PANORAMIC

ONLINE SAFETY REGULATION 2026

Contributing Editors

Jenna Rennie, **Rory Hishon** and **Alexander Beaton**

White & Case LLP

LEXOLOGY

Online Safety Regulation 2026

Contributing Editors

Jenna Rennie, Rory Hishon and Alexander Beaton

White & Case LLP

A comparative guide to online safety regulation in key jurisdictions worldwide. Topics covered include the legal framework for combating online harms; obligations for online service providers, including risk assessments and mitigation; enforcement and penalties; and disputes, including remedies and defences.

Generated on: February 3, 2026

Overview

Jenna Rennie, Rory Hishon and Alexander Beaton

White & Case LLP

Overview

The rapidly developing global online safety environment

Over the past decade, online safety has become the subject of intense legislative and regulatory debate across multiple jurisdictions. Globally, the regulation of online safety is experiencing a clear trend away from reactive notice-and-takedown regimes toward risk-based, systemic regulation, particularly focusing on child protection, harmful but lawful content and platform accountability.

However, while there is global convergence in many areas, some significant differences remain. The chapters that follow provide detailed jurisdiction-specific analyses of major jurisdictions, including Brazil, the European Union (and its constituent member states), the United Kingdom and the United States. This overview chapter identifies the key themes in online safety regulation emerging across those jurisdictions.

Comprehensive frameworks versus sector-specific laws

Several jurisdictions, including the UK (through the Online Safety Act 2023) and the EU (through the Digital Services Act) have implemented broad, cross-sectoral regimes specifically targeting online safety. These comprehensive frameworks represent a shift from harm-specific interventions to a systemic, risk-based approach backed by robust regulatory oversight. These laws establish duties for online intermediaries to assess, mitigate and report on the risks that their services pose to users.

In contrast, jurisdictions such as Brazil, the Dominican Republic and the US tend to regulate content online by relying on existing laws (eg, relating to criminal, consumer protection, data protection and child protection matters) rather than enacting a single unified statute. In the US, some state-level laws are emerging but facing legal challenges. Brazil is currently a hybrid model, with court rulings imposing some proactive duties, but is moving toward a more comprehensive approach.

This fragmentation reflects not only different regulatory philosophies but also constitutional and political constraints.

Harmful but legal content

All jurisdictions regulate illegal content, such as child sexual abuse material and content that constitutes terrorism, hate speech or fraud to some extent. This represents the (uncontroversial) core of online safety regulation; namely content that is illegal offline should

also be illegal online. However, the regulatory landscape becomes more complex when it comes to content that is harmful but not unlawful, and wider societal risks.

Brazil, the EU and the UK address content that is harmful but not necessarily unlawful, especially regarding child protection, by imposing duties on platforms to protect minors from exposure to harmful material such as pornography, content promoting self-harm, eating disorders or bullying, even where such content may be lawful for adult audiences.

However, the US's approach is more limited, in part reflecting constitutional free speech protections. These divergent approaches highlight one of the fundamental questions in online safety law: how to balance freedom of expression with protecting people, especially minors, from harmful content.

Many regimes are also starting to address new risks such as AI-generated content (such as deepfakes), disinformation and addictive platform features. These emerging harms often sit outside the traditional boundaries of legal and illegal content, requiring regulators to grapple with novel questions about algorithmic amplification and the psychological impacts of platform design.

Changing platform obligations: from notice-and-takedown to proactive risk management

Most jurisdictions have some form of notice-and-takedown mechanism for illegal content, although the scope and process of these varies. In the Brazil, the EU and the UK, these statutory mechanisms provide a procedural framework for users, trusted flaggers and authorities to report illegal content, with platforms potentially becoming liable for such content if they do not act expeditiously to remove it once on notice of it.

However, in the US, notice-and-takedown is sector-specific (eg, relying on the DMCA for copyright; the Take It Down Act for non-consensual intimate imagery), with no general obligation to put in place a reporting mechanism for all unlawful content. Similarly, in the Dominican Republic, there is no comprehensive notice-and-takedown regime, with removal often requiring a court order.

However, the shift in many jurisdictions towards comprehensive regulation has resulted in a significant evolution of platform obligations. Brazil, the EU and UK now require or strongly encourage risk assessments and proactive mitigation measures, especially for platforms likely to be accessed by minors. Accordingly, this approach represents a move away from purely reactive content moderation toward a system whereby platforms must identify, assess and mitigate foreseeable risks before harm occurs.

Balancing competing rights

All regimes recognise the need to balance online safety with freedom of expression, privacy and due process. The US stands out in this regard for its strong First Amendment protections, which limit the ability of lawmakers to regulate lawful but harmful content.

Proportionality tests, transparency requirements and user rights to challenge content removal are common, especially across the EU. These procedural safeguards are intended to ensure that platform moderation decisions are not arbitrary, that users understand why content has been removed or restricted and that there are meaningful avenues for appeal and redress.

The tension between safety and rights is particularly evident in debates over disinformation and misinformation. The EU and UK place obligations on large platforms to assess and mitigate systemic risks from disinformation, especially during elections. In the US, there is no general obligation due to the First Amendment, with action limited to cases of fraud, defamation or deceptive commercial practices. Brazil has no unified statutory obligation but courts and electoral authorities have imposed requirements in specific contexts, while the Dominican Republic has no explicit obligations, but related harms (such as defamation and fraud) are addressed under general law.

Enforcement

Specialised regulators (including ANPD in Brazil, ARCOM in France, BNetzA in Germany and Ofcom in the UK) are empowered to enforce online safety laws, often with the ability to impose substantial fines. Online service providers can face administrative, civil and sometimes criminal penalties for non-compliance, with individual liability for directors or employees rare but possible in cases of wilful misconduct or criminal acts.

In the UK and EU, regulators can impose significant fines (up to 6-10 per cent of global turnover), corrective orders and, in some cases, criminal sanctions.

In the US, the FTC and DoJ can impose civil and criminal penalties, and state attorneys-general enforce state laws, but civil liability for intermediaries is generally limited. Brazil provides for fines, suspension and criminal penalties, especially for child protection violations, while in the Dominican Republic, administrative, civil and criminal penalties apply, with personal liability possible for directors or employees in some cases.

Although regulators across jurisdictions are increasingly empowered to impose significant penalties, the availability of private enforcement varies. In Brazil, the Dominican Republic and the EU, individuals can bring civil claims for damages and/or injunctive relief. In the UK, there is no general private right of action under the Online Safety Act, with enforcement primarily regulatory. In the US, section 230 of the Communications Act generally bars civil claims against platforms for user-generated content, but claims may proceed on other grounds, such as for product liability or deceptive practices.

Safe harbours still provide refuge

Most regimes provide conditional liability exemptions for intermediaries, especially when they act expeditiously to remove illegal content upon notice. These safe harbour provisions reflect a policy judgement that intermediaries should not be treated as publishers or held strictly liable for user-generated content, provided they meet certain conditions.

Demonstrating due diligence, prompt action and compliance with codes of practice can limit liability. However, the scope and conditions of these exemptions vary considerably. In the US, section 230 has historically provided broad immunity, shielding intermediaries from most civil liability for third-party content. Conversely, the Digital Services Act and national laws in the EU impose more stringent conditions, requiring platforms to act expeditiously upon notice.

The road ahead

There is broad agreement across jurisdictions on the need to combat illegal content, protect children and increase accountability. Comprehensive frameworks, proactive risk assessment and strong regulators are becoming the norm.

However, significant differences remain, shaped by constitutional traditions, political cultures and regulatory philosophies. The US remains less interventionist when it comes to regulating online safety, in part due to its strong constitutional protections for free speech. The EU, UK and several other jurisdictions are instead moving toward more proactive, comprehensive regimes. The treatment of harmful but legal content, the regulation of disinformation, the scope of safe harbours and the availability of private enforcement all vary considerably.

In the immediate future, AI-generated content and disinformation are becoming central to online safety debates, with regulatory responses evolving rapidly. As technology evolves and new harms emerge, online safety law will continue to develop. The chapters that follow provide detailed insights into how individual jurisdictions are navigating these challenges, offering valuable lessons for practitioners seeking to understand and shape the future of global online safety regulation.

Any views expressed in this publication are strictly those of the authors and should not be attributed in any way to White & Case LLP.

WHITE & CASE

Jenna Rennie — jenna.rennie@whitecase.com
Rory Hishon — rhishon@whitecase.com
Alexander Beaton — alexander.beaton@whitecase.com

White & Case LLP