution in Brazil's current landscape.

1.1 About Internet Society (ISOC)

The Internet Society (ISOC) is a nonprofit organization established in 1992 with a global presence. Its mission is to promote leadership in the development of Internet standards, as well as to advance educational initiatives and public policies related to the worldwide network. To achieve this, ISOC facilitates collaboration with governments, businesses, and other entities to adopt Internet policies aligned with its core principles: an open, universally accessible network that fosters innovation, creativity, and commercial opportunities. For example, ISOC provides financial and administrative support to the Internet Engineering Task Force (IETF), responsible for developing and refining Internet operational guidelines and standards. The organization has over 100 local chapters and more than 100,000 individual and organizational members worldwide.

1.2 About ISOC Brasil

ISOC Brasil is the Brazilian Chapter of the Internet Society, with over 1,150 active members across the country. Its membership spans diverse communities: Technical professionals involved in the technological development and operation of the Internet; Civil society representatives engaged in public policy discussions related to the Internet; Business stakeholders working on Internet infrastructure, access provision (e.g., ISPs), and content development (e.g., media and application companies); Academic researchers across disciplines studying the Internet's evolution, usage, and socioeconomic impacts. ISOC Brasil serves as a platform to promote and discuss the principles championed by the Internet Society, as well as its major initiatives and positions. While it operates independently and autonomously, it occasionally adopts complementary stances to the global organization. For instance, this was observed during ISOC Brasil's involvement in developing the "Policy Framework on Intermediary Liability."

2. About the Judgment

The Brazilian Federal Supreme Court's judgment of RE 1037396 (General Repercussion Theme No. 987) and RE 1057258 (General Repercussion Theme No. 533) has become a pivotal arena for decisions impacting Brazil's entire framework of digital intermediary liability. These appeals, originating from illustrative cases involving the liability of social media platforms for third-party content, have sparked a broader debate about the intended goals and unintended consequences of radically altering intermediary liability rules. By designating these cases as General Repercussion Themes, the Court's rulings will shape the application and interpretation of article 19 of the MCI nationwide.

Resumed in 2024, the trial received votes from three of the Court's 11 justices before being adjourned for recess: the two votes from the case rapporteurs, Justices Dias Toffoli and Luis Fux, arguing for the unconstitutionality of article 19, and a dissenting vote from the current STF President, Luis Roberto Barroso.

RE 1037396, filed in 2017 by Facebook Serviços Online do Brasil LTDA, challenges a judicial order requiring the company to compensate a plaintiff for failing to act on a fake profile without a court order. Facebook contests this liability under article 19 of the MCI.

RE 1057258, filed in 2017 by Google Brasil Internet LTDA, involves a pre-MCI case where a teacher requested the removal of an offensive community on the defunct social network Orkut. Google appeals the court-ordered removal and compensation for moral damages, citing the impossibility of preemptive content moderation and risks of prior censorship under constitutional principles.

Under Brazilian jurisprudence, rulings on these General Repercussion Themes will directly influence the interpretation of article 19. When assessing a law's constitutionality, the STF follows a decision-making process that evaluates compatibility with the Federal Constitution. If a law is deemed unconstitutional, the Court may apply techniques like "conforming interpretation" (narrowing the law's application to align with the Constitution) or "partial declaration of unconstitutionality without text suppression" (invalidating only specific unconstitutional aspects). The Court may also modulate the temporal effects of its decision, determining whether it applies retroactively or prospectively.

In this context, the STF's judgment could either nullify article 19 entirely or redefine its interpretation. The votes cast so far – particularly by the rapporteurs – raise concerns about the Court's technical understanding of the Internet's functioning and the harmful consequences of declaring article 19 unconstitutional. Conversely, an overreach into legislative territory amid prolonged congressional inaction could also distort the law's intent.

