
The Far-Reaching Implications of Brazil's Supreme Court Decision for Platform Governance

Beatriz Kira and Ivar Hartmann

In October 2025, Brazil's Federal Supreme Court declared Article 19 of the Marco Civil da Internet partially unconstitutional, fundamentally restructuring the country's intermediary liability regime. For nearly a decade, platforms could only be held liable for third-party content upon failing to comply with a specific judicial removal order, subject to limited statutory exceptions. Concluding that this model no longer afforded adequate protection to fundamental rights and democratic institutions, the Court replaced it with four distinct liability regimes while introducing a duty of care alongside new transparency and due-process obligations. This commentary examines the ruling and situates it within Brazil's institutional and political context, arguing that this decision reaches far beyond the allocation of liability in individual cases to influence broader governance arrangements applicable to digital platforms. Although adopted through constitutional adjudication rather than changes in legislation, the decision responded to pressing structural concerns and shifted Brazilian platform regulation toward a preventive, risk-oriented model that has helped to shape a hybrid framework combining judicial standards with regulatory supervision.

1 Introduction

Observers worldwide might be familiar with the proactive stance of Brazilian courts and especially the Federal Supreme Court (*Supremo Tribunal Federal*, STF) in relation to internet platforms (Nicas 2022). The STF famously blocked Telegram in 2022 (Hirabahasi and Tortella 2022) and again in 2023 (Lima 2023), and also suspended X for over a month in 2024 (Mendes 2024). However, the decision that is likely to have the most enduring implications for online speech came a year later. In October 2025, the STF redefined the intermediary liability framework established by the Internet Civil Rights Framework (*Marco Civil da Internet*, Law No. 12.965/2014, or MCI).

For nearly a decade, Article 19 of the MCI had functioned as the general rule governing platform liability: internet platforms could only be held liable for third-party content if they failed to comply with a specific court order requiring its removal. Alongside this judicial-order model, however, the MCI already contained limited exceptions, such as Article 21 on non-consensual intimate imagery and special rules for copyright law, allowing for extrajudicial notification to trigger liability. In its recent ruling, the STF declared Article 19 partially unconstitutional, holding that the model “does not afford sufficient protection to constitutional interests of high relevance” (*MCI Ruling 2025*, at 7), such as democratic institutions and the fundamental rights of vulnerable groups. The decision replaced the previous framework with a fourfold structure of liability, comprising a revised Article 19 regime, an expanded Article 21 regime, and two newly recognized forms of liability applicable to specific categories of content.

Beyond this reconfiguration of the liability regime, the Court articulated a set of transparency, governance, and due-process obligations. Many of the obligations and objectives reflected in the STF’s reasoning resemble those found in recent legislative initiatives such as the European Union’s Digital Services Act and the United Kingdom’s Online Safety Act, which embody the emerging expectation that platforms adopt proactive measures to protect users’ rights and mitigate harms that arise from the scale and dynamics of internet platforms. Yet in Brazil they emerged through constitutional adjudication rather than through the enactment of new legislation or a regulatory framework.

This commentary examines the decision and situates it within Brazil’s legal and policy landscape. We argue that the judgment marks a turning point in Brazilian digital regulation, replacing a model built on judicial orders with a layered framework that incorporates preventive obligations and procedural duties. The decision affects not only intermediary liability—the rules determining when platforms may be held responsible for content created by their users (Edwards 2009)—but also broader arrangements of platform governance, understood as the constellation of rules (including those on intermediary liability), institutions, and actors that shape the operation of digital platforms and their relationships with users, governments, and other stakeholders (Gorwa 2019).

Our analysis also provides a useful lens through which to examine how courts can influence the evolution of platform governance, particularly in settings where legislative responses remain incomplete or contested. Much of the existing literature examines platform decisions without reference to courts (Flew, Martin, and Suzor 2019), or analyzes the complex interplay between states, civil society and private companies in content moderation while leaving judicial review aside (Gorwa 2019). Yet courts can play an important role in platform governance through interpretation of constitutional rights and statutory provisions, influencing how responsibilities, duties, and safeguards are defined and applied to internet platforms. At the same time, online content moderation provides a particularly important setting for studying processes of judicial dialogue (Psychogiopoulou 2021). The STF’s decision therefore offers an opportunity to analyze

how courts influence the legal frameworks governing online speech.

The paper is structured as follows. Section 2 introduces key elements of the legal and political background leading to the ruling. It discusses how the courts, platform business models, and Brazil's political context have shaped the stakes of the STF's decision and identifies key actors and milestones in the national debate on digital regulation. Section 3 examines the decision itself, setting out the Court's reasoning and detailing the new liability framework and the additional, proactive duties it introduced. It shows that the ruling produced two major changes to the operation of digital platforms in Brazil: the establishment of four regimes of liability, and the recognition of new positive duties for intermediaries that may define the diligence standard shielding platforms from liability for systemic risks and provide the normative basis for future regulatory oversight. Section 4 assesses the broader implications for Brazil's platform regulation agenda, considering how the STF's decision may constrain or enable future reforms, and briefly analyses immediate institutional ripple effects, such as the May 2026 executive decrees, which reflect the impact of the ruling on platform governance in Brazil.

2 The Context of the Ruling

The ruling on Article 19 must be understood against the institutional and regulatory context in which the MCI was enacted. This section revisits the liability regime established by the MCI, the assumptions that informed its design, and the way it operated in practice over the decade following its enactment. It also situates Article 19 within Brazil's broader model of constitutional review, in which courts play a central role in mediating conflicts between fundamental rights and in shaping the practical contours of platform regulation. We make no claims of causality between any of the events described in this section and the STF decision. Rather, our purpose is to provide contextual information relevant to understanding the ruling and its possible effects.

2.1 The Making of the MCI

Brazilian society's relationship with the internet changed profoundly between 2014 and 2024, the decade separating the enactment of the MCI and the STF's decision on Article 19. In 2014, when Congress enacted the MCI, the Brazilian government had been implementing digital inclusion policies for more than a decade (Joia 2004) with positive results, but the digital literacy divide remained a problem (Nishijima, Ivanauskas, and Sarti 2017). Brazilians in the two lowest income brackets (classes D and E) made up close to a third of the population, while the middle bracket accounted for half (Neri 2019). In the bottom two income brackets, 21% of people were online, compared with 54% of those in the middle class (CGI.br 2015). In 2024, when the STF Justices began handing down their opinions on the MCI case, both shares exceeded 99% (CGI.br 2025). In the five years following the enactment of the MCI, mobile phones became the primary

device through which Brazilians accessed news, rising from 23% in 2013 to 77% in 2019 (Newman et al. 2019, 123). In 2023, Brazil ranked third in daily use of social media at an average of 3 hours and 37 minutes, 50% above the worldwide average (We Are Social 2024). The number of Brazilian internet users was radically larger and arguably so was that of the victims of abusive and illegal speech online. The internet now played a different role in Brazilian society and politics, with electoral disinformation increasing since 2018 (Ribeiro and Ortellado 2018). Although these developments cannot be said to have caused the STF ruling, the growth in internet access and use of internet platforms is critical to understanding the broader context in which the STF found itself in 2024.

The MCI, adopted in 2014 through a praised multistakeholder process (Brito Cruz 2015), established a distinctive intermediary liability regime that positions courts as central actors in platform regulation (Zingales 2015). It can be conceived as a middle path between the United States and European approaches. Unlike the broad immunity provided by the U.S. Communications Decency Act, the MCI did not grant platforms blanket protection. Yet, unlike European notice-and-takedown systems, for most cases it required a prior judicial order before a provider could be held liable for third-party content, with two exceptions: copyright infringements and image-based sexual abuse.

The element that makes Brazilian law clearly different from that of the U.S. is the level of restrictions to expression. Before and after the MCI, the law provided for a large number of viable claims against online content (Sarmiento 2006). Changing what types of expression are illegal was never the purview of the MCI. Instead, it provided courts with a rule for arbitrating when platforms would be held liable along with the speaker. Before the MCI, Brazilian courts agreed that platforms were by default vicariously liable for user content, but disagreed on what the circumstances were under which they might be exempt. What the MCI did was define precisely what platforms needed to do in order to achieve immunity.

Article 19 of the MCI set out the general rule: an internet application provider could only be held liable within tort law for damages caused by user-generated content if two conditions were met. First, there had to be a “specific court order” requiring the provider to “make the infringing material unavailable.” Courts interpreted the term “specific” narrowly, requiring that such orders identify the precise URL of the content in question (Souza and Lemos 2016, 88). Second, liability would arise only if the platform failed to comply with the order within the timeframe and technical limits established by the court. If the content was removed as instructed, the platform bore no liability.

This rule reflected a deliberate normative choice. Article 19 expressly stated that its purpose was “to ensure freedom of expression and to prevent censorship.” Stakeholders involved in drafting the legislation feared that under a private notice-and-takedown model, platforms would act as private censors, removing content pre-emptively to avoid liability (Brito Cruz 2015). The argument was that decisions about the legality of speech, such as whether it constituted defamation or hate speech, were understood as questions

involving legal interpretation, and thus should be the responsibility of judges and not of private actors. This reasoning carried particular weight in Brazil, where defamation and related offenses are criminal rather than civil matters. Declaring that a post was defamatory implied the possibility of criminal liability for the speaker, which further supported the view that only courts should make such determinations. Neither platforms nor their operators can be held criminally liable for user-generated content, and this has not changed following the STF ruling.

The Article 19 liability rule also applied uniformly to all “internet application providers,” the term the MCI used for any service offering functionalities through the internet. The law distinguished between access providers and application providers, but it made no further distinctions among the wide range of services that fell within this latter category. As Justice Dias Toffoli later observed in the recent Supreme Court’s decision, under the MCI, “an application provider is an umbrella concept that encompasses the most diverse functionalities and services,” including online marketplaces such as Amazon and Mercado Livre, messaging services such as WhatsApp and Telegram, social networks like Facebook and TikTok, email providers, and search engines (*MCI Ruling 2025*, at 106). Indeed, the broad wording of the law favored a form of technological neutrality, but failed to account for the very different scales, functions, and risks of these business models, and for the ways in which they evolved over time.

This judicial-order regime of liability was also coherent with Brazil’s constitutional emphasis on due process and judicial oversight, and civil society organizations strongly defended it as a necessary protection for freedom of expression during the MCI’s legislative process (Brito Cruz 2015). A foreign observer might be excused for believing that after the enactment of the MCI and before the STF ruling, a liability regime that requires a court order for takedown would have been hostile to victims seeking content removal. Compared to the likelihood and costs of obtaining a favorable court order restricting expression, however, Brazil was and remains a much more favorable jurisdiction for plaintiffs than the United States (de Freitas and de Castro 2013).

2.2 The Gradual Demise of Article 19

In 2023, 35 million new lawsuits were filed in Brazil, bringing the total to 83 million cases pending at the end of that year (Conselho Nacional de Justiça 2024). Access to courts is not uniform across the country and depends mostly on variables related to court staffing (Sátiro et al. 2025), but litigation costs are low, especially since plaintiffs can file content removal cases against platforms in small claims courts. Securing an injunction against online speech was easier in Brazil before 2024 than in most other countries.

Trial and appellate courts may exercise constitutional review in concrete cases and decline to apply a statutory provision they consider unconstitutional. In freedom of expression disputes, Brazilian courts have often adopted an expansive approach (Lancieri et al. 2026), treating the Constitution’s structure of competing fundamental rights as

authorizing frequent balancing between expression and privacy or honor. As C. I. Keller (2021) notes, the MCI's liability model places courts at the center of that process. This design choice may help explain a long-standing pattern in which some trial courts have disregarded Article 19 immunity and held platforms liable, sometimes without even engaging with the statute directly (Almeida, Leite, and Assis 2024). Such rulings do not generate binding precedent, and even when a lower court set aside the MCI rule, the effects extended only to the parties to the case. Over the years, thousands of content removal cases reached courts, and plaintiffs prevailed in roughly one out of three (Oliva 2019). Obtaining a favorable judgment was by no means a rare occurrence. Even a system in which courts were normally willing to exercise viewpoint-specific review of speech and order content removals proved unable to overcome the critique of excessive illegal content available on social media.

Over time, the judicial-liability model proved difficult to reconcile with the dynamics of modern social media, including industrial-scale content moderation (Caplan 2018) and algorithmic recommendation systems (Gorwa, Binns, and Katzenbach 2020) as well as with the complexities of one-to-many encrypted messaging apps (Santos et al. 2019). By the late 2010s, platforms had become central arenas for political mobilization, but also sources of disinformation, abuse, and harassment (Evangelista and Bruno 2019). The argument was often made that Article 19 of the MCI, by requiring a judicial order for each removal, exposed a growing gap between the pace of litigation and the speed of online communication (de Lima 2015). There were critics of the court-order-and-takedown regime ever since the MCI bill was drafted (e.g. Thompson 2016) and their stance became gradually more popular over time. At its core, the argument was that the MCI's design placed the most urgent moderation challenges on an already overburdened judiciary and insulated platforms from accountability for harms facilitated by their own systems (Schreiber 2015).

Public sentiment gradually shifted in favor of stronger regulation. By 2025, surveys showed that more than three-quarters of Brazilians supported stricter oversight of platforms (Nexus 2025). Scholars and policymakers increasingly agreed that the MCI, designed as a charter of rights for internet users, was not equipped to address the systemic influence of social networks, recommendation algorithms, and encrypted messaging (Kira et al. 2025; Machado et al. 2019). The MCI bill was submitted to Congress by the Federal Government under the Workers' Party. Over a decade later, the same party, back in power, felt the MCI's intermediary liability standard was too soft on platforms and warranted an update, but Congress refused to tighten the grip on platforms.

It was not for a lack of proposals. Over the years, several legislative proposals sought to amend the MCI. A majority introduced stricter standards of responsibility for platforms (Hartmann and Iunes 2020), while others, most notably supporters of Bill 2630/2020 (known colloquially as "The Fake News Bill"), aimed to build a comprehensive regulatory regime introducing duties of care, transparency, and oversight (Kira 2025). Despite

broad recognition of the need for reform, none of these legislative initiatives advanced. Brazil's polarized political climate and the intense lobbying efforts of large technology companies led to a persistent legislative stalemate (Brito Cruz, Kira, and Hartmann 2025). The context is somewhat similar to that of India, where a major ruling addressing ambiguities in the law on intermediary liability only came after a long silence from the legislature (Gupta and Srinivasan 2023).

Before the STF ruling, the Federal Government, through agencies and regulatory bodies, had been pushing the boundaries of other rules on liability, such as the Consumer Defense Code, to force a modicum of accountability on platforms (Hartmann et al. 2026). But it could not outright change the MCI. Trial courts remained willing to restrict online speech despite the MCI. More recently, the Brazilian Superior Electoral Court (TSE) had begun filling in the regulatory vacuum by addressing issues that directly affected online speech and platform governance during elections (Kira et al. 2025; Lancieri et al. 2026).

2.3 The STF Was a Willing Protagonist

The STF's 2025 ruling emerged within this setting of institutional dualism, where legislative inaction coexisted with judicial activism. Importantly, even when compared to Brazilian trial courts, the STF is uncommonly proactive and bold in reviewing online speech. This fits the Court's expansive strategy across most areas of Brazilian law. The STF is anything but a court that reads its own powers conservatively. While it mostly errs on the side of caution by aligning with general sentiment when deciding issues on which the public clearly supports a specific outcome, the Court does not shy away from challenging Congress (Taylor 2024). In both its willingness to defy powerful political parties and expand its powers as an institution—as well as those of its judges when ruling individually (Arguelhes and Ribeiro 2018b)—the STF is a far bolder apex court than the United States' Supreme Court.

The STF has also shown political will to push back against Congress (Da Ros and Taylor 2022) and its assertiveness regarding online speech has appeared in other contexts. In 2019, the Court launched a maximalist investigation into crimes against the honor of its Justices, later dubbed the “fake news investigation,” which has been the vehicle for violations of due process, a systematic concentration of powers and a high rate of secret prosecutions (Lorenzetto and Pereira 2020). The STF pivoted from the original goal of protecting the honor of its members to an investigation into politicians and dissidents for producing and spreading online disinformation to protect democratic institutions—which, to its credit, the STF did accomplish (Hartmann 2026).

More recent events compounded the political pressures in the period leading up to the start of the STF deliberations. Tensions between digital platforms and Brazilian authorities had escalated further in 2024. In August of that year, Justice Alexandre de Moraes ordered the nationwide suspension of X (formerly Twitter) after the company repeatedly refused to comply with court orders for content removal and account suspension, while

deliberately avoiding being legally served in Brazil (Jost and Brito Cruz 2024). The episode followed months of conflict between platforms and state institutions, including allegations that online networks were used to coordinate an attempted coup to depose President-elect Luiz Inácio Lula da Silva and the storming of federal buildings at Brazil's capital, Brasília, on 8 January 2023. These events underscored the fragility of Brazil's 2014 framework while highlighting the growing gap between the MCI's liability-focused and individualistic model and the realities of a globalized, large-scale, algorithmically driven digital environment.

The U.S. Supreme Court has always avoided ruling on the proper limits of legislative immunity for internet intermediaries, sidestepping the issue on procedural grounds (Garfield Tenzer 2025). Similarly, the STF waited ten years after the enactment of the MCI to meet a challenge to Article 19 head on. The MCI ruling was not a mere injunction or the result of an investigation but rather the exercise of constitutional review by the apex court. The STF can declare the unconstitutionality of statutes in abstract with *erga omnes* effect and also exercise constitutional review on appeals, when rulings usually will not generate binding precedents. The MCI case consisted of two appeals concerning intermediary liability, which normally would mean that the effects of the ruling would bind only the parties of the case. However, a mechanism called “general repercussion” allows the court to select an appeal that contains a nationally relevant constitutional issue and exceptionally to give the ruling on such appeal *erga omnes* effect, with binding effects throughout Brazilian law. The MCI case was tried under this “general repercussion” rule.

The Court itself framed the question in constitutional terms, concluding that Article 19 was “not fully capable of offering effective protection to fundamental rights and safeguarding the fundamental constitutional principles and values in virtual environments” (MCI Ruling 2025, at 6). But it is undeniable that the Court's reasoning was also shaped by the political climate. Indeed, the Court's decision specifically mentions the attacks on Brazil's Supreme Court and Congress on 8 January 2023, which it explicitly linked to the storming of the U.S. Capitol in 2021 (MCI Ruling 2025, at 117, 317). In both cases, the Court noted that online platforms had failed to contain the dissemination of content that incited violence and undermined democratic institutions. It was evident from the decision that, for the Justices of the STF, this concentration of private power, operating without transparency or accountability, constituted an active threat to the rule of law. The majority described this development as one of “progressive unconstitutionality,” suggesting that a framework initially compatible with constitutional guarantees back in 2014 had, in practice, become insufficient to protect them.

The decision, therefore, sits at the intersection of a series of developments. Article 19 expressed a legislative choice about how disputes over online speech would be resolved and who would be responsible for determining content illegality. A decade later, the digital and institutional landscape had changed significantly. Internet access

in Brazil had expanded at a remarkable pace, reshaping patterns of communication, political mobilization and exposure to harm. The operation of the Article 19 regime became increasingly contested in litigation and political debate. Public opinion supported stricter regulation and the Federal Government exercised creativity to pressure digital platforms. From 2014 to 2024, the STF continued to consolidate its role in resolving constitutional disputes with broad regulatory implications and began intervening firmly in online speech.

3 The Content of the Ruling: Analysis of the STF Decision

The Federal Supreme Court's recent judgment in two cases (classified as Themes 987 and 533 under the Court's general repercussion procedure) reshaped Brazil's approach to intermediary liability. Although the disputes arose years apart, they both turned on the same question: when, and under what conditions, can an online platform be held responsible for harmful user-generated content? This section revisits the facts of each case before turning to the Court's reasoning and ruling, which ultimately led to the partial invalidation of Article 19 of the MCI.

3.1 Facts of the Two Cases on Appeal

The two cases unfolded along different timelines. Theme 533 concerned events that occurred before the MCI was enacted in 2014, when courts had to rely directly on constitutional principles to arbitrate intermediary liability in the absence of a statutory framework. Theme 987, by contrast, involved disputes that took place after the MCI entered into force and tested whether its liability model continued to satisfy constitutional guarantees in a transformed digital environment.

The first case, known as the Aliandra case (Theme 533, RE 1057258, rapporteur Justice Luiz Fux),¹ originated in Minas Gerais in 2010. A schoolteacher, Aliandra Cleide Vieira, discovered an anonymous community on the then-popular social media platform Orkut titled *Eu Odeio a Aliandra* (I Hate Aliandra). On the page, its eight members mocked her appearance and personality. Aliandra requested that the page be suspended, but Google Brasil (owner of Orkut) refused to remove the page, stating that the content did not clearly violate any laws or infringe its policies. The teacher then filed suit seeking deletion of the page and compensation for the moral damages caused by the content. The appellate court sided with her, ordering removal and compensation of R\$10,000.00 (ten thousand Brazilian reais). Google complied with the order but appealed to the Supreme Court in 2011, arguing that no liability could exist without a prior judicial order.

1. Even though both RE 1037396 and RE 1057258 were decided together by the STF, the full text of the ruling for each case is not identical. Throughout this article, when we cite portions of the ruling and their specific pages, we are referring to the full text of the decision in RE 1037396, which is 1323 pages long. The full text of the RE 1057258 is similar, but not identical, comprising 1118 pages. To the best of our knowledge, there are no differences in the substance of the majority and minority opinions as they appear in both rulings.

A similar dispute emerged years later, in November 2014, under a new legal framework. In the Lourdes case (Theme 987, RE 1037396, rapporteur Justice Dias Toffoli), Lourdes Pavioto Corrêa discovered a fake Facebook profile using her photos and name to post offensive messages. She requested its removal and the disclosure of the perpetrator's identity, but Facebook refused, invoking Article 19 of the MCI, which conditioned liability on non-compliance with a judicial order. Lourdes then filed suit, seeking removal of the profile, disclosure of the IP address, and compensation for moral damages. The trial court ordered the profile's removal and the disclosure of the identity behind it, but denied damages. The appellate court partially reversed, holding Facebook liable and awarding compensation, while exempting the company from providing the IP address of the person responsible for the fake account. Facebook appealed to the STF in 2017, arguing that freedom of expression and the prohibition of prior censorship outweighed rights to honor and privacy, and that platforms could not be required to monitor user content proactively (*MCI Ruling 2025*, at 99–100).

By hearing these two appeals together, the STF could determine whether Article 19's model of judicial-order liability provided adequate protection for constitutional rights, or whether platforms should bear greater responsibility once notified of unlawful content. By the time the court began voting on the merits in 2024, 13 years had passed since the first case and 7 since the second reached its docket. The STF only handed down the decision in 2025.

3.2 Rationale of the Decision

The two appeals brought before the Court required a broader examination of the constitutional foundations of Brazil's intermediary liability regime. By eight votes to three, the Federal Supreme Court held that Article 19 of the Marco Civil da Internet was partially unconstitutional. The outcome, however, does not capture the range of constitutional positions expressed in the case.

In Brazil, high-profile constitutional disputes are decided through individual votes delivered in public session. Each Justice prepares a written opinion and presents it during a deliberation that is open to the public and frequently broadcast on television and online. The file with the final judgment opens with what the Court deems a "winning thesis" that synthesizes the binding position of the majority and, in some cases (such as the MCI case), produces *erga omnes* effects. The full opinions are published alongside that thesis, which makes it possible to trace the different lines of reasoning that converged in the final result.

Three Justices dissented from the majority opinion. Taken together, their arguments are simpler to understand and much less consequential than those of the majority, so we address them first before moving to the several majority concurring opinions. André Mendonça, Nunes Marques and Edson Fachin each defended the constitutionality of Article 19, though their arguments reflected different concerns about the allocation of

authority over online speech.

Justice Edson Fachin grounded his dissent in the idea that Article 19 embodied a deliberate legislative commitment to judicial oversight. Questions about the legality of expression, in his view, require case-by-case evaluation under constitutional parameters. Given the weight of the interests involved, courts remain the institution entrusted with that task. Allowing platforms to make such determinations, particularly for complex or ambiguous expression, would displace a function that the Constitution reserves to the Judiciary and would increase reliance on automated or discretionary filtering.

Justice André Mendonça offered a broader defense of the statutory framework. He rejected the characterization of Article 19 as a shield insulating platforms from responsibility and stressed that primary liability always lies with the author of the content. Platforms are required to comply with judicial orders and to assist in identifying users so that victims may seek redress directly. In his view, the existing model could be refined through a form of “regulated self-regulation,” with clearer compliance standards and differentiated obligations, especially in relation to private messaging services, which implicate the constitutional secrecy of communications. Expanding platform liability risked encouraging continuous monitoring and preventive removal of lawful speech.

Justice Nunes Marques likewise supported maintaining Article 19 as the general rule governing intermediary liability. He focused on the implications of granting platforms authority to remove content on their own initiative. Once companies assume responsibility for determining what remains online, they exercise significant influence over the boundaries of public discourse. Exposure to liability would tend to favor precautionary removal, particularly in disputes involving alleged “offenses against honor.” Civil responsibility, he emphasized, arises when speech exceeds legally defined limits, and even then it is the author, not the intermediary, who bears primary accountability.

These dissenting opinions reflect a shared concern with preserving the judicial-order model adopted in 2014, but the majority reached a different conclusion. In their view, the constitutional assessment of Article 19 could not be separated from the transformation of the digital environment over the past decade and from the scale at which platforms now mediate communication. The majority considered that the assumptions on which Article 19 had been built had weakened over time, a process the Court described as

“progressive unconstitutionality” (*inconstitucionalidade progressiva*).² But the reasoning supporting the majority opinion was not uniform. Although eight Justices endorsed the outcome, their separate opinions reveal distinct lines of argument that can be grouped into several strands. None of the eight concurred without filing a separate opinion, which is common in high-profile cases.

A first strand of reasoning revisited the balance among fundamental rights. The Court reaffirmed that Article 19 had been enacted to protect freedom of expression and to prevent private censorship by online intermediaries. Yet, over time, that design came to unduly restrict the effective protection of other constitutional rights such as privacy, intimacy, honor, image, and human dignity. These rights were identified as “constitutional interests of high relevance” that must be balanced in concrete cases rather than subordinated to expressive freedom (*MCI Ruling 2025*, at 4). The judicial-order requirement, the Court found, imposed excessive procedural and temporal barriers that left victims of digital harm without timely remedies and weakened the constitutional guarantee of access to justice.³

In addressing the protection of fundamental rights, several Justices referred to the impact of online harms on vulnerable populations, relying on empirical data and concrete episodes to illustrate their scale and distribution. Children and adolescents, women, and other communities disproportionately targeted by hate speech, exploitation and coordinated harassment featured prominently in these accounts. Justice Dias Toffoli cited figures from the Brazilian Forum on Public Security indicating a 48% increase, between 2022 and 2023, in the online dissemination of sexual abuse content, including material involving children and adolescents (*MCI Ruling 2025*, at 235). Justice Luís Roberto Barroso referred to data from Safernet showing that, in 2022, 74,000 reports of online hate crimes were submitted to the National Cybercrime Reporting Center, with xenophobia, religious intolerance and misogyny among the most frequently reported categories (*MCI Ruling 2025*, at 397). He also cited data indicating that, in the first week

2. The idea of “progressive unconstitutionality” was not introduced in this case. It refers to a form of constitutional review in which a statute that was compatible with the Constitution when enacted may, over time, become incompatible with it due to changes in factual circumstances. The premise is that constitutional validity is not assessed only at the moment of enactment. When social, economic, or institutional conditions shift, a norm’s continued conformity with constitutional principles may also change. An earlier example is the Court’s case law concerning the civil representation of persons in need. Under the 1988 Constitution, the Public Prosecutor’s Office was entrusted with representing vulnerable individuals, including victims of crimes. Over time, however, the Public Defender’s Office became the institution constitutionally designated to provide legal assistance to the vulnerable. The STF acknowledged that this institutional shift gave rise to a process of progressive unconstitutionality in relation to the continued exercise of that function by the Public Prosecutor’s Office. It nevertheless concluded that the process had not yet culminated in invalidity, since in many parts of the country the Public Defender’s Offices were still being established or lacked sufficient structure to assume the role fully. See RE nº 135.328-7/SP, DJ 1 August 1994.

3. Several Justices referred to proportionality in their votes. Justice Cristiano Zanin provided what was perhaps the most structured application of the proportionality test, explicitly adopting a three-step analysis of suitability, necessity and proportionality *stricto sensu*. He concluded that the existing regime placed freedom of expression in a position of unjustified superiority and imposed a disproportionate sacrifice on other constitutional values, including dignity and equality, while concerns about overblocking remained largely speculative. The final thesis, however, did not formally organize its reasoning around a proportionality test, instead emphasizing the inadequacy of the current framework in protecting fundamental rights and the resulting protection deficit.

of the 2022 electoral campaign, 97 female candidates were subjected to nearly 4,500 attacks or insults on a single social media platform (*MCI Ruling 2025*, at 398). In his vote, Justice Alexandre de Moraes displayed screenshots of posts that platforms had failed to remove or classified as compliant with their community standards, including overtly racist, homophobic and antisemitic content (*MCI Ruling 2025*, at 1013–19).

These examples supported the Court’s understanding that digital violence affects particular groups in patterned and recurrent ways. The judgment treated these patterns of harm as giving rise to a distinct category of factual and legal vulnerability, described as “digital vulnerability,” which falls especially on women, children and adolescents. The final thesis relied on Article 5 of the Constitution, which enshrines equality and non-discrimination, and on Article 227, which establishes a duty of comprehensive protection of children and adolescents (*MCI Ruling 2025*, at 6–7). The Court read these provisions as requiring timely and effective responses to digital violence impacting vulnerable groups. Against that constitutional framework, the majority concluded that a model centered on platform self-regulation through content moderation, combined with liability conditioned on prior judicial orders, and the absence of specific public policies adopted by the Legislative and Executive branches, produced what it termed a “protection deficit” for fundamental rights on the internet.

Central to the Court’s normative claims is a somewhat narrow assessment of the current moderation practices of platforms. Such practices include voluntary moderation of both legal yet abusive content and illegal content, as well as compliance mechanisms designed to receive and enforce the large number of court orders directed at platforms. Much like the U.S. Supreme Court in *Twitter v. Taamneh* (D. Keller 2023), the STF largely understated or downplayed the complex and repressive (Kaye 2019) voluntary moderation systems employed by social media. Both courts assumed a level of platform passivity that does not match reality while curiously reaching opposing conclusions: the U.S. Supreme Court preserved and the STF significantly curtailed intermediary liability rules.

A second strand of reasoning focused on the technological and economic transformation of the digital environment, which the majority viewed as having eroded the factual and legal premises of Article 19. The Court agreed that the rule, conceived in 2014 under the assumption of platform neutrality, no longer reflected the structural reality of global digital intermediaries. Justice Dias Toffoli, the rapporteur, cited the position of lawyer and scholar Gustavo Binenbojm to state that “if it [Article 19] was once constitutional, when it was enacted, it has moved toward unconstitutionality in light of the reality of relations that take place in the world of social networks” (*MCI Ruling 2025*, at 97). He described the system of judicial notification as one that “penalizes the victims of online offenses” (*MCI Ruling 2025*, at 152) and “is incapable of keeping pace with the speed of information dissemination on the internet” (*MCI Ruling 2025*, at 160). For Toffoli, platforms are “no longer mere intermediaries” but active participants that “manage the informational flow of their ecosystems” (*MCI Ruling 2025*, at 139). It is perhaps a

reflection of how the debate on platform governance has shifted over the years that the Indian Supreme Court in 2015 proactively protected intermediary safe harbor based on a court order for removal, in contrast with the most recent trend toward a liability standard that requires proactive measures (Gupta and Srinivasan 2023). A decade later, the STF all but abandoned the court-order-and-takedown model.

Other members of the majority developed similar arguments. Justice Luís Roberto Barroso observed that “the factual and legal bases that once justified the regime defined by Article 19 of the Marco Civil da Internet evidently have not withstood the passage of time” (*MCI Ruling 2025*, at 392). He noted that the “algorithmic design of these platforms privileges engagement and virality” (*MCI Ruling 2025*, at 402), amplifying disinformation and violent speech, and concluded that the regime “no longer affords sufficient protection to constitutional interests of high relevance, such as the protection of fundamental rights and democracy” (*MCI Ruling 2025*, at 331). Justice Gilmar Mendes added that the immunity provided by Article 19 “rests on a premise [of neutrality] that no longer exists in practice” since platforms act as “true regulators of online discourse” (*MCI Ruling 2025*, at 808). Several other Justices, including Luiz Fux and Flávio Dino, echoed this concern, stressing that the delay inherent in judicial proceedings and the scale of online communication make the 2014 model incapable of providing real-time protection for fundamental rights.

A third strand of reasoning situated this constitutional insufficiency within Brazil’s democratic context. The majority warned that the absence of effective accountability for online intermediaries “interferes in political and electoral processes and undermines democratic institutions” (*MCI Ruling 2025*, at 6). The judgment referenced the country’s recent experience with coordinated disinformation and political violence, including the attacks on the National Congress on 8 January 2023, drawing a parallel with the events of 6 January 2021 in the United States. The Court concluded that online platforms now play a constitutive role in the formation of public discourse and that legal frameworks must take into account the structural effects of algorithmic amplification and economic incentives on collective deliberation.

Although the Justices agreed on the need to reinterpret Article 19 to address these new realities, they differed on how this constitutional recalibration should translate into liability. Justice Dias Toffoli, the rapporteur, argued that requiring victims to prove fault imposes “an abyssal technical and informational inequality” that creates “an almost insurmountable barrier” to obtaining redress (*MCI Ruling 2025*, at 193). He invoked liability based on risk, a common basis for consumers to demand compensation from product and service providers in Brazil, to suggest that platforms, by profiting from the circulation of harmful material, engage in activities that inherently generate risk and therefore should bear heightened responsibility.⁴

4. *MCI Ruling (2025, at 85–87)* makes reference to the theory of intermediary liability based on risk developed by Brazilian scholar Antonio Junqueira de Azevedo.

Other Justices accepted the need for stronger safeguards but resisted strict or objective liability. Justice Luís Roberto Barroso maintained that “there is no known system in democratic nations that adopts objective responsibility for content intermediaries,” describing such a model as “disproportionate and unrealistic” and warning that it would lead to excessive removals and a chilling effect on expression (*MCI Ruling 2025*, at 425). He proposed reframing the analysis around a “duty of care,” a subjective standard focused on negligence and systemic failure rather than strict liability.

The Court ultimately adopted this approach. The final thesis of the judgment makes clear that “there will be no objective responsibility in the application of the thesis enunciated here” (*MCI Ruling 2025*, at 9). All four liability regimes recognized by the decision operate within a framework of subjective liability. Platforms are not automatically liable for third-party content; liability arises when they act negligently or fail to exercise the diligence that constitutional values require. What constitutes negligence or fault, however, varies across each regime.

In sum, the Court’s reasoning shows the Justices viewed the decision as an attempt to realign constitutional principles with internet platforms’ current business models. The judgment did not abandon the MCI’s protection of free expression entirely but recognized that its framework no longer ensured adequate protection of other fundamental rights. By addressing both the deficits of Article 19 and the growing problem of digital vulnerability, the Court sought to situate platform regulation within the broader constitutional duty to protect rights and democracy. The next section turns to how this reasoning was translated into four liability regimes and new proactive obligations for platforms.

3.3 The New Liability Regimes

The STF’s ruling replaced the single liability model created by Article 19 of the Marco Civil da Internet (MCI) with a differentiated framework consisting of four main regimes (Table 1). These regimes vary according to the nature of the platform and the type of content involved, forming a layered system that seeks to make platform liability more proportionate to the nature and scale of the risks they pose.

3.3.1 Article 19, the judicial-order regime: Crimes against honor and private communications

The first regime preserves the model of Article 19 (which was declared only *partially* unconstitutional), under which internet application providers could only be held liable for third-party content if they failed to comply with a judicial order requiring its removal. The Court maintained this rule for “crimes against honor” (defamation, slander, and calumny) and for certain categories of services, including email providers, platforms used for private video or voice meetings, and instant messaging services when the communication is interpersonal and protected by confidentiality.

This preservation of Article 19 was intended as a safeguard for freedom of expression. The Court reasoned that entrusting platforms with the task of assessing the legality of content involving crimes against honor risked overenforcement and undue restrictions on legitimate criticism, since drawing the line between criticism and defamation requires difficult legal interpretation. Justice Barroso was explicit on this point, arguing that “whenever there is reasonable doubt about the illicitness or otherwise of a manifestation, one must, indeed, await a judicial order” (*MCI Ruling 2025*, at 321). He further noted that accusations framed as crimes against honor “commonly convey criticism of the government, public officials, and people in general,” as well as reports of misconduct, such that judicial supervision is needed “to prevent censorship and attempts to silence people or conceal censurable, dishonest, or criminal facts” (*MCI Ruling 2025*, at 419–20). In line with this reasoning, Barroso proposed, and the majority agreed, that Article 19 should be preserved in specific scenarios to protect high-value political expression and to prevent a chilling effect on public debate.

At the same time, the final thesis added a narrow but significant exception to this preservation of judicial control. Even for crimes against honor, once a court has recognized a specific statement as unlawful, platforms are not required to wait for a new judicial order every time the same material circulates. The ruling specifies that, “in cases of successive replications of the offensive act already recognized by judicial decision, all social media providers must remove posts with *identical* content, irrespective of new judicial decisions, upon either judicial or extrajudicial notification.” This provision streamlines the handling of *identical* repetitions of already adjudicated unlawful speech, while preserving the requirement of judicial assessment for the initial determination, although in practice this may prove difficult to implement. A civil federal court in Argentina reached a similar compromise in a defamation case, rejecting a platform obligation to filter all future content and instead relying on proportionality to decide that intermediaries need only remove specific posts indicated by the victim (Tuchtfeld 2024).

3.3.2 Article 21, the notice-and-takedown model: Unlawful content and inauthentic accounts

The second regime builds upon Article 21 of the MCI, which previously applied only to cases of non-consensual intimate imagery. Article 21 provides that:

Art. 21. *An internet application provider that makes third-party content available shall be subsidiarily liable for violations of privacy arising from the unauthorized disclosure of images, videos, or other materials containing scenes of nudity or private sexual acts when, after receiving notification from the participant or their legal representative, it fails to act diligently, within the scope and technical limits of its service, to make such content unavailable.*

The STF judgment expanded this rule to include other types of unlawful content and inauthentic accounts. Under this model, liability no longer depends on a judicial order but

on the provider's knowledge of the violation, which arises from extrajudicial notification. Once notified, the provider must act diligently and within the technical limits of its service. If it remains passive, it may be held liable for resulting damages. In other words, the Court established that liability arises when a provider, after receiving an *extrajudicial notice* identifying specific unlawful content or an account reported as inauthentic, fails to act diligently and within its technical limits to make the material unavailable.

This change represents a shift from judicial to notice-based responsibility, adding a new layer to the liability system in Brazil. The Court drew on the logic of Article 21 to create a general rule for unlawful content, in practice establishing a mechanism of notice and takedown. In this system, a provider's knowledge of the illegality is sufficient to trigger liability, while judicial intervention is reserved for cases requiring complex interpretation, such as defamation. The choice to include inauthentic profiles within the Article 21 rules could also be explained by the fact that one of the cases being judged, RE 1037396 (Theme 987), concerned a fake profile used for a sustained campaign of offensive posts.

The Court considered that this extension ensures more effective protection of rights, but emphasized that there was no general obligation to monitor content. Liability under Article 21 thus depends on the provider's knowledge of the illegality through notification.

3.3.3 The “presumed knowledge” regime: Paid content and bots

A third regime applies to situations in which a provider is presumed to have knowledge of illegal content even without notification. The judgment provides that:

[P]roviders are presumed to be responsible for illegal content when it involves (a) paid advertisements and boosted content, or (b) artificial distribution networks (bots). Providers shall be exempt from liability if they prove that they acted diligently and within a reasonable time to make the content unavailable.

This regime, thus, covers two contexts: a) paid advertisements and boosted content, and b) artificial distribution networks operated by bots. In both, the Court considered that platforms exercise a degree of control that justifies an assumption of knowledge. For paid or boosted posts, this control arises from the platform's prior review and monetization of material. Justice Gilmar Mendes described this as a “presumption [...] applicable in the cases of advertisements and paid boosting,” noting that the process of pre-publication review “establishes a presumption of effective knowledge of illicit content,” which in such cases does not require prior notification for the purpose of civil liability (*MCI Ruling 2025*, at 816). Even so, the final thesis generated ambiguity by referring to a “presumption of liability,” a formulation that risked implying strict or objective responsibility. Justice Luís Roberto Barroso emphasized that the presumption should concern *knowledge* rather than responsibility itself (*MCI Ruling 2025*, at 425).

Read together, Barroso's and Mendes's statements suggest the following understanding:

the presumption attaches to knowledge in contexts where the provider's active role makes ignorance implausible, but liability still depends on proof of negligence or omission. Under this interpretation, the regime functions primarily as a burden-shifting mechanism. Once the content falls into one of these categories, the provider must show that it acted diligently and within a reasonable time after becoming (or being deemed) aware of the illegality. This logic is coherent for paid content, where pre-approval and monetization create a viable basis for a legal presumption of knowledge by the platform and for evaluating diligence.

Its application to automated distribution networks, however, remains unclear. Bots may operate without human review, and the decision does not define "knowledge" in this context or how diligence can be demonstrated. The presumption therefore poses interpretive and evidentiary challenges: it is uncertain whether the Court intended a rebuttable presumption of knowledge or a more general expectation that providers maintain detection systems against automated dissemination of unlawful material.

Overall, the presumed knowledge regime illustrates the STF's effort to link the degree of platform responsibility to the level of control exercised over content circulation and monetization. It seeks to preserve the principle of subjective liability but increases the standard of diligence in contexts where the provider's economic and technical role makes awareness of illegality reasonably foreseeable.

3.3.4 The duty of care regime: Gravely illegal content and systemic failures

The fourth regime represents perhaps the most innovative element of the judgment. It concerns cases of large-scale dissemination of "gravely illegal content" and creates a regime of liability for systemic failure. According to the thesis adopted by the Court:

In cases of mass circulation of gravely illegal content, the internet application provider is liable when it fails to ensure the immediate unavailability of content that constitutes serious crimes. The liability established in this item concerns the configuration of systemic failure. Systemic failure, attributable to the internet application provider, is defined as the omission to adopt adequate measures of prevention or removal of the illegal content previously listed, constituting a violation of the duty to act responsibly, transparently, and cautiously.

The regime, therefore, does not attach liability to the non-removal of a specific post but to breakdowns in the platform's broader preventive systems. The Court characterized this as a form of subjective liability based on negligence or omission, though under a heightened standard of diligence. Justice Luís Roberto Barroso emphasized that "the failure must be systemic, not merely the absence of removal of a specific item of content" (MCI Ruling 2025, at 340), distinguishing the duty of care from a general obligation of active monitoring, which the Court rejected as incompatible with the constitutional

prohibition of censorship (*MCI Ruling 2025*, at 432).

The decision also clarifies what compliance requires. Adequate measures are those that, “according to the state of the art, provide the highest levels of safety for the type of activity performed by the provider” (*MCI Ruling 2025*, at 18). Platforms therefore bear an obligation of means rather than of result, as we have argued along with other co-authors (Hartmann et al. 2026): they must adopt preventive and remedial mechanisms capable of addressing the forms of criminal content the Court identified as sufficiently serious to trigger this duty. To that end, the decision provides a closed list of offenses for which the duty of care applies, comprising:

- Crimes against the “Democratic Rule of Law”
- Terrorism or preparation of terrorism
- Inducement, incitement, or assistance to suicide or self-harm
- Incitement to discrimination based on race, color, ethnicity, religion, national origin, sexuality, or gender identity (homophobic and transphobic conduct)
- Misogyny
- Sexual crimes against vulnerable persons, child sexual abuse, and serious crimes against children and adolescents
- Human trafficking

In *Twitter v. Taamneh*, the appellant explicitly questioned the U.S. Supreme Court whether an intermediary can be liable for terrorist activity on its platform—more specifically, for actively recommending content that radicalizes users and helps recruitment. Although the appellants never brought the STF anything resembling online terrorism issues, the court actually ruled on the same matter as the U.S. Supreme Court but with a much less piecemeal approach. The distinction reveals much about the potential downsides of the STF decision. The U.S. Supreme Court entered into minute details regarding the role of the platform that might trigger liability, such as substantial assistance and what that would look like (Parr 2024, 558). The STF left intermediaries with less foreseeability as failure to provide the “highest levels of safety” may be a hard threshold to identify and one that outlines the liability by omission that the U.S. Supreme Court expressly denied in *Twitter v. Taamneh* (Parr 2024, 559).

The STF decision left unanswered the question of who will determine whether a systemic failure has occurred. It is unclear whether this assessment will remain within the judiciary or fall under the purview of a regulatory authority. The fact that the Court makes an explicit appeal for legislative action to establish a supervisory framework suggests a preference for an administrative model of oversight. Such determinations will likely depend on compliance and auditing standards to be defined by regulation, drawing on the annex and instrumental duties that the judgment introduced (discussed below). In practice, this would mean that a specialized authority, rather than individual courts, would be responsible for assessing whether a platform has met the expected standard of diligence

or has failed in its duty of care.

While the ruling does innovate in providing this duty of care model of liability, the notion of a duty of care was not entirely new to Brazil's digital-regulation landscape. Although not yet codified in statute, it had already appeared in institutional practice. Justice Cármen Lúcia, then also serving as President of the Superior Electoral Court, recalled during the STF's deliberations that the duty of care had been incorporated into the TSE's 2024 resolution on online campaigning for municipal elections.

Notably, TSE Resolution 23,732/2024 already requires providers to adopt terms of use and prevention efforts to avoid or minimize the use of their services in the practice of electoral misconduct (Kira et al. 2025). In Paragraph 4 of Article 9-D, the resolution states that a series of measures and obligations for platforms stems “from the social function and the duty of care of application providers, which guide their terms of use and prevention efforts to avoid or minimize the use of their services in the practice of electoral misconduct, and do not depend on notification from the judicial authority.”⁵

The European Court of Justice (ECJ) and the European Court of Human Rights (ECHR) have produced a series of precedents on intermediary liability that bear resemblance to the approach selected by the STF for gravely illegal content. There is a parallel in the contrast between a legal provision setting the same standard for multiple types of illegal user speech—as both the European Union E-Commerce Directive and Article 19 of the MCI did—and applying jurisprudence that creates distinct outlines for intermediary liability depending on whether the user content can be characterized, for example, as hate speech (Angelopoulos and Smet 2016, 275). A decade before the STF, the ECHR decided that an intermediary was strictly liable for user hate speech in *Delfi v. Estonia* (2015), but notice-and-takedown was effective in shielding the intermediary from liability over defamation in *MTE v. Hungary* (2016).

Both ECHR cases followed reasoning established by the ECJ in earlier cases regarding injunctive relief against platforms for copyright violations that acknowledged, much like the STF, that deciding what internet intermediaries are legally mandated to do about illegal user content is, at its core, a matter of arbitrating a clash of fundamental rights. The answer offered by the European courts was to establish a balancing test. In *UPC Telekabel Wien* (2014), a copyright case, the ECJ decided that an intermediary was safe so long as it i) avoided going overboard and unduly depriving users of lawful content and ii) avoided or made difficult access to illegal content while also discouraging its users from viewing it (Angelopoulos and Smet 2016).

This caselaw sets overall guidelines for content moderation best practices that, if followed, would allow intermediaries to avoid injunctions or liability claims. For gravely illegal content, the STF has done the same. Both in Europe and in Brazil, this approach,

5. Available at: <https://www.tse.jus.br/legislacao/compilada/res/2024/resolucao-no-23-732-de-27-de-fevereiro-de-2024>

Table 1: Civil liability regime for application providers. According to the thesis adopted by the STF in the judgment of Themes 987 and 533.

Liability regime	Applicable rule	Content type
1. Requires a court order for content removal and liability.	Article 19 of the MCI	Crimes against honor (defamation, slander and related offenses).*
2. Liability for damages based solely on extrajudicial notification.	Article 21 of the MCI (notice and takedown)	Crimes or illicit acts, including inauthentic accounts. Includes image-based sexual abuse content, which already followed this regime.
3. Liability for damages based on presumption of knowledge, even without notification. Exemption from liability if due diligence and timely action are proven.	New rule	Paid advertisements, sponsored content, and artificial distribution networks (bots).
4. Liability for systemic failure in failing to adopt adequate preventive or removal measures for content that constitutes serious crimes.	New rule	Mass circulation of gravely illegal content. Breach of duty of care and configuration of “systemic failure.”

* Applies to email service providers, application providers for private meetings (video/voice), and instant messaging providers (exclusively for interpersonal communications).

despite its merits, fails to ensure a sufficient degree of legal certainty for platforms. What are the “highest levels of safety”? What counts as making access to illegal content properly difficult? In both jurisdictions, the courts—as the legislators before them—are foregoing their obligation to provide a legal framework that settles how the balance between fundamental rights is to be struck (Angelopoulos and Smet 2016, 282).

By framing it as a duty of care, the STF at least connects its formulation with pre-existing regulatory approaches: it reinterprets the duty of care as a broader concept applicable to platform governance in Brazil, one that links preventive diligence, transparency, and risk management, all concepts that have been employed by Brazilian courts across different legal fields for many years (Hartmann et al. 2026).

3.3.5 Residual regimes: Marketplaces and electoral content

The Court also addressed certain residual areas that do not fit neatly within the four main liability regimes: digital marketplaces and electoral content. These carve-outs demonstrate the limits of the new framework and the Court’s effort to preserve coherence with existing branches of Brazilian law.

In relation to marketplaces, the Justices disagreed on whether such platforms fell within the scope of the ruling. Justice Barroso maintained that the matter should not form part of the decision, observing that it “had not been the object of the debate in the

main appeals” (*MCI Ruling 2025*, at 304, 354). In his view, extending the ruling to e-commerce platforms would exceed the scope of the general repercussion theme, which concerned only intermediary liability for user-generated content under the Marco Civil da Internet (MCI) (*MCI Ruling 2025*, at 303). Justice Dias Toffoli disagreed, affirming that “the issue was debated in the public hearings and falls within the broad scope of the general repercussion theme” (*MCI Ruling 2025*, at 354). He argued that the general rule for marketplaces should be the Consumer Defense Code (CDC), with specific objective liability carve-outs (*MCI Ruling 2025*, at 355).

The final thesis of the judgment reflected both positions without resolving their tension. It states that “internet application providers that operate as marketplaces are civilly liable in accordance with the Consumer Defense Code (Law No. 8.078/1990)” while also reaffirming that “there will be no objective liability in the application of the thesis enunciated here.” Read literally, these two statements appear to be at odds.

A plausible interpretation is that the decision implicitly creates a hybrid model. For activities that fall within consumer relations (sales of goods or services) the CDC continues to govern, imposing objective and joint liability, for example in cases of a defective product. For matters related to content moderation or platform governance, the subjective standard of diligence developed under the MCI and elaborated in the STF’s judgment would prevail. This reading reconciles the two parts of the decision and reflects the Court’s broader effort to harmonize existing consumer-protection law with the new framework for intermediary liability.

Still, significant uncertainties remain. The decision does not specify how mixed situations should be treated, such as the advertising of prohibited or uncertified products, nor does it clarify how the boundary between commercial and expressive activity will be drawn in future litigation. The result is an interpretative gap that points back to the need for legislative clarification. The STF provided the contours of a solution but left its details to be defined through future regulation.

A second residual category concerns electoral content, which the STF expressly excluded from the general regimes. The final thesis provides that internet application providers “are subject to civil liability, except where the specific provisions of electoral legislation and the normative acts issued by the Superior Electoral Court (TSE) apply.” This clause preserves the TSE’s jurisdiction over electoral matters and the comprehensive regulatory regime it has already developed to address online campaigning, misinformation, and political advertising (Bentes 2023). In practice, this means that content related to elections (such as campaign materials, electoral propaganda, or paid political advertisements) during the electoral period remains governed by the Electoral Code and by the TSE’s resolutions rather than by the general liability or duty-of-care rules set out by the STF.

The distinction also reflects an institutional division of labor. As previously mentioned, the TSE has, in recent years, advanced its own framework of platform obligations, including

transparency requirements for political advertisements, restrictions on paid boosting during electoral periods, and safeguards for the use of artificial intelligence in campaigns (Kira et al. 2025). Notably, as mentioned by Justice Cármen Lúcia during the court proceedings, these electoral rules already embody a version of the duty of care (*MCI Ruling 2025*, at 328). The STF's ruling thus reaffirms rather than replaces this existing system, ensuring that electoral integrity remains under the TSE's oversight.

3.3.6 Annex and instrumental duties

Beyond redefining liability regimes, the STF ruling introduced an additional layer of norms governing user-to-user application providers: a set of proactive duties, referred to by the Court as “annex and instrumental” duties, that determine how providers must structure their internal systems of moderation, transparency, and accountability (Table 2).

The judgment portrays these obligations as an exercise in self-regulation (*autorregulação*), requiring that internet application providers “adopt self-regulatory rules that necessarily include a notification system, due process guarantees, and annual transparency reports regarding extrajudicial notifications, advertisements, and sponsored content.” In effect, the Court transformed the idea of self-regulation about content moderation decisions into a regulated governance framework concerning procedural guarantees: platforms must formalize their moderation systems, document their procedures, and publish the outcomes through transparency reporting.

The decision further details these annex and instrumental duties. Providers must make available “specific service channels for users and non-users, preferably electronic, accessible and permanently publicized on their platforms.” They must ensure that internal moderation rules and complaint procedures are “published and reviewed periodically, in a transparent and publicly accessible manner.” In addition, every company operating in Brazil must “establish and maintain a headquarters and a legal representative in the country,” with powers to respond before administrative and judicial authorities, to supply information on moderation processes, to comply with judicial orders, and to satisfy financial penalties arising from breaches of legal or judicial obligations.

Taken together, these provisions suggest that the Court views procedural transparency and local accountability as important components of platform governance. While the judgment does not explicitly link the annex duties to the liability framework, they can be read as helping to define the standard of diligence underlying the duty of care. The systems for notification, review, and reporting required here could provide measurable indicators of whether a provider has acted responsibly to prevent or mitigate harm. In this way, the annex and instrumental duties could be seen as a bridge between the liability regimes, particularly the duty of care regime, and the broader expectation that platforms maintain governance structures capable of addressing systemic risks. Either way, the ruling goes well beyond answering the question brought by the appellants.

Table 2: Annex and instrumental duties.

Category	Annex and instrumental duty
Notification system	System for notifying about moderated content or accounts
Transparency	Preparation of annual transparency reports (regarding extrajudicial notifications, ads, and sponsored content)
Due process	Right to appeal moderation decisions
Support channels	Provide specific support channels for users and non-users, accessible and permanently disclosed on platforms
Publication and review of rules	Periodically publish and review internal rules and procedures transparently and accessibly to the public
Legal representation in Brazil	Establish and maintain headquarters and a legal representative in the country with full powers to respond judicially and administratively, and to provide information to authorities

The decision, however, leaves enforcement unresolved. The STF appealed to Congress to establish or designate an authority with the competence to audit transparency reports, monitor compliance, and impose sanctions. Yet the broader regulatory framework needed to make these duties operational remains undefined. It is still unclear how such an authority would interact with the courts in overseeing the liability regimes or how judicial and administrative enforcement mechanisms would coordinate in practice.

4 Implications of the Ruling

The STF stepped into a legislative vacuum left by the failure of the Brazilian Congress to pass comprehensive platform regulation. For several years, proposals had been developed in Congress but failed to become law. A prominent example was Bill No. 2630/2020, which sought to create a comprehensive duty of care framework obliging platforms to detect and mitigate systemic risks, including disinformation and threats to electoral integrity. Despite Senate approval, the bill stalled in the Chamber of Deputies after years of lobbying and polarization and was effectively shelved in 2023. As discussed in Section 2, this left a visible regulatory gap alongside strong political demand for responses to online harms. The STF attempted to fill this policy gap by reinterpreting the existing framework to align it with current technological realities. In doing so, the Court performed a role typically reserved to the legislature. The final thesis recognizes this by explicitly appealing to Congress to draft legislation to address existing deficiencies and to define a regulatory body (*MCI Ruling 2025*, at 13).

From a pragmatic perspective, the decision can be read as a functional response to congressional paralysis: a means of keeping the law relevant to the speed and scale of digital networks. Yet from an institutional standpoint, it blurs the line between adjudication and law-making. For readers unfamiliar with Brazil's legal system, the STF

decision may appear unusually legislative in scope. It stands in stark opposition to that of the ECHR in *Delfi v. Estonia* (2015). Like the STF, the ECHR dealt a monumental blow to intermediary immunity by confirming that a news portal was strictly liable for user expression in its comments section despite the European Union E-Commerce Directive forbidding Member States from requiring platforms to filter user content (Brunner 2016). However, the ECHR did not touch social media liability, as it greatly restricted the scope of its ruling by claiming it only applied to “a large professionally managed Internet news portal run on a commercial basis which published news articles of its own and invited its readers to comment on them” (*Delfi v. Estonia*). According to an ECHR judge, the main motivation for refraining from establishing a broad precedent was the fact that Delfi constituted the court’s very first ruling on intermediary liability (Spano 2017). The STF did not share such caution in its first ruling about MCI Article 19.

The explanation might lie in the STF’s overall approach to judging and not in its understanding of the challenges of regulating online speech. Judicial norm-creation is not exceptional in Brazilian constitutional practice. The Court often puts itself at the center of regulatory and policy debates in Brazil (Arguelhes and Ribeiro 2018a). Some Brazilian scholars argue that the STF is justified in most of its bolder moves restricting online speech amid serious threats to democratic institutions during and right after the far-right presidency of Jair Bolsonaro (Vieira 2023). In the MCI ruling, however, the STF performed expansive, forward-looking, norm-creation, not reactive, defensive restrictions of individual instances of online expression. What is distinctive here is the breadth of the STF’s intervention: the judgment reads less as the interpretation of a statute and more as the drafting of one. By introducing four liability regimes and a comprehensive set of procedural duties, the STF moved beyond statutory interpretation into the terrain of regulatory design, in an expansion that some will probably regard as constitutionally creative and others as exceeding judicial authority.

From a substantive perspective, two subsequent developments demonstrate the ripple effects of the STF ruling on platform governance in Brazil. The first is the enactment of Law No. 15.211/2025 in September 2025, commonly known as ECA Digital, which established new online protections for children and adolescents. The second involves two executive decrees published in May 2026 that updated the regulatory framework of the MCI to reflect the STF’s new interpretation. These instruments solidify two core features introduced by the STF decision. First, they formally embed proactive duties for platforms, specifically the concept of a duty of care connected to the prevention of systemic failures. Second, they designate a central administrative regulator to oversee these new positive obligations.

Regarding the duty of care, the MCI ruling recast responsibility as an ongoing obligation to prevent foreseeable risks through internal governance. This *obligation of means* requires platforms to demonstrate that they have adopted systems that identify and mitigate risks (Hartmann et al. 2026). Justice Luís Roberto Barroso made this preventive orientation

explicit, stating that “with respect to the duty to mitigate systemic risks, the National Congress is called upon to regulate the measures necessary to assess and minimize those risks, including the preparation of impact reports and audits, as well as to define the sanctions and a regulatory authority responsible for conformity analysis, monitoring, and the eventual application of sanctions” (*MCI Ruling 2025*, at 340).

The STF framework has already begun to evolve into a more fully developed regulatory regime through subsequent legislative action. ECA Digital creates specific obligations for digital service providers regarding access control and the protection of minors using applications, electronic games, and social networks. During the legislative process, the rapporteur of the bill in the Chamber of Deputies explicitly noted that the proposal aimed to establish more technical and restrictive parameters building on the baseline set by the STF, introducing objective criteria and formal requirements that provide greater legal certainty (Agência Câmara 2025). Most importantly for present purposes, the law incorporates the same preventive logic that underpins the STF’s understanding of platform responsibility. The law explicitly enshrines a duty of care for both parents and service providers. Brazil now prohibits online platforms from using the data of children and adolescents in ways that violate their fundamental rights and best interests and requires companies to assess and mitigate the risks to which they expose younger users. Key measures in ECA Digital include prohibitions on manipulative design and commercially exploitative practices such as behavioral profiling and emotional analysis.

The developments extending from the STF decision are also visible in the two regulatory decrees issued under the President’s constitutional regulatory authority. Decree No. 12.975/2026 updates the 2016 MCI regulations to establish the administrative procedures and parameters necessary to implement the STF’s framework. The STF had shifted the focus of platform liability from the analysis of individual pieces of content to the evaluation of systemic failures and ancillary duties such as transparency and due process. The decree gives practical effect to this approach by specifying how providers must organize compliance structures, reporting channels, transparency mechanisms, and risk-management processes. For example, Article 16-A mandates that platforms must provide comprehensive information regarding their internal moderation procedures, algorithmic profiling, and systemic risk management, and that they are required to maintain permanent and accessible reporting channels for illegal content. A companion instrument, Decree No. 12.976/2026, focuses specifically on violence against women. This decree organizes and specifies the duty of care regarding digital harassment and the non-consensual production of sexual deepfakes, directly targeting the massive circulation of such content on internet platforms. Together, the decrees demonstrate how concepts first articulated by the STF, particularly the duty of care, systemic risk, transparency, and due process, are being incorporated into Brazil’s emerging governance framework for digital platforms. In key sections, the government reproduced in the decrees the exact wording of the STF ruling.

The second major feature consolidated by these post-ruling developments is the appointment of an administrative authority to implement and supervise the new duties. This shift moves from a strictly civil liability regime enforced by the courts to a risk-management model overseen by a dedicated regulator. The need for this institutional structure was also debated during the STF proceedings. Although the justices broadly agreed that stronger oversight is indispensable, they disagreed on how it should be achieved. Justice Dias Toffoli referred to the National Justice Council, Flávio Dino to the Prosecutor General's Office, Alexandre de Moraes to the telecommunications regulator, Anatel, Luís Roberto Barroso to a multistakeholder arrangement, Cristiano Zanin to enhanced self-regulation, and Gilmar Mendes to the National Data Protection Authority (ANPD) as the most suitable forum for "accountability and supervision" (*MCI Ruling 2025*, at 819).

This judicial disagreement over the exact institutional design did not prevent the Executive from selecting an agency. First, Congress designated the ANPD to regulate proactive duties of platforms created by ECA Digital. Several months later, the Executive also selected the ANPD, but for the role of overseeing the duty of care, transparency and due-process obligations established by Decree No. 12.975/2026. The government claimed it was merely following the Congressional decision to hand the task to the ANPD (Galf 2026). It is unclear whether the role created by Congress in ECA Digital is the same as that envisaged by the STF. Either way, both the ECA Digital legislation and the May 2026 regulatory decrees explicitly designate the ANPD as the regulator responsible for implementing and overseeing the new regimes of proactive duties. But both also make it explicit that the agency's role is not to determine the legality of individual pieces of content but to supervise compliance processes, internal policies, transparency obligations, and risk-management mechanisms.

This distinction is central to the emerging model of platform governance in Brazil. Questions concerning liability for specific content remain subject to judicial determination, while the ANPD is tasked with overseeing the organizational and procedural obligations associated with the duty of care. In this capacity, the agency can develop technical standards, supervisory guidance, and assessment criteria for concepts such as systemic failure, risk mitigation, and compliance with platform duties. These standards may contribute to greater consistency and legal certainty by providing courts with a more structured basis for evaluating whether a platform has fulfilled its duty of care when liability is alleged to arise from systemic failures, as discussed above. Such an arrangement may also help safeguard freedom of expression by reducing the uncertainty associated with broadly framed duties and by clarifying the circumstances under which platforms may be held responsible under this new regime.

Our analysis therefore suggests the emergence of a hybrid model combining judicial standards with administrative oversight. The STF established the core normative framework by redefining intermediary liability and introducing preventive duties linked to systemic risks. Subsequent legislation and executive regulation have translated those principles

into more specific obligations and assigned responsibility for their supervision to the ANPD. This arrangement aligns with the preventive logic of the duty of care, which as we previously argued (Hartmann et al. 2026) pairs judicial enforcement of liability with ongoing administrative monitoring.

5 Concluding Remarks

This commentary examined how the Federal Supreme Court's decision on the Marco Civil da Internet attempts to reconfigure the relationship between platforms, users, and the State. The judgment emerged from the structural weaknesses of Brazil's intermediary liability framework. Article 19's narrow, court-order model proved unable to address the scale and complexity of contemporary platforms, where content distribution is shaped by algorithmic systems and monetized amplification. Against this background, the STF's intervention was almost unavoidable. It responded to a real deficit of protection, but in doing so it crossed into a space that normally belongs to the legislature.

The ruling marks a significant conceptual shift. By introducing a new liability regime linked to a duty of care and to the idea of systemic failure, the Court sought to move from a reactive system of content removal toward one centered on preventive governance. It also introduced annex and instrumental duties (e.g. obligations of transparency, due process, and local representation) that can serve as reference points for interpreting what diligence should mean under the new regime. While these were only partial solutions, recent legislative developments in Brazil—including ECA Digital and the regulatory decrees of the MCI which appointed the ANPD as a dedicated regulatory authority capable of auditing compliance and enforcing these duties—point to a hybrid system of judicial standards and administrative compliance.

The decision therefore exposes a dual reality. It demonstrates the Court's capacity to adapt an outdated statute to the new realities of digital platforms, but it also highlights the fragility of judicial law-making as a means of sustaining governance at scale. While some will see the STF's expansive approach as necessary to fill a political and legislative vacuum, others will read it as a form of judicial overreach that risks blurring the boundary between interpretation and regulation. Both perspectives reveal the same truth: effective platform accountability requires not only new *ex post* liability regimes, but also new *ex ante* positive obligations and functioning institutions able to implement them.

References

- Agência Câmara de Notícias. 2025. “Câmara aprova projeto sobre proteção de crianças em ambientes digitais.” Câmara dos Deputados, August 20, 2025. <https://www.camara.leg.br/noticias/1191188-camara-aprova-projeto-sobre-protecao-d-e-criancas-em-ambientes-digitais>.
- Almeida, Guilherme da Franca Couto Fernandes de, Fábio Carvalho Leite, and Rodolfo Assis. 2024. “O direito sem respeito às regras.” *Revista de Informação Legislativa* 61 (242): 215–34. https://doi.org/10.70015/ril_v61_n242_p215.
- Angelopoulos, Christina, and Stijn Smet. 2016. “Notice-and-Fair-Balance: How to Reach a Compromise between Fundamental Rights in European Intermediary Liability.” *Journal of Media Law* 8 (2): 266–301. <https://doi.org/10.1080/17577632.2016.1240957>.
- Arguelhes, Diego Werneck, and Leandro Molhano Ribeiro. 2018a. “Ministrocracia: O Supremo Tribunal individual e o processo democrático brasileiro.” *Novos Estudos CEBRAP* 37 (1): 13–32. <https://doi.org/10.25091/S01013300201800010003>.
- . 2018b. “‘The Court, It Is I’? Individual Judicial Powers in the Brazilian Supreme Court and Their Implications for Constitutional Theory.” *Global Constitutionalism* 7 (2): 236–62. <https://doi.org/10.1017/S2045381718000072>.
- Bentes, Anna. 2023. *Eleições, direitos digitais e desinformação: Desafios e aprendizagens a partir da experiência brasileira em 2022*. Derechos Digitales. <https://www.derechosdigitales.org/wp-content/uploads/DD-Desinfo-2023-PT.pdf>.
- Brito Cruz, Francisco. 2015. “Direito, democracia e cultura digital: A experiência de elaboração legislativa do Marco Civil da Internet.” Master’s thesis, Universidade de São Paulo.
- Brito Cruz, Francisco, Beatriz Kira, and Ivar A. Hartmann. 2025. *Duty of Care and Regulation of Digital Platforms: A Brazilian Perspective*. Policy Brief No. 1. University of Sussex & Insper. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5176187.
- Brunner, Lisl. 2016. “The Liability of an Online Intermediary for Third Party Content: The Watchdog Becomes the Monitor: Intermediary Liability after *Delfi v Estonia*.” *Human Rights Law Review* 16 (1): 163–74. <https://doi.org/10.1093/hrlr/ngv048>.
- Caplan, Robyn. 2018. *Content or Context Moderation? Artisanal, Community-Reliant, and Industrial Approaches*. Data & Society Research Institute. <https://datasociety.net/library/content-or-context-moderation/>.
- Comitê Gestor da Internet no Brasil (CGI.br). 2015. *ICT Households 2014*. https://cgi.br/media/docs/publicacoes/2/TIC_DOM_2014_LivroEletronico.pdf.
- . 2025. *Pesquisa sobre o uso das tecnologias de informação e comunicação nos domicílios brasileiros: TIC Domicílios 2024*. https://cetic.br/media/docs/publicacoes/2/20250512120132/tic_domicilios_2024_livro_eletronico.pdf.

- Conselho Nacional de Justiça. 2024. *Justiça em Números 2024*. <https://www.cnj.jus.br/pesquisas-judiciarias/justica-em-numeros/>.
- Da Ros, Luciano, and Matthew M. Taylor. 2022. "Bolsonaro and the Judiciary: Between Accommodation and Confrontation." In *Brazil under Bolsonaro: How Endangered Is Democracy?*, edited by Peter Birle and Bruno Speck, 44–54. Berlin: Ibero-Amerikanisches Institut Preußischer Kulturbesitz. https://publications.iai.spk-berlin.de/servlets/MCRFileNodeServlet/iai_derivate_00000130/IO_14_DaRosTaylor_BolsonaroJudiciary_Web.pdf?ref=europeans.today.
- de Freitas, Riva Sobrado, and Matheus Felipe de Castro. 2013. "Liberdade de expressão e discurso do ódio: Um exame sobre as possíveis limitações à liberdade de expressão." *Seqüência Estudos Jurídicos e Políticos* 34 (66): 327–55. <https://doi.org/10.5007/2177-7055.2013v34n66p327>.
- de Lima, Cíntia Rosa Pereira. 2015. "A responsabilidade civil dos provedores de aplicação de internet por conteúdo gerado por terceiro antes e depois do Marco Civil da Internet (Lei n. 12.965/14)." *Revista da Faculdade de Direito da Universidade de São Paulo* 110:155–76. <https://doi.org/10.11606/issn.2318-8235.v110i0p155-176>.
- Edwards, Lilian. 2009. "The Rise and Fall of Online Intermediary Liability." In *Law and the Internet*, 3rd ed., edited by Lilian Edwards and Charlotte Waelde, 47–88. Hart Publishing.
- Evangelista, Rafael, and Fernanda Bruno. 2019. "WhatsApp and Political Instability in Brazil: Targeted Messages and Political Radicalization." *Internet Policy Review* 8 (4). <https://doi.org/10.14763/2019.4.1434>.
- Flew, Terry, Fiona Martin, and Nicolas Suzor. 2019. "Internet Regulation as Media Policy: Rethinking the Question of Digital Communication Platform Governance." *Journal of Digital Media & Policy* 10 (1): 33–50. https://doi.org/10.1386/jdmp.10.1.33_1.
- Galf, Renata. 2026. "Decreto de Lula sobre redes com atribuições para agência fiscalizadora gera debate sobre legalidade." *Folha de S.Paulo*, May 26, 2026. <https://www1.folha.uol.com.br/poder/2026/05/decreto-de-lula-sobre-redes-com-atribuicoes-para-agencia-fiscalizadora-gera-debate-sobre-legalidade.shtml>.
- Garfield Tenzer, Leslie Y. 2025. "A Supreme Sidestep: The Justices' Artful Dodge on Platform Immunity." *Northwestern Journal of Technology and Intellectual Property* 22 (2). <https://scholarlycommons.law.northwestern.edu/njtip/vol22/iss2/3/>.
- Gorwa, Robert. 2019. "The Platform Governance Triangle: Conceptualising the Informal Regulation of Online Content." *Internet Policy Review* 8 (2). <https://doi.org/10.14763/2019.2.1407>.
- Gorwa, Robert, Reuben Binns, and Christian Katzenbach. 2020. "Algorithmic Content Moderation: Technical and Political Challenges in the Automation of Platform Governance." *Big Data & Society* 7 (1). <https://doi.org/10.1177/2053951719897945>.

- Gupta, Indranath, and Lakshmi Srinivasan. 2023. "Evolving Scope of Intermediary Liability in India." *International Review of Law, Computers & Technology* 37 (3): 294–324. <https://doi.org/10.1080/13600869.2022.2164838>.
- Hartmann, Ivar. 2026. "The Pitfalls of Judicial Intervention on Disinformation: An Account of the Brazilian 2022 Election." *Information, Communication & Society*, <https://doi.org/10.1080/1369118X.2026.2631701>.
- Hartmann, Ivar, Ramon Costa, Francisco Brito Cruz, and Beatriz Kira. 2026. "Platform Duty of Care after the Supreme Court Ruling on the Marco Civil da Internet." *Seqüência Estudos Jurídicos e Políticos* 46 (99): 1–33. <https://doi.org/10.5007/2177-7055.2025.e109919>.
- Hartmann, Ivar, and Julia Iunes. 2020. "Fake news no contexto de pandemia e emergência social: Os deveres e responsabilidades das plataformas de redes sociais na moderação de conteúdo online entre a teoria e as proposições legislativas." *Revista de Direito Público* 17 (94): 388–414. <https://www.portaldeperiodicos.idp.edu.br/direitopublico/article/view/4607>.
- Hirabahasi, Guilherme, and Thais Tortella. 2022. "Alexandre de Moraes determina bloqueio do Telegram no Brasil." CNN Brasil. <https://www.cnnbrasil.com.br/nacional/alexandre-de-moraes-determina-bloqueio-do-telegram-no-brasil/>.
- Joia, Luiz Antonio. 2004. "Bridging the Digital Divide: Some Initiatives in Brazil." *Electronic Government: An International Journal* 1 (3). <https://doi.org/10.1504/EG.2004.005554>.
- Jost, Iná, and Francisco Brito Cruz. 2024. "X vs. Brazil: What Questions Remain after the Turmoil?" Tech Policy Press, October. <https://techpolicy.press/x-vs-brazil-what-questions-remain-after-the-turmoil/>.
- Kaye, David. 2019. *Speech Police: The Global Struggle to Govern the Internet*.
- Keller, Clara Iglesias. 2021. "Policy by Judicialisation: The Institutional Framework for Intermediary Liability in Brazil." *International Review of Law, Computers & Technology* 35 (3): 185–203. <https://doi.org/10.1080/13600869.2020.1792035>.
- Keller, Daphne. 2023. "Carriage and Removal Requirements for Internet Platforms: What Taamneh Tells Us." *Journal of Free Speech Law* 4 (1): 87–138. <https://www.journaloffreespeechlaw.org/keller3.pdf>.
- Kira, Beatriz. 2025. "Regulatory Intermediaries in Content Moderation." *Internet Policy Review* 14 (1). <https://doi.org/10.14763/2025.1.1824>.
- Kira, Beatriz, Clara Iglesias Keller, Gabriel Wajman, Francisco Brito Cruz, Bruno R. Bioni, Laura Schertel, Gabriel Fonseca, and Nina Fernandes dos Santos. 2025. *Current Challenges in Digital Elections: Lessons from Electoral Regulation and Digital Campaigning in Brazil*. Discussion Paper No. 52. Weizenbaum Institute. <https://www.econstor.eu/bitstream/10419/334438/1/Full-text-report-Kira-et-al-Current-challenges.pdf>.

- Lancieri, Filippo, Caio Mario da Silva Pereira Neto, Rodrigo Moura Karolczak, and Barbara Marchiori de Assis. 2026. "Adjudicating Fake News." *Cornell International Law Journal* 58 (3): 407–56. <https://publications.lawschool.cornell.edu/cilj/2026/05/07/adjudicating-fake-news/>.
- Lima, Daniel. 2023. "Moraes determina suspensão do Telegram por 72 horas caso aplicativo não remova mensagem sobre PL das Fake News." CNN Brasil. <https://www.cnnbrasil.com.br/politica/moraes-determina-suspensao-do-telegram-por-72-horas-caso-aplicativo-nao-remova-mensagem-sobre-pl-das-fake-news/>.
- Lorenzetto, Bruno Meneses, and Ricardo dos Reis Pereira. 2020. "O supremo soberano no estado de exceção: A (des)aplicação do direito pelo STF no âmbito do inquérito das 'Fake News' (Inquérito n. 4.781)." *Seqüência Estudos Jurídicos e Políticos* 41 (85): 173–203. <https://doi.org/10.5007/2177-7055.2020v41n85p173>.
- Machado, Caio, Beatriz Kira, Vidya Narayanan, Bence Kollanyi, and Philip Howard. 2019. "A Study of Misinformation in WhatsApp Groups with a Focus on the Brazilian Presidential Elections." In *Companion Proceedings of the 2019 World Wide Web Conference*, 1013–19. <https://doi.org/10.1145/3308560.3316738>.
- MCI Ruling: STF, Recurso Extraordinário 1.037.396 (Tema 987), Plenário, Rel. Min. Dias Toffoli (2025), <https://redir.stf.jus.br/paginadorpub/paginador.jsp?docTP=TP&docID=792325589>.
- Mendes, Luís. 2024. "Alexandre de Moraes ordena suspensão imediata do X no Brasil." CNN Brasil. <https://www.cnnbrasil.com.br/politica/alexandre-de-moraes-manda-bloquear-o-x-no-brasil/>.
- Neri, Marcelo. 2019. *As classes médias brasileiras*. FGV Social. <https://www.cps.fgv.br/cps/bd/papers/es106-As-Classes-Medias-Brasileiras.pdf>.
- Newman, Nic, Richard Fletcher, Antonis Kalogeropoulos, and Rasmus Kleis Nielsen. 2019. *Reuters Institute Digital News Report 2019*. Reuters Institute for the Study of Journalism. https://reutersinstitute.politics.ox.ac.uk/sites/default/files/inline-files/DNR_2019_FINAL.pdf.
- Nexus Pesquisa e Inteligência de Dados. 2025. *A visão dos brasileiros sobre regulamentação das redes sociais*. <https://www.nexus.fsb.com.br/estudos-divulgados/6-em-cada-10-apoiam-a-regulamentacao-das-redes-sociais/>.
- Nicas, Jack. 2022. "To Fight Lies, Brazil Gives One Man Power over Online Speech." *New York Times*, October 21, 2022. <https://www.nytimes.com/2022/10/21/world/americas/brazil-election-misinformation-alexandre-de-moraes.html>.
- Nishijima, Marislei, Terry Macedo Ivanauskas, and Flavia Mori Sarti. 2017. "Evolution and Determinants of Digital Divide in Brazil (2005–2013)." *Telecommunications Policy* 41 (1): 12–24. <https://doi.org/10.1016/j.telpol.2016.10.004>.

- Oliva, Thiago. 2019. "Responsabilidade de intermediários e a garantia da liberdade de expressão na rede." InternetLab. <https://internetlab.org.br/pt/especial/responsabilidade-de-intermediarios-e-a-garantia-da-liberdade-de-expressao-na-rede/>.
- Parr, Nathaniel. 2024. "How Civil Aiding and Abetting Liability for Terrorist Activities Applies to Social Media Companies and How It Does Not." *University of Chicago Legal Forum* 2024. <https://chicagounbound.uchicago.edu/uclf/vol2024/iss1/17/>.
- Psychogiopoulou, Evangelia. 2021. "Judicial Dialogue in Social Media Cases in Europe: Exploring the Role of Peers in Judicial Adjudication." *German Law Journal* 22 (6): 915–35. <https://doi.org/10.1017/glj.2021.57>.
- Ribeiro, Márcio Moretto, and Pablo Ortellado. 2018. "Fake News: What It Is and How to Deal with It." *Sur* 15 (27): 69–81. <https://sur.conectas.org/en/fake-news-what-it-is-and-how-to-deal-with-it/>.
- Santos, João Guilherme Bastos dos, Miguel Freitas, Alessandra Aldé, Karina Santos, and Vanessa Cristine Cardozo Cunha. 2019. "WhatsApp, política mobile e desinformação: A hidra nas eleições presidenciais de 2018." *Comunicação & Sociedade* 41 (2): 307–34. <https://doi.org/10.15603/2175-7755/cs.v41n2p307-334>.
- Sarmiento, Daniel. 2006. *Livres e iguais: Estudos de direito constitucional*. Rio de Janeiro: Lumen Juris.
- Sátiro, Renato Máximo, Marcos de Moraes Sousa, Murilo Marques Costa, and Pedro Miguel Alves Ribeiro Correia. 2025. "Unlocking the Judiciary: Predictive Determinants of Actual and Potential Access to Brazilian State Courts." *Brazilian Administration Review* 22 (3). <https://doi.org/10.1590/1807-7692bar2025240160>.
- Schreiber, Anderson. 2015. "Marco Civil da Internet: Avanço ou retrocesso? A responsabilidade civil por dano derivado do conteúdo gerado por terceiro." In *Direito & Internet III—Tomo II: Marco Civil da Internet (Lei n. 12.965/2014)*, edited by Newton De Lucca, Adalberto Simão Filho, and Cíntia Rosa Pereira de Lima, 277–304. São Paulo: Quartier Latin.
- Souza, Carlos Affonso, and Ronaldo Lemos. 2016. *Marco Civil da Internet: Construção e aplicação*.
- Spano, Robert. 2017. "Intermediary Liability for Online User Comments under the European Convention on Human Rights." *Human Rights Law Review* 17 (4): 665–79. <https://doi.org/10.1093/hrlr/ngx001>.
- Taylor, Matthew M. 2024. "Brazil's Rule-of-Law Regression." *Current History* 123 (850): 43–49. <https://doi.org/10.1525/curh.2024.123.850.43>.
- Thompson, Marcelo. 2016. "Beyond Gatekeeping: The Normative Responsibility of Internet Intermediaries." *Vanderbilt Journal of Entertainment & Technology Law* 18 (4). <https://scholarship.law.vanderbilt.edu/jetlaw/vol18/iss4/4/>.

- Tuchtfeld, Eike. 2024. *Case Law on Content Moderation and Freedom of Expression*. 2nd ed. <https://globalfreedomofexpression.columbia.edu/wp-content/uploads/2025/01/Second-Edition-November-2024.pdf>.
- Vieira, Oscar Vilhena. 2023. “O STF e a defesa da democracia no Brasil.” *Journal of Democracy em Português* 12 (1): 7–55. <https://fundacaofhc.org.br/arquivos/jun-23/JoD-jun23-completo.pdf>.
- We Are Social. 2024. *Digital 2024: Global Overview Report*. <https://wearesocial.com/uk/blog/2024/01/digital-2024/>.
- Zingales, Nicolo. 2015. “The Brazilian Approach to Internet Intermediary Liability: Blueprint for a Global Regime?” *Internet Policy Review* 4 (4). <https://doi.org/10.14763/2015.4.395>.

Authors

Beatriz Kira is an Associate Professor of Law at the University of Exeter, United Kingdom. Email: b.kira@exeter.ac.uk.

Ivar Hartmann is an Associate Professor of Law at Insper, São Paulo. Email: ivaragmlh@insper.edu.br.

Acknowledgments

The authors would like to thank participants at ICON-S Annual Conference 2025 in Brasília, AoIR 2025 in Niterói, a panel at Chicago-Kent College of Law, and the panel “Platforms, Courts and Online Speech” at Harvard Law School, where an earlier version of this work was presented, for the discussions that greatly benefited it. We are particularly grateful to Clara Iglesias Keller, Marcelo Thompson, Francisco Brito Cruz, Artur Pericles Lima Monteiro, Rafael Bezerra Nunes, and Marshall van Alstyne. We also thank the anonymous peer reviewers for their suggestions, which greatly improved the work.

Funding Statement

This work was produced as part of the academic project “Platform regulation in Brazil and in the UK: designing and enforcing ‘duty of care’ frameworks,” funded by the British Academy’s ODA Challenge-Oriented Research Grants 2024 Programme, supported under the UK Government’s International Science Partnerships Fund (No. IOCRG 100823).

Disclosure Statement

The authors declare no competing interests.

Keywords

Intermediary liability; platform regulation; Marco Civil da Internet; duty of care; Brazil