The notice and judicial takedown liability model for social media providers emerged from a hard-won societal consensus. Even exceptional reforms to this framework should be grounded in studies assessing regulatory impacts on the Internet's core characteristics: openness, global connectivity, security, reliability, technological neutrality, and innovation. Ideally, such reforms should follow open, pluralistic legislative debate led by the National Congress[3].

That said, there is no denying the harmful actions (or inactions) of certain platforms, which have facilitated – or failed to reasonably mitigate – socially damaging behaviors like disinformation proliferation, aggressive political polarization, and institutional destabilization. ISOC Brasil has repeatedly criticized platforms' conduct, including in the recent case involving X (formerly Twitter). However, article 19 applies far beyond social media platforms. Radically altering or invalidating this provision without careful consideration risks harming Brazil's entire Internet ecosystem, disproportionately affecting service providers unrelated to these issues and, ultimately, all users[4].

A judgment of such magnitude must incorporate the technical aspects involved and the concrete consequences of its decisions, just as the Court appears to be increasingly taking these into account in its decision-making processes, supported by diverse methodological tools in other fields – such as the economic analysis of law framework.

---

[3] As we argued in our previous contribution, an incidental declaration of unconstitutionality of aarticle 19 of the Civil Rights Framework for the Internet in the context of an Extraordinary Appeal would be undesirable. This approach would amount to an indirect legislative reform and, ultimately, an interference with the institutional role of the Legislative branch.

[4] Amending aarticle 19, if poorly designed, could trigger a cascading impact extending far beyond social media platforms, affecting a broad spectrum of application and infrastructure providers. This includes, for example: e-commerce platforms; online collaboration tools; distance education platforms; health apps; streaming services; hosting providers; cloud storage services; DNS providers; security tools; startups and small developers. Imposing overly broad liability on these diverse actors could render business models unviable, restrict service diversity, compromise the Internet's stability, and ultimately harm users.

2.1 The First Days of the Judgment

The statements (in votes or supplementary comments by the justices) leading up to the trial's suspension in late 2024 – due to Justice André Mendonça's request for additional review – raise critical questions about the analytical approach adopted in these cases. However, we emphasize that arguments favoring unconstitutionality risk sidelining technical considerations related to the Internet ecosystem, such as network operations, intermediary functions, or legal possibilities under the law. Furthermore, while the use of "conforming interpretation" is more appropriate in this context, it must still be grounded in relevant technical aspects.

The complexity of the case is evident in the published votes, where STF justices present divergent views on the constitutionality of article 19 of the Civil Rights Framework for the Internet (MCI) and its implications, as summarized below and analyzed in this document.

Table 1: S*ummary of Votes Until the Trial's Suspension in December 2024*

Justice	Position	Key arguments
Dias Toffoli	Unconstitutionality	Proposes a Decalogue Against Disinformation with multiple mandates. Argues that article 19 of the MCI is outdated and fails to protect fundamental rights. Advocates extending the article 21[5] framework (notice and takedown) as the new general rule, imposing **strict liability** on providers for cases involving boosted content, unauthenticated/unidentified profiles, and a defined list of serious crimes. Groups most intermediaries under "application providers," differentiating them only from access/backbone providers – even including domain registrars and IP allocators. Claims **network neutrality** does not exempt platforms that actively manage content. Calls

[5] Article 21 of the Civil Rights Framework for the Internet stipulates that application providers may be held subsidiarily liable (notice and judicial takedown) if they fail to remove content published by third parties containing scenes of nudity or private sexual acts without authorization from the individuals involved, after receiving a notification from the participant or their legal representative.

		for specific regimes for journalistic entities and marketplaces, exempting interpersonal communication services (e.g., email). Proposes ancillary duties of transparency, accountability, and due process. Requires foreign application providers to appoint a local representative and urges detailed regulation by the Executive and Legislative branches.
Luis Fux	Unconstitutionality	Argues article 19 is unconstitutional for inadequately protecting fundamental rights, claiming freedom of expression was unduly prioritized. Demands immediate removal of illegal content upon **extrajudicial notice or when there is manifest evidence**, with courts deciding on republication. Criticizes platforms' **lack of transparency** in content moderation and stresses liability for AI-generated content, especially during elections, citing TSE resolutions on AI identification.
Luis Roberto Barroso	Partial Unconstitutionality (without text suppression) / Conforming Interpretation	Advocates partial unconstitutionality while applying a **conforming interpretation** to align article 19 with the Constitution. Expands exceptions to cover criminal offenses (excluding subjective crimes like defamation). Upholds **subsidiary liability (notice and judicial takedown)** for platforms, penalizing only systemic failures. Rejects state-only oversight bodies, favoring multistakeholder models. References EU regulations and limits the ruling's scope to social media providers. Insists content removal requires prior judicial orders for civil liability and urges detailed legislative regulation.

Source: Prepared by ISOC Brasil.

The votes favoring unconstitutionality rely on bibliographic research and arguments critiquing harmful content circulation on social media. However, they contain significant technical inaccuracies.

While acknowledging the MCI's history, the votes overlook the extensive public participation in its creation, its motivations, and the practical consequences of the 2014 framework. The MCI resulted from robust debates among civil society, academia, government, and the private sector – not a "naive" model prioritizing freedom of expression over other rights. This claim contradicts international principles, academic literature, and positions of UN and OAS free expression rapporteurs.

On the contrary, the framework established by the MCI is widely recognized internationally as an arrangement that was not built on the idea of disregard for problematic issues involving application providers. Rather, it grants the national judiciary the prerogative to assess such cases, as a direct outcome of intentional legislative and regulatory choices, while remaining open to exceptions and future adaptations. Therefore, we consider it harmful to the debate when the Marco Civil is portrayed as legislation for a so-called "lawless Internet," as if only now Brazilian Internet usage were to be brought under the rule of national law.

Additionally, the rapporteurs' proposals – strict liability (Toffoli) and immediate removal without judicial orders (Fux) – apply uniform standards to diverse intermediaries. These standards, derived from social media platforms' challenges, would inadvertently extend to application providers (e.g., e-commerce, cloud services, DNS providers) and even infrastructure actors, despite technical and legal distinctions.

For the other side, Barroso's approach offers a balanced path. Framing the debate around "where to draw the line" between free expression and preventing societal harm, he defended article 19's core requirement for judicial removal orders while advocating complementary "duty of care" obligations for platforms (with liability for systemic failures). He emphasized the diversity of intermediaries (e.g., marketplaces, domain registrars) and maintained subjective liability for social media platforms.

However, his critique of network neutrality as a "naive" MCI flaw reflects a technical misunderstanding. Network neutrality ensures equal treatment of data packets (without

discrimination by origin, content, or destination), safeguarding competition and innovation. It applies to infrastructure – not application-layer content moderation. Practices like zero-rating (exempting specific services from data caps) or CDN optimization are separate issues.

With such reservations noted, the position presented by Justice Barroso is constructive in rejecting the outright dismissal of article 19, distinguishing the ongoing issues, and advancing legal mechanisms that address both demands falling outside the scope of the Civil Rights Framework for the Internet and reinforce the value of judicial orders, due process, and models distinct from strict liability.

In this regard, the debate on the scope of the judgment, emphasized by Justices Cristiano Zanin and Luis Roberto Barroso, before trial suspension due to Justice André Mendonça's request for review, – is also valuable. Limiting the judgment's effects to specific providers or functions seems appropriate, given that the overwhelming majority of discussions and examples presented in the Court's plenary focus exclusively on social media platforms.

Adapting the question that guided Justice Barroso's reasoning, we present our contributions on "where to draw the line" between efforts to legally model behaviors in digital environments and the Internet's functioning.

3. The risks of declaring article 19 unconstitutional

The first line to be drawn concerns the constitutionality of article 19. Currently, this article shields application providers from judicial liability for third-party content unless they fail to remove it after a notice and judicial takedown order. This protection extends not only to social media platforms but also to hosting services, cloud storage providers, domain registrars, and other types of intermediaries. The framework embedded in article 19 recognizes the diversity of the Internet ecosystem and the distinct roles played by different services. It avoids imposing disproportionate obligations on entities that do not exercise editorial control over content, thereby ensuring legal certainty for innovation and the free flow of online information.

A potential declaration of article 19's unconstitutionality disregards this context and could expand liability to intermediaries with no influence over user-generated content. This would increase their operational costs and impose obligations often unrelated to their service's

purpose or technically unfeasible. In these terms, the primary risk we emphasize is undue liability.

Entities with no control over user-published content – including those foundational to the Internet's operation – could be forced to implement preventive filtering and takedown systems, jeopardizing fundamental rights and the network's stability. This scenario risks triggering a domino effect across the ecosystem, prompting providers to adopt excessive preventive measures, such as mass content removal without rigorous analysis. Such actions would stifle freedom of expression and reduce the diversity of information available online.

As highlighted by Justice Barroso, given the vast volume of daily digital content, moderation will likely rely on automated identification and filtering technologies. However, no technical solution is foolproof for detecting content that violates the categories listed in the ruling. Moreover, corporate incentives will rarely align with the social values the justices aim to uphold.

Current filtering tools used by companies have intrinsic flaws, such as inability to grasp local contexts and linguistic nuances and high error rates, producing false positives (legitimate content wrongly removed) and false negatives (harmful content undetected).

Except for cases requiring minimal contextual analysis – such as child sexual abuse material (which must never be permitted) or non-consensual intimate image sharing (easier to detect through nudity filters combined with user reports) – content removal demands careful, context-sensitive scrutiny. Given the sheer volume of content, automated systems alone cannot reliably balance rights protection with accuracy.

However, there is a widespread perception that content recommendation algorithms are far more efficient and accurate than content moderation algorithms. No evidence supports this view. This perception likely stems from the fact that inaccurate recommendations are far less noticeable than improperly removed or preserved content. Thus, it is unreasonable to dismiss claims of technical infeasibility in implementing certain solutions for one type of problem simply because similar solutions exist for others – without at least demonstrating concrete, data-backed technical alternatives.

If even the Judiciary, trained to assess content illegality and operating in its native language, makes errors that often require correction through appeals, it is highly unlikely that platforms could adequately handle vastly larger volumes of content using automated filters, as advocated by the reporting justices. Furthermore, the need to standardize moderation and the inherent algorithmic biases could lead to a serious risk of political homogenization on socially relevant issues.

Another critical point is the lack of clarity in the rules. While the MCI acknowledges the complexity of the digital ecosystem, the regulatory debate at the time resulted in a law that categorizes Internet providers into only two "classes": access providers and application providers. Consequently, all services not classified as access providers are deemed application providers.

In this judgment, if the Court decides to adopt a broader interpretation of these intermediaries, diverse categories of providers could be subjected to the same liability regime, creating legal uncertainty. Given that the STF's plenary debates appear focused on large providers of a specific service type (e.g., social media), applying the same standards to all other providers would be problematic. Companies operating in different segments of the digital chain may struggle to understand their rights and obligations, undermining regulatory predictability and their capacity for innovation.

This is particularly relevant in light of some discussions raised during the trial that seem unrelated to the case – such as holding journalistic service providers liable when they act as social media users (e.g., sharing news articles on a platform). If a media outlet uses social media like any other user, this falls outside the scope of article 19 of the MCI, which addresses intermediary liability for third-party content. Moreover, the fact that a media outlet operates a website subject to a distinct liability regime for user comments does not alter its position when acting solely as a social media user.

In light of this scenario, it is imperative that the STF conducts its analysis of article 19 through an approach that accounts for both the constitutional principles at stake and the practical impacts of its decision on the diverse actors within the Brazilian digital ecosystem. The outcome of this judgment will have profound repercussions not only for technology companies but also for users, affecting freedom of expression and innovation in the digital environment.

4. Limits and possibilities for advancing regulation

The debate on Internet regulation requires a delicate balance between protecting fundamental rights, fostering innovation, and preserving the Internet's open and decentralized architecture. Amid evolving digital landscapes and challenges posed by new Internet uses, it is essential to assess the extent to which regulatory adjustments are necessary and what limits must be observed to avoid adverse effects.

In this section, we explore limits and possibilities we deem relevant – though not exhaustive – for a balanced solution that addresses the interests at stake in these Extraordinary Appeals (REs) while ensuring the Internet remains an open, globally connected, secure, and trustworthy resource for all.

The STF has focused not only on the constitutionality of article 19 of the MCI but also on establishing mechanisms to safeguard essential legal principles, such as fundamental rights and democracy. Among the debated possibilities are: (i) judicial orders for removing illegal content as the general rule (ii) extrajudicial or *ex officio* takedowns in specific cases.

Barroso advocated not only the preservation of the subjective liability regime for application providers regarding third-party content, but also the expansion of exceptions to this rule, in line with Article 21 of the MCI.

1. His proposal suggests preserving Article 19 for non-criminal offenses, while introducing a notice-and-takedown regime for criminal offenses, excluding those involving highly subjective assessments, such as crimes against honor.

Under the notice-and-takedown model, platforms would bear the burden of demonstrating that they acted appropriately upon receiving a notification. This includes assessing whether the content is indeed unlawful, and liability would only arise if the judiciary confirms that a crime has occurred. However, if there is reasonable doubt about the criminal nature of the content, the platform could not be held civilly liable.

Additionally, the proposal introduces a "duty of care", defined as a "genuine obligation to employ all efforts to prevent and mitigate systemic risks created or amplified by platform activities and content disseminated through their services." This duty is distinct from the subjective liability discussed earlier. Under this framework, providers must act proactively to ensure their platforms are free of severely harmful content.

Content subject to this rule includes, but is not limited to: (a) Child sexual abuse material and severe crimes against children and adolescents; (b) Inducement, incitement, or assistance to suicide or self-harm; (c) Human trafficking; (d) Acts of terrorism; (e) Violent overthrow of the democratic rule of law and coup attempts. Liability does not arise from the failure to remove specific content but rather from systemic failures to fulfill the duty of care.

Regarding advertisements or boosted content, the proposal argues that a platform's approval of content for advertising purposes would suffice to demonstrate its awareness of the material being disseminated. Under this model, prior notice would not be required to establish the provider's liability.

While the importance of enhancing fundamental rights protections online is undisputed, we urge caution regarding the modulation of article 19 of the MCI. It is critical that exceptions or complementary adjustments to the general liability framework do not distort the original intent of the law.

In our impact analysis of the latest public version of Legislative Project 2.630/2020, we found that the proposed formulation of the "duty of care" risked undermining the entire framework of fault-based liability and notice-and-judicial-takedown. The mechanism created an exceptional regime that, without previously establishing a regulatory body, opened the door to radically changing liability under the duty of care. This risked imposing strict liability on intermediaries for a technically unfeasible and potentially harmful role – effectively privatizing detailed content analysis rather than fostering systemic risk mitigation frameworks.

Content moderation requires contextual analysis and an understanding of linguistic nuances. When automated, the high volume of uploaded content amplifies the risk of false positives (legitimate content wrongly removed) and false negatives (harmful content undetected). While some illegal content is easily identifiable, the challenge lies in material

occupying a gray area between legality and illegality. Expanding scenarios where platforms unilaterally decide content removal increases the risk of excessive restrictions on public debate, potentially inverting the rule-exception balance.

A recent Harvard study on machine learning models used in content moderation raises another critical concern: predictive multiplicity. The study found that different content classification models can achieve similar average performance yet produce conflicting predictions for the same specific content. This arbitrariness could lead to inconsistent restrictions on discourse, disproportionately harming marginalized groups. Discriminatory effects from such models risk being scaled, undermining freedom of expression – particularly for minorities.

The study also highlights that most AI moderation models are developed by a small group of actors, concentrated in the Global North due to high investment barriers. These models may inadequately reflect the needs and values of the Global South, exacerbating inequities in content governance.

Thus, we recognize the harms caused by the spread of illegal content in the digital environment, but we remain cautious about granting application providers the legitimacy to determine the legality of content – especially given their limited capacity to assess the quality of moderation practices.

In this context, we believe efforts to promote transparency, accountability, and due process are essential and should be required of application providers to ensure users receive clear information about how platform actions may impact their rights. This includes: easy access to Internet application providers' terms of service: due process measures allowing users to challenge moderation decisions; robust, auditable reports on algorithmic models to clarify their effects on public discourse and fundamental rights online.

However, the effectiveness of these measures depends on establishing a regulatory body capable of enforcing obligations and preventing abuses. Such an entity must have technical expertise, a multidisciplinary and multistakeholder composition, and financial autonomy and independence. Crucially, both the creation of this body and the regulation of providers' transparency duties require legislative action by the National Congress.

Finally, we emphasize the importance of the terminology adopted in any eventual guidance resulting from the rulings. For this analysis, we present as relevant instruments the ISOC Brasil Decalogue and the recently launched Internet Society Policy Framework[6], which should be interpreted in conjunction with the contribution we submitted during its respective Policy Development Process.

These documents highlight that Internet policies are most effective when they adopt definitions based not on the specificities of a fleeting moment in the digital environment, but on criteria that ensure greater durability and adaptability to technological changes. From this perspective, the ISOC Policy Framework suggests that liability policies should target not specific "types" of intermediary companies (such as "application providers," "social networks," "access providers," e.g.), but rather the "functions" of intermediation they implement.

This becomes especially relevant considering that, in the current digital ecosystem, many companies offer distinct services corresponding to vastly different types of intermediation, including across different layers of the Internet. Thus, the ISOC document provides a detailed and comprehensive list of intermediary functions performed by companies operating on the Internet, such as functions of communication from one person to another or from one person to many, and search mechanisms. The document also notes that complex systems, such as social media platforms, simultaneously perform multiple functions covered by this typology[7].

Given the potential impacts of this judgment on the Internet, we urge that any proposed measures be informed not only by legal rigor – as rightly emphasized by the justices – but also by the technical and organizational infrastructure of a complex ecosystem of diverse intermediaries. We believe it is essential that normative development processes related to the Internet be conducted transparently, openly, and inclusively, ensuring regulations effectively

---

[6] The Internet Society's Policy Framework is available in English here: https://www.Internetsociety.org/resources/doc/2024/a-policy-framework-for-Internet-intermediaries-and-content/. Starting on page 60, it provides an exhaustive list of digital intermediary types categorized by their functions.

[7] The Policy Framework for Internet Intermediaries and Content, developed by the Internet Society, details essential intermediary functions of the Internet, grouped into: 1) Transmission; 2) Routing; 3) Hosting/Caching; 4) Communications (Personal); 5) Search; 6) Cybersecurity/Privacy; 7) Software; 8) Complex Environments (e.g., social media platforms, which combine multiple functions).

fulfill their protective role for rights while establishing measures that are necessary and proportionate to the interests at stake, respecting the balance among affected sectors.

Second, in line with the Decalogue on Intermediary Liability, we argue that future discussions must focus on how proposed changes will be implemented in practice. This means clearly defining how regulation, penalties, and oversight will be structured and enforced.

These tasks could be carried out by specific judicial bodies or, for a time, through a combination of public oversight and independent commissions (as previously suggested in Justice Luis Roberto Barroso's vote). This point – often overlooked in detailed technical discussions – is critical. We must ensure that the interpretation of the rules does not distort the original intent of the law or create excessive and vague obligations for intermediaries. After all, the Civil Rights Framework for the Internet defines intermediaries broadly, not limited to large digital social media platforms, and it would be highly beneficial for the STF to keep these distinctions in mind